

***‘Een AVG-proof privacybeleid’***

**Toetsing van:**

**Afstudeeronderzoek**

[**HBR-AS17-AS**](https://studievolg.hsleiden.nl/student/OnderwijsToonCursus.do?cursuscode=HBR-AS17-AS&collegejaar=2017&aanvangsblok=JAAR)

**Hogeschool Leiden Opleiding HBO-Rechten**

Rosaline Rodenburg – s1047384 Onderzoeksdocent: mw. M. Rietmeijer

Afstudeerbegeleider: dhr. R. Koning

Opdrachtgever:

Praktijkbegeleider:

Inleverdatum: 13 juni 2018

Klas: RE4B, collegejaar 2017/2018 Reguliere kans

# Voorwoord

*Geachte lezer,*

*Voor u ligt mijn afstudeeronderzoek, mijn scriptie. Een onderzoek waar ik heel trots op ben. Ondanks alle tegenslagen tijdens mijn studie ben ik dan toch op het punt beland dat ik mijn scriptie heb mogen schrijven.*

*Mijn grootste dank gaat uit naar mijn familie, die mij waar mogelijk geholpen en gesteund heeft. Ook wil ik graag mijn afstudeerbegeleider, dhr. Koning en mijn onderzoeksdocent, mevr. Rietmeijer bedanken voor alle hulp, fijne en goede feedback en het begrip voor mijn persoonlijke situatie.*

*Tot slot wil ik graag mijn opdrachtgever, bedanken voor het bieden van een afstudeeropdracht over een interessant en actueel onderwerp.*

*Ik wens u veel leesplezier*

*Rosaline Rodenburg  
Uitgeest, 11 juni 2018*

# Samenvatting

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing in de hele Europese Unie (EU). De AVG vervangt de Wet bescherming persoonsgegevens (Wbp), een wet die gebaseerd was op een richtlijn uit 1995.

De AVG geeft natuurlijke personen waarvan de persoonsgegevens verwerkt worden meer rechten en organisaties die de persoonsgegevens verwerken meer plichten, met als voornaamste doel: het niveau van bescherming van persoonsgegevens verhogen.

Opdrachtgever, een toeleverancier van fijnmechanische onderdelen en mechatronische modules bestemd voor de hightech industrie heeft mij verzocht om haar privacybeleid waar nodig aan te passen zodat zij voldoet aan de bepalingen uit de AVG. Dit bracht mij tot de volgende centrale vraag: *“Welke aanpassingen dient opdrachtgever op basis van wetsanalyse, literatuuronderzoek en interviews met medewerkers te maken aan haar huidig privacybeleid om aan te kunnen tonen dat zij voldoet aan de Algemene Verordening Gegevensbescherming?”* Met als doel het opstellen van een privacybeleid waarmee opdrachtgever aan kan tonen dat zij voldoet aan de verplichtingen uit de AVG. Om dit doel te behalen, heb ik een format verwerkingsregister, privacyverklaring, format datalekregister en verwerkersovereenkomst opgesteld.

Verder heb ik aan de hand van onderstaande deelvragen en bijbehorende onderzoeksmethoden de centrale vraag beantwoord:

1. Welke verplichtingen heeft Opdrachtgever op grond van wetsanalyse en literatuuronderzoek volgens de AVG?
2. Welke persoonsgegevens verwerkt Opdrachtgever volgens de geïnterviewde medewerkers en dossieronderzoek?
3. Op welke manier worden persoonsgegevens volgens de geïnterviewde medewerkers en dossieronderzoek door Opdrachtgever verwerkt?
4. Op welke manier kan Opdrachtgever volgens wetsanalyse en literatuuronderzoek aantonen dat zij voldoet aan haar verplichtingen die volgen uit de AVG?

Uit het onderzoek blijkt dat Opdrachtgever aan een zevental verplichtingen moet voldoen om aan te kunnen tonen dat zij voldoet aan de AVG:

* Een verwerkingsregister opstellen en bijhouden;
* Een privacyverklaring opstellen om betrokkenen te informeren;
* De grondslag “gerechtvaardigd belang” onderbouwen;
* Verwerkersovereenkomsten afsluiten met alle verwerkers;
* Een datalekregister en datalekprocedure opstellen en bijhouden;
* Privacy by design en privacy by default in acht nemen;
* DPIA uitvoeren of beargumenteren waarom dit niet noodzakelijk is.

Na de interviews met medewerkers van verschillende afdelingen is gebleken dat er nog geen privacybeleid is, er dient dus vanaf stap 1 gestart te worden met het opstellen van een nieuw beleid. In de tijd die ik voor het uitvoeren van dit onderzoek had, is het niet gelukt om een geheel beleid op te stellen, wel heb ik documenten opgesteld die als goede basis kunnen dienen.

Het advies aan Opdrachtgever is om de door mij opgestelde documenten zo spoedig mogelijk in gebruik te nemen en aan de hand van deze documenten en het volledige onderzoek een passend privacybeleid op te stellen. Tevens heb ik aanbevolen om één persoon aan te stellen die verantwoordelijk is voor het bijhouden van de registers en als aanspreekpunt dient voor alle privacy gerelateerde zaken.

Tot slot heb ik geadviseerd om een datalekprocedure en een intern beleid met betrekking tot privacy by design en privacy by default op te stellen, daar ik daar in dit onderzoek niet aan toe ben gekomen.

Inhoudsopgave

[Voorwoord 2](#_Toc516561919)

[Samenvatting 4](#_Toc516561920)

[Afkortingen 8](#_Toc516561921)

[Begrippen 8](#_Toc516561922)

[1. Inleiding 10](#_Toc516561923)

[1.1. Aanleiding onderzoek en probleemanalyse 10](#_Toc516561924)

[1.1.1. Organisatieschets Opdrachtgever 11](#_Toc516561925)

[1.2. Doelstelling, centrale vraag en deelvragen 12](#_Toc516561926)

[1.2.1. Centrale vraag 13](#_Toc516561927)

[1.2.2. Deelvragen 13](#_Toc516561928)

[2. Onderzoeksmethoden 14](#_Toc516561929)

[3. Juridisch kader 16](#_Toc516561930)

[3.1. Algemene Verordening Gegevensbescherming (AVG) 16](#_Toc516561931)

[3.1.1. Begrippen AVG 16](#_Toc516561932)

[3.1.2. Grondslagen voor verwerking 17](#_Toc516561933)

[3.1.3. Verantwoordingsplicht 20](#_Toc516561934)

[3.1.4. Verwerkersovereenkomst 30](#_Toc516561935)

[3.1.5. Datalekken 34](#_Toc516561936)

[3.2. Verwerking van persoonsgegevens door Opdrachtgever 35](#_Toc516561937)

[3.2.1. Welke persoonsgegevens verzameld Opdrachtgever? 36](#_Toc516561938)

[3.2.2. Hoe worden de persoonsgegevens verwerkt? 37](#_Toc516561939)

[4. Resultaten 42](#_Toc516561940)

[4.1. De door Opdrachtgever te nemen maatregelen 42](#_Toc516561941)

[5. Conclusies 50](#_Toc516561942)

[5.1. Beantwoording centrale vraag 50](#_Toc516561943)

[6. Aanbevelingen 52](#_Toc516561944)

[Literatuurlijst 54](#_Toc516561945)

[Bijlagen 58](#_Toc516561946)

[1. Schema 1: verwerker of verwerkingsverantwoordelijke? 58](#_Toc516561947)

[2. Schema 2: sancties/boetes AVG 59](#_Toc516561948)

[3. Datalek tabel 61](#_Toc516561949)

[4. Verwerkersovereenkomst 64](#_Toc516561950)

[5. Privacyverklaring 72](#_Toc516561951)

[6. Verwerkingsregister 77](#_Toc516561952)

[7. Vooraf opgestelde interviewvragen 78](#_Toc516561953)

[8. Transcripts 79](#_Toc516561954)

# Afkortingen

**AP**  
Autoriteit Persoonsgegevens

**AVG**  
Algemene Verordening Gegevensbescherming

**DPIA**Data Protection Impact Assessment

**EU**Europese Unie

**FG**Functionaris voor Gegevensbescherming

**Wbp**Wet bescherming persoonsgegevens

# Begrippen

**Toereikend privacybeleid**Het privacybeleid wordt aangemerkt als zijnde toereikend indien de bepalingen uit de AVG in acht worden genomen, Opdrachtgever aan kan tonen dat zij voldoet aan de AVG en de medewerkers aan de hand van het beleid hun werkzaamheden uit kunnen voeren zonder in strijd te handelen met de AVG.

**Voldoende beveiligd**De persoonsgegevens zijn voldoende beveiligd als er voldoende technische en organisatorische maatregelen zijn getroffen die een op het risico gebaseerde bescherming waarborgen.[[1]](#footnote-1)

# Inleiding

## Aanleiding onderzoek en probleemanalyse

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (hierna: AVG) van toepassing in de hele Europese Unie (EU). De AVG vervangt de Wet bescherming persoonsgegevens (Wbp), een wet die gebaseerd was op een richtlijn uit 1995.[[2]](#footnote-2) Sinds de invoering van de Wbp, is de mate waarin persoonsgegevens worden verwerkt flink gestegen.[[3]](#footnote-3) Mede daarom is de Algemene Verordening Gegevensbescherming (hierna: AVG) in het leven geroepen.

De AVG versterkt de rechten van de betrokkenen en de plichten van degenen die persoonsgegevens verwerken met als voornaamste doel het niveau van bescherming van persoonsgegevens te verhogen. Een ander doel van de AVG is het gelijk trekken van het niveau van gegevensbescherming in alle lidstaten van de EU.[[4]](#footnote-4)

Opdrachtgever is een toeleverancier van fijnmechanische onderdelen en mechatronische modules bestemd voor de hightech industrie.[[5]](#footnote-5) Met ongeveer 100 werknemers in dienst, een ruim klantenbestand en met het oog op de sancties[[6]](#footnote-6) die de Autoriteit Persoonsgegevens (AP) op kan leggen als niet voldaan wordt aan de bepalingen uit de AVG[[7]](#footnote-7), is het voor Opdrachtgever belangrijk om een toereikend privacybeleid te hebben.

Opdrachtgever verwerkt persoonsgegevens binnen de klant- en leveranciersadministratie en binnen de personeels- en loonadministratie. In de huidige situatie wordt er wel voldaan aan de hoofdregels van de Wbp ten aanzien van de bewaartermijnen en de manier van bewaren. Onder de AVG is dit echter niet toereikend.

Ook heeft opdrachtgever te maken met verwerkersovereenkomsten. Een organisatie die (een deel van) de verwerking van persoonsgegevens uitbesteed aan een verwerker, is verplicht om een verwerkersovereenkomst te sluiten met deze verwerker.[[8]](#footnote-8)

De AVG noemt verschillende specifieke punten die in ieder geval opgenomen moeten worden in deze verwerkersovereenkomsten. Het grootste verschil tussen de bewerkersovereenkomst en de verwerkersovereenkomst is de grotere verantwoordelijkheid van zowel de verwerkingsverantwoordelijke als de verwerker die terug te vinden is in art. 28 AVG.

Om te voldoen aan de nieuwe wetgeving, wil opdrachtgever haar huidig privacybeleid onder de loep nemen en deze waar nodig aanpassen en/of uitbreiden.

### Organisatieschets Opdrachtgever

Opdrachtgever heeft de volgende afdelingen:

* Inkoop/verkoop
* Kwaliteit
* Productie
* Financiële administratie
* Personeelszaken

Uit de informatie die ik van de medewerkers van de verschillende afdelingen heb gekregen[[9]](#footnote-9), blijkt dat er grote verschillen zijn tussen de afdelingen met betrekking tot verwerking van persoonsgegevens en het volgen van de wet- en regelgeving op dit gebied.

Op de afdelingen “verkoop” en “inkoop”, worden er voornamelijk persoonsgegevens geregistreerd van klanten en leveranciers.

Op dit moment wordt er op de afdelingen “verkoop” en “inkoop” niet tot nauwelijks rekening gehouden met de geldende wet- en regelgeving op het gebied van privacy. Medewerkers van deze afdelingen zijn niet op de hoogte van bewaartermijnen en weten niet in welke gevallen ze persoonsgegevens wel/niet mogen verwerken en hoe ze dit dan moeten doen.

De afdelingen “financiële administratie” en “personeelszaken”, voldoen voor het grootste deel wel aan de huidige wet- en regelgeving. Bewaartermijnen worden in acht genomen, persoonsgegevens worden niet zomaar gedeeld met derden en de persoonsgegevens zijn voldoende beveiligd.

Op de afdeling “productie” worden geen persoonsgegevens verzameld. Wel krijgen de managers van deze afdeling gegevens van een sollicitant door van personeelszaken. Daarnaast krijgen zij van de afdeling inkoop offertes doorgestuurd. Doordat ze op deze afdeling weinig bezig zijn met het verwerken van persoonsgegevens, wordt hier vrijwel geen aandacht aan besteed. Wel wordt er rekening gehouden met de bewaartermijnen van gegevens die zij doorkrijgen van andere afdelingen.

Tot slot geldt voor alle afdelingen dat persoonsgegevens zowel fysiek als digitaal opgeslagen worden. De fysiek opgeslagen gegevens zitten in kasten die alleen toegankelijk zijn voor de medewerkers van de afdelingen waar deze opgeslagen zijn. Digitaal worden de gegevens op servers opgeslagen die in eigen beheer zijn. Daarnaast zijn er persoonsgegevens terug te vinden in het e-mailprogramma dat door de medewerkers gebruikt wordt.

Delen van gegevens met derden  
Ook is het al bekend dat er in ieder geval drie partijen zijn die deze persoonsgegevens ook verwerken of er kennis van kunnen nemen:

* ADP voert een deel van de salarisadministratie uit en ontvangt hiervoor NAW-gegevens en bankgegevens van de medewerkers;
* ISSYS biedt ondersteuning bij computerproblemen en kan daardoor kennis nemen van de gegevens die opgeslagen zijn op de computers van medewerkers;
* Baken 5 ondersteunt Opdrachtgever bij de verzuimadministratie.

## 1.2. Doelstelling, centrale vraag en deelvragen

Het doel van dit onderzoek is door het huidig privacybeleid van Opdrachtgever te analyseren en te toetsen aan de nieuwe regels van de AVG, een nieuw privacybeleid op te stellen zodat Opdrachtgever aan kan tonen dat zij voldoet aan de verplichtingen uit de AVG.

Om ervoor te zorgen dat Opdrachtgever aan kan tonen dat zij voldoet aan de AVG, zal ik de volgende producten opnemen in het nieuwe privacybeleid:

* Format verwerkingenregister
* Privacyverklaring
* Datalek procedure
* Format datalekregister

### Centrale vraag

Welke aanpassingen dient Opdrachtgever op basis van wetsanalyse, literatuuronderzoek en interviews met medewerkers te maken aan haar huidig privacybeleid om aan te kunnen tonen dat zij voldoet aan de Algemene Verordening Gegevensbescherming?

### Deelvragen

Voor het beantwoorden van de centrale vraag, maak ik gebruik van onderstaande deelvragen:

1. Welke verplichtingen heeft Opdrachtgever op grond van wetsanalyse en literatuuronderzoek volgens de AVG?
2. Welke persoonsgegevens verwerkt Opdrachtgever volgens de geïnterviewde medewerkers en dossieronderzoek?
3. Op welke manier worden persoonsgegevens volgens de geïnterviewde medewerkers en dossieronderzoek door Opdrachtgever verwerkt?
4. Op welke manier kan Opdrachtgever volgens wetsanalyse en literatuuronderzoek aantonen dat zij voldoet aan haar verplichtingen die volgen uit de AVG?

# Onderzoeksmethoden

|  |  |
| --- | --- |
| Deelvraag 1 | Deelvraag 2 |
| Welke verplichtingen heeft Opdrachtgever op grond van wetsanalyse en literatuuronderzoek volgens de AVG? | Welke persoonsgegevens verwerkt Opdrachtgever volgens de geïnterviewde medewerkers en dossieronderzoek? |
| **Onderzoeksmethode** | **Onderzoeksmethode** |
| Voor het beantwoorden van deze deelvraag ga ik de AVG analyseren. Daarnaast zal ik gebruik maken van de volgende literatuur:  Boeken   * Grip op de AVG, de nieuwe privacywet * De Algemene Verordening Gegevensbescherming, artikelsgewijs commentaar * Checklist Privacy AVG, privacybeleid in 46 checklists   Handleidingen en richtlijnen   * Richtsnoeren voor gegevensbeschermingseffectbeoordelingen * Handleiding AVG van de Rijksoverheid | Voor het beantwoorden van deze vraag zal ik gebruik maken van een kleine inventarisatie van de door opdrachtgever verwerkte persoonsgegevens die reeds door opdrachtgever uitgevoerd is. Daarnaast zal ik gebruik maken van de kennis van medewerkers door onderstaande personen te interviewen:   * Manager en medewerker inkoop/verkoop * Manager en medewerker kwaliteit * Medewerker personeelszaken * Manager (tevens General Manager) productie * Manager en medewerker financiële administratie   De interviews zullen semigestructureerd zijn.[[10]](#footnote-10)  Tot slot zal ik dossieronderzoek uitvoeren door in de opslagsystemen van de geïnterviewde medewerkers te controleren of er nog meer persoonsgegevens opgeslagen zijn dan in de interviews naar voren is gekomen. |

|  |  |
| --- | --- |
| Deelvraag 3 | Deelvraag 4 |
| Op welke manier worden persoonsgegevens volgens de geïnterviewde medewerkers en dossieronderzoek door Opdrachtgever verwerkt? | Op welke manier kan Opdrachtgever volgens wetsanalyse en literatuuronderzoek aantonen dat zij voldoet aan haar verplichtingen die volgen uit de AVG? |
| **Onderzoeksmethode** | **Onderzoeksmethode** |
| Net als de tweede vraag zal ik deze vraag beantwoorden aan de hand van de kennis van medewerkers die bij de tweede deelvraag genoemd zijn. Daarnaast zal ik dossieronderzoek verrichten, op dezelfde manier als genoemd bij vraag 2. | Voor het beantwoorden van de laatste ga ik de AVG analyseren en gebruik maken van onderstaande literatuur:  Boeken   * Grip op de AVG, de nieuwe privacywet * De Algemene Verordening Gegevensbescherming, artikelsgewijs commentaar * Checklist Privacy – privacybeleid in 46 checklists   Handleidingen en richtlijnen   * Richtsnoeren voor gegevensbeschermingseffectbeoordelingen * Handleiding AVG van de Rijksoverheid * AVG-check van de Metaalunie |

# Juridisch kader

3.1. Algemene Verordening Gegevensbescherming (AVG)De AVG is van toepassing in de gehele EU en strekt zich tot het beschermen van natuurlijke personen bij de verwerking van persoonsgegevens (Art. 1 lid 1 en art. 3 lid 1 AVG). Op grond van art. 8 lid 1 van het Handvest van de grondrechten van de Europese Unie en art. 16 lid 1 van het Verdrag betreffende de werking van de Europese Unie (VWEU) heeft eenieder recht op bescherming van zijn persoonsgegevens.[[11]](#footnote-11)

### Begrippen AVG

In de AVG staan een aantal begrippen centraal die in dit onderzoek ook veelvuldig gebruikt zullen worden:

* Verwerking (art. 4 onder 2 AVG)

Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, 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.

* Verwerker (art. 4 onder 8 AVG)

Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

* Verwerkingsverantwoordelijke (art. 4 onder 7 AVG)

Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Uiteraard is “persoonsgegeven” ook een belangrijk begrip, dit begrip zal later in dit onderzoek uitgebreider aan bod komen.

### Grondslagen voor verwerking

Nieuw in de AVG zijn de zes wettelijke grondslagen. Het verwerken van “gewone” persoonsgegevens is alleen rechtmatig indien dit gebaseerd is op één van deze grondslagen. Het verwerken van bijzondere en strafrechtelijke persoonsgegevens is verboden. Tenzij verwerker zich kan beroepen op een specifieke wettelijke uitzondering *en* op één van de zes grondslagen voor het verwerken van “gewone” persoonsgegevens.[[12]](#footnote-12) De zes wettelijke grondslagen zijn terug te vinden in art. 6 lid 1 AVG:

1. De betrokkene heeft **toestemming** gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
2. De verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
3. De verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting** die op de verwerkingsverantwoordelijke rust;
4. De verwerking is noodzakelijk om de **vitale belangen** van de betrokkene of van een andere natuurlijke persoon te beschermen;
5. Verwerking is noodzakelijk voor de vervulling van een **taak van algemeen belang** of van een taak in het kader van de **uitoefening van het openbaar gezag** dat aan de verwerkingsverantwoordelijke is opgedragen;
6. De verwerking is noodzakelijk voor de **behartiging van de gerechtvaardigde belangen** van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

*Toestemming van de betrokkene*Art. 4 onder 11 AVG geeft toelichting op wat er wordt verstaan onder “toestemming”:  
*“Onder toestemming van de betrokkene wordt in de AVG verstaan: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt”.*

Daarnaast worden er een aantal eisen gesteld aan de manier waarop er toestemming wordt gevraagd aan betrokkene:

* Betrokkene moet op een duidelijke manier geïnformeerd worden over waarom zijn toestemming gevraagd wordt;
* Betrokkene moet geïnformeerd worden over de mogelijkheid om te allen tijde zijn toestemming weer in te kunnen trekken. Het intrekken van toestemming moet net zo eenvoudig zijn als het geven van toestemming;
* De toestemming mag niet vaag of algemeen van aard zijn. De toestemming dient gevraagd te worden voor één specifiek doel;
* Betrokkene moet vrij zijn om geen toestemming te verlenen. De hiërarchie tussen betrokkene en verwerkingsverantwoordelijke is hier van belang. Bij relaties als overheid-burger en werknemer-werkgever, zullen de burger en werknemer minder vrij zijn om geen toestemming te verlenen;
* Toestemming is niet geldig als dit als voorwaarde gesteld wordt voor het aangaan van een overeenkomst met de betrokkene als de gegevensverwerking hiervoor niet nodig is;
* De toestemming moet door een duidelijke actieve handeling gegeven worden. Bijvoorbeeld bij stilzwijgen en vooraf aangevinkte vakjes, is dit dus niet het geval. De handeling hoeft niet uitdrukkelijk gericht te zijn op het geven van toestemming, wel moet uit de handeling duidelijk blijken dat betrokkene toestemming geeft. Bijvoorbeeld: betrokkene is een bezoeker van een bedrijfsbeurs en geeft zijn visitekaartje af om eventueel samen zaken te doen.[[13]](#footnote-13)

*Uitvoering van een overeenkomst*Het verwerken van persoonsgegevens baseren op deze grondslag mag alleen als er sprake is van een rechtsgeldige overeenkomst op grond van het burgerlijk recht, waarbij het verwerken van persoonsgegevens noodzakelijk is. De overeenkomst zelf mag niet gericht zijn op het verwerken van persoonsgegevens, maar moet een ander doel hebben.[[14]](#footnote-14) Ook een verwerking die nodig is voor het voorbereiden van een overeenkomst, valt onder deze grondslag, maar alleen als de betrokkene zelf om de verwerking gevraagd heeft.[[15]](#footnote-15)

*Wettelijke verplichting*Overweging 45 AVG stelt dat de verwerking een grondslag dient te hebben in het Unierecht of het lidstatelijke recht. Het hoeft niet letterlijk in de wet te staan dat het verwerken van persoonsgegevens nodig is voor de uitvoering van een specifieke taak. Het kan gaan om een concrete wettelijke verplichting om persoonsgegevens te verwerken, maar ook een algemene wettelijke verplichting biedt voldoende basis om zich te beroepen op deze grondslag.[[16]](#footnote-16)

*Vitale belangen*Er is sprake van een vitaal belang als het belang essentieel is voor iemands leven of gezondheid en betrokkene niet om toestemming gevraagd kan worden. Bijvoorbeeld bij grootschalige rampen of wanneer de betrokkene bewusteloos is of mentaal niet in staat om toestemming te geven.[[17]](#footnote-17) Omdat het bij dit soort gevallen vaak om bijzondere persoonsgegevens zal gaan (bijv. medische gegevens), is dit een zeer beperkte grondslag die alleen gebruikt kan worden als het voor betrokkene fysiek of juridisch onmogelijk is om toestemming te verlenen.[[18]](#footnote-18)

*Algemeen belang/openbaar gezag*Het gaat hier om taken die in de wet zijn vastgelegd. Ook hier geldt op grond van overweging 45 AVG weer dat de verwerking grondslag dient te hebben in het Unierecht of het lidstatelijke recht. Deze grondslag is met name van toepassing voor de overheid maar ook voor bijvoorbeeld netbeheerders, De Nederlandsche Bank en APK-keuringsstations.[[19]](#footnote-19)

*Gerechtvaardigde belangen*Deze grondslag kan alleen gebruikt worden als de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder wegen, rekening houdend met de redelijke verwachtingen van de betrokkene op basis van zijn verhouding met de verwerkingsverantwoordelijke.[[20]](#footnote-20) Ook het verwerken van persoonsgegevens ten behoeve van direct marketing, valt onder deze grondslag (overweging 47 AVG).

Betrokkene heeft bij deze grondslag ten alle tijden recht om bezwaar te maken tegen de verwerking (art. 21 lid 1 AVG). Indien de betrokkene gebruik maakt van dit recht, moet de verwerkingsverantwoordelijke direct stoppen met de verwerking van zijn/haar persoonsgegevens, tenzij de verwerkingsverantwoordelijke met dwingende gerechtvaardigde gronden komt die zwaarder wegen dan het bezwaar van betrokkene. Indien deze grondslag gebruikt wordt ten behoeve van direct marketing of profilering, is het bezwaar van betrokkene altijd gegrond (art. 21 lid 3 AVG). [[21]](#footnote-21)

Ook bij doorgifte aan zuster- en/of dochtermaatschappijen kan er sprake zijn van een gerechtvaardigd belang wegens administratieve doeleinden.

### Verantwoordingsplicht

Met de komst van de AVG krijgen organisaties te maken met een grotere verantwoordelijkheid bij het verwerken van persoonsgegevens, de verantwoordingsplicht. Deze is terug te vinden in art. 5 lid 2 AVG. Art. 24 lid 1 AVG gaat verder in op de verantwoordingsplicht van organisaties. Organisaties moeten niet alleen voldoen aan de beginselen inzake persoonsgegevens, maar ook aan kunnen tonen dat zij hier aan voldoen. Daarnaast dienen organisaties de juiste technische en organisatorische maatregelen te nemen voor de bescherming van persoonsgegevens, “privacy by design” en “privacy by default”.[[22]](#footnote-22)

Beginselen inzake persoonsgegevensDe AVG kent verschillende beginselen van gegevensbescherming, welke terug te vinden zijn in art. 5 lid 1 AVG. Bij elke verwerking van persoonsgegevens dienen de volgende beginselen in acht te worden genomen:

|  |  |
| --- | --- |
| 1. *Rechtmatigheid, behoorlijkheid en transparantie* | *De verwerking van persoonsgegevens moet netjes en verantwoord gebeuren en de verwerking moet gebaseerd zijn op 1 van de 6 grondslagen van de AVG. Daarnaast moet het doel en de manier van verwerken duidelijk zijn.* |
| 1. *Doelbinding* | *Verzamelen en verwerken van persoonsgegevens mag alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen.* |
| 1. *Minimale gegevensverwerking* | *De persoonsgegevens die verwerkt worden, moeten toereikend en noodzakelijk zijn voor het doel.* |
| 1. *Juistheid* | *De verwerkingsverantwoordelijke moet alle redelijke maatregelen nemen om ervoor te zorgen dat de gegevens correct en actueel zijn. Onjuiste of onvolledige gegevens dienen gewist, gecorrigeerd of aangevuld te worden.* |
| 1. *Opslagbeperking* | *Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk voor het doel van de verwerking. Persoonsgegevens die niet meer noodzakelijk zijn, moeten vernietigd of gewist worden.* |
| 1. *Integriteit en vertrouwelijkheid* | *Persoonsgegevens moeten worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.* [[23]](#footnote-23) |

Zoals eerder al aangegeven is, moet de verwerkingsverantwoordelijke niet alleen voldoen aan de beginselen inzake persoonsgegevens, maar moet zij dit ook aan kunnen tonen. Om aan te kunnen tonen dat voldaan wordt aan de beginselen, dient de verwerkingsverantwoordelijke in ieder geval de volgende maatregelen te nemen:

* Een register van verwerkingsactiviteiten bijhouden (verwerkingsregister);
* Afhankelijk van de mate van verwerkingsactiviteiten, een geschreven passend gegevensbeschermingsbeleid;
* In bepaalde gevallen een functionaris voor gegevensbescherming (FG) aanstellen\*;
* In sommige gevallen het documenteren van gegevensbeschermingseffectbeoordelingen (in de praktijk Data Protection Impact Assessment (DPIA) genoemd);
* Documenteren van de gehanteerde passende waarborgen bij overdracht van gegevens buiten de EU\*\*;
* Betrokkene informeren over de bescherming van zijn gegevens (privacyverklaring);
* Voor de grondslag “toestemming”, vastleggen hoe er toestemming wordt gevraagd;
* Voor de grondslag “gerechtvaardigd belang”, dit gerechtvaardigde belang documenteren;
* Verwerkersovereenkomsten opstellen volgens de regels van de AVG;
* Datalek procedure opstellen;
* Alle datalekken bijhouden (datalek register);
* Bij het inrichten van verwerkingen rekening houden met het principe van privacy by design en privacy by default.[[24]](#footnote-24)

\* Een FG is op grond van art. 37 lid 1 AVG alleen verplicht als:

* De gegevens worden verwerkt door een overheidsinstelling of -orgaan;
* De organisatie belast is met verwerkingen die betrekking hebben op regelmatige of stelselmatige observatie op grote schaal van betrokkenen; of
* De organisatie belast is met grootschalige verwerkingen van bijzondere persoonsgegevens.[[25]](#footnote-25)

Omdat geen van bovenstaande punten van toepassing is op Opdrachtgever, wordt de FG verder niet behandeld in dit onderzoek.

\*\* Het documenteren van passende waarborgen bij overdracht van gegevens buiten de EU is voor Opdrachtgever niet van toepassing, daar zij geen persoonsgegevens verwerkt buiten de EU.

#### Verwerkingsregister

Het opstellen van een (schriftelijk/elektronisch) verwerkingsregister is niet verplicht als de organisatie minder dan 250 werknemers heeft, tenzij de verwerking niet incidenteel is, en/of het een verwerking van bijzondere of strafrechtelijke persoonsgegevens betreft en/of de verwerking risicovol is. Daar het verwerken van persoonsgegevens door een organisatie bijna nooit incidenteel is, is het opstellen van een verwerkingsregister bijna altijd verplicht.[[26]](#footnote-26)

In het verwerkingsregister moeten in ieder geval de volgende zaken staan:

|  |  |
| --- | --- |
| Naam en contactgegevens van de verwerkingsverantwoordelijke(n). | Art. 30 lid 1 sub a AVG |
| De doelen/het doel van elke verwerking. | Art. 30 lid 1 sub b AVG |
| Een beschrijving van de categorieën betrokkenen waarvan persoonsgegevens verwerkt worden en categorieën van soort persoonsgegevens. | Art. 30 lid 1 sub c AVG |
| Een lijst van derden partijen aan wie de persoonsgegevens verstrekt zijn of verstrekt zullen worden. | Art. 30 lid 1 sub d AVG |
| Indien van toepassing, lijst van derde landen of internationale organisaties aan wie de persoonsgegevens doorgegeven worden.[[27]](#footnote-27) | Art. 30 lid 1 sub e AVG |
| Bewaartermijnen van de categorieën van persoonsgegevens | Art. 30 lid 1 sub f AVG |
| Indien mogelijk, een beschrijving van de technische en organisatorische beveiligingsmaatregelen. | Art. 30 lid 1 sub g AVG |

#### Gegevensbeschermingseffectbeoordeling/DPIA

De gegevensbeschermingseffectbeoordeling (verder DPIA) is terug te vinden in art. 35 AVG. Een DPIA is een instrument om te beoordelen wat de effecten zijn van een voorgenomen verwerkingsactiviteit op de bescherming van persoonsgegevens en de rechten en vrijheden van betrokkenen. Op basis van deze beoordeling, dienen er maatregelen genomen te worden om de effecten voor betrokkenen te voorkomen of te verkleinen. Daarnaast kan de verwerkingsverantwoordelijke hiermee aantonen dat zij voldoet aan de verantwoordingsplicht van de AVG. [[28]](#footnote-28)

Een DPIA dient voorafgaand aan de betreffende gegevensverwerking uitgevoerd te worden als de verwerking waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van de betrokkenen.[[29]](#footnote-29) Het niet, of niet juist, uitvoeren van een DPIA of het niet raadplegen van de Autoriteit Persoonsgegevens terwijl dit wel verplicht is, kan leiden tot een administratieve boete van maximaal 10 miljoen Euro of, in het geval van een onderneming, maximaal 2% van de totale wereldwijde jaaromzet van het voorgaande boekjaar, waarbij het hoogste bedrag van toepassing is.[[30]](#footnote-30)

*Wel of niet verplicht?*  
Om te bepalen of een DPIA wel of niet verplicht is, is het van belang om te weten wat er in art. 35 AVG bedoeld wordt met “hoog risico voor de rechten en vrijheden van betrokkenen”. Hoewel “rechten en vrijheden” voornamelijk betrekking heeft op de bescherming van persoonsgegevens en het recht op privacy, wordt er hier ook gedoeld op andere grondrechten.[[31]](#footnote-31)

In art. 35 lid 3 AVG wordt genoemd wanneer er in ieder geval sprake is van een hoog risico. Als er sprake is van:

* Een systematische en uitgebreide beoordeling van persoonlijke aspecten van betrokkenen, die gebaseerd is op geautomatiseerde verwerking (waaronder profilering) en waarop besluiten worden gebaseerd waaraan voor betrokkenen rechtsgevolgen zijn verbonden of die betrokkenen op vergelijkbare wijze wezenlijk treffen;
* Grootschalige verwerking van bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard;
* Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Als toevoeging op bovenstaande lijst, hebben Europese toezichthouders onderstaande criteria opgesteld om te bepalen of er waarschijnlijk sprake is van een hoog risico. Wanneer de voorgenomen verwerking aan twee of meer van de volgende criteria voldoet, is er sprake van een hoog risico:

* Evaluatie van personen of scoretoekenning;
* Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg;
* Stelselmatige monitoring;
* Gevoelige gegevens of gegevens van zeer persoonlijke aard;
* Op grote schaal verwerkte gegevens;
* Matching of samenvoeging van datasets;
* Gegevens met betrekking tot kwetsbare betrokkenen;
* Innovatieve toepassing van nieuwe technologische of organisatorische oplossing;
* Blokkering van een recht, dienst of contract.[[32]](#footnote-32)

Het uitvoeren van een DPIA is **niet** verplicht als de verwerking:

* Waarschijnlijk geen hoog risico oplevert;
* Sterk lijkt op een andere gegevensverwerking waarvoor al een DPIA is uitgevoerd;
* Wordt geregeld door een andere Europese of nationale wet en er bij de totstandkoming van deze wet al een DPIA is uitgevoerd. Tenzij de AP oordeelt dat er toch een DPIA nodig is.
* Op een lijst staat van verwerkingen waarvoor een DPIA niet verplicht is.[[33]](#footnote-33)

Daarnaast geldt dat het uitvoeren van een DPIA in principe niet verplicht is voor bestaande verwerkingen, tenzij er sprake is van één van onderstaande situaties:

* De bestaande, reeds door de AP of FG gecontroleerde gegevensverwerking is gewijzigd op (een van) onderstaande punten:
  + Het bereik;
  + Het doel;
  + De verwerkte persoonsgegevens;
  + De identiteit van de verwerkingsverantwoordelijke of ontvangers;
  + Bewaartermijnen
  + Technische en organisatorische maatregelen;
  + Risico’s.[[34]](#footnote-34)

*Gegevensbeschermingseffectbeoordeling/DPIA vs. verantwoordingsplicht*Om te voldoen aan de verantwoordingsplicht, is het van belang om goed te kunnen onderbouwen waarom er voor gekozen is om geen DPIA uit te voeren wanneer de verwerking aan slechts één van de criteria voldoet.[[35]](#footnote-35) Daarnaast moet de verwerkingsverantwoordelijke ondanks dat de DPIA niet verplicht is, wel voldoen aan haar verantwoordingsplicht. Het is voor verwerkingsverantwoordelijken daarom raadzaam om voor elke nieuwe soort verwerking vast te stellen of deze waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.[[36]](#footnote-36)

*Het uitvoeren van een DPIA*In art. 35 lid 7 AVG is terug te vinden welke punten in ieder geval aan bod dienen te komen bij het uitvoeren van een DPIA:

* Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden. Als de grondslag “gerechtvaardigd belang” wordt gebruikt, moet ook dit belang worden gesteld en gemotiveerd;
* Een beoordeling van de noodzakelijkheid en evenredigheid met betrekking tot het doel van de verwerking;
* Een uitwerking van mogelijke risico’s en wanneer deze een verhoogde kans hebben om op te treden;
* De beoogde maatregelen die genomen zullen worden om de gesignaleerde risico’s te beperken. De maatregelen dienen de bescherming van persoonsgegevens te garanderen en de rechten en plichten van betrokkenen te respecteren. [[37]](#footnote-37)

#### Informatieplicht/Privacyverklaring

Betrokkenen dienen geïnformeerd te worden over de manier waarop de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Ook dienen zij gewezen te worden op hun rechten.[[38]](#footnote-38)

Het informeren van betrokkenen dient op een transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal te gebeuren. Dit mag zowel schriftelijk als elektronisch gebeuren, indien dit passend is. Ook het mondeling informeren van betrokkenen is toegestaan, mits betrokkenen dit zelf verzoeken en de identiteit van de betrokkenen bewezen is (art. 12 lid 1 AVG).

Om te voldoen aan deze informatieplicht stellen veel organisaties een privacyverklaring op die op de website wordt geplaatst. In deze privacyverklaring worden alle privacyaspecten van een dienst, of de gehele dienstverlening besproken. [[39]](#footnote-39) Ook voor Opdrachtgever heb ik ervoor gekozen om te voldoen aan de informatieplicht door middel van het plaatsen van een privacyverklaring op de website omdat deze manier van informeren het makkelijkst in te breien is in de werkprocessen.

*Inhoud van de informatieplicht/privacyverklaring*Art. 13 AVG noemt de informatie die in ieder geval aan betrokkenen verstrekt dient te worden, in het geval de gegevens verzamelt worden bij betrokkene zelf:

* Identiteit en contactgegevens van de verwerkingsverantwoordelijke, indien van toepassing, van de vertegenwoordiger van de verwerkingsverantwoordelijke;
* Indien van toepassing, de contactgegevens van de FG;
* Het doel en de rechtsgrond van de verwerking;
* Indien er sprake is van de grondslag “gerechtvaardigde belangen”, de belangen van de verwerkingsverantwoordelijke;
* Indien van toepassing, de ontvangers of categorieën van ontvangers van de persoonsgegevens;
* In geval van doorgifte aan derde landen;
  + Of er een adequaatheidsbesluit van de Commissie is;
  + Passende waarborgen noemen en aangeven of hier een kopie van verstrekt kan worden of inzage mogelijk is;
* Bewaartermijnen van de persoonsgegevens;
* Het recht van betrokkenen om te verzoeken om inzage, rectificatie of het wissen van de persoonsgegevens of het recht van betrokkenen om te verzoeken om beperking van de verwerking;
* Het recht van betrokkenen om bezwaar te maken tegen de verwerking en het recht op gegevensoverdraagbaarheid;
* Het recht van betrokkenen om de gegeven toestemming voor verwerking bij de grondslag “toestemming” altijd weer in te trekken;
* Het recht van betrokkenen om een klacht in te dienen bij de AP over een verwerking;
* Of de betrokkenen verplicht zijn om gegevens te verstrekken en wat de gevolgen zijn van het niet verstrekken in geval de verwerking voortvloeit uit een wettelijke plicht of noodzakelijk is voor de uitvoering van een overeenkomst;
* In geval van geautomatiseerde besluitvorming, informatie over de onderliggende logica, het belang van de verwerking en de verwachte gevolgen die de verwerking voor betrokkenen heeft.[[40]](#footnote-40)

Naast bovenstaande punten die in ieder geval onder de informatieplicht vallen, dient de verwerkingsverantwoordelijke zelf te bepalen of er meer informatie verstrekt dient te worden om een behoorlijke en transparante verwerking te waarborgen.[[41]](#footnote-41)

*Verstrekken van de informatie*De AVG maakt onderscheid tussen:

|  |  |
| --- | --- |
| 1. **Het verstrekken van informatie indien de persoonsgegevens direct bij de betrokkenen worden verzameld (art. 13 AVG)** | 1. **Het verstrekken van informatie indien de persoonsgegevens niet direct van de betrokkenen zijn verkregen (art. 14 AVG)** |
| * Informatie moet worden verstrekt op het moment van verkrijging van de persoonsgegevens.[[42]](#footnote-42) | * Betrokkenen moeten geïnformeerd worden binnen een redelijke termijn na verkrijging van de gegevens. Dit is in ieder geval niet langer dan één maand na ontvangst.[[43]](#footnote-43) |
| * Als de verwerkingsverantwoordelijke denkt dat betrokkenen de informatie al hebben ontvangen, is er al voldaan aan de informatieplicht. Verwerkingsverantwoordelijke mag er vanuit gaan dat dit het geval is als naar objectieve maatstaven, uit een gedraging of verklaring van betrokkenen afgeleid kan worden dat deze reeds geïnformeerd zijn.[[44]](#footnote-44) | * Verwerkingsverantwoordelijke hoeft betrokkenen niet te informeren als verkrijging of verstrekking van de persoonsgegevens uitdrukkelijk bij wet is voorgeschreven en de gerechtvaardigde belangen van betrokkenen in die wet zijn gewaarborgd.[[45]](#footnote-45) |
|  | * Verwerkingsverantwoordelijke hoeft betrokkenen niet te informeren indien dit onmogelijk is of een onredelijke inspanning vereist.[[46]](#footnote-46) |
|  | * Verwerkingsverantwoordelijke hoeft betrokkenen niet te informeren als deze reeds geïnformeerd is, bijvoorbeeld door de oorspronkelijke verantwoordelijke.[[47]](#footnote-47) |
|  | * Verwerkingsverantwoordelijke hoeft betrokkenen niet te informeren indien de persoonsgegevens vertrouwelijk moeten blijven in verband met een beroepsgeheim. |
|  |  |

Privacy by design & privacy by default  
Op grond van art. 25 AVG moeten er passende technische en organisatorische maatregelen genomen worden gedurende het gehele proces van het verwerken van persoonsgegevens.[[48]](#footnote-48) In het Nederlands wordt dit “privacy door ontwerp en door standaardinstellingen” genoemd. Omdat in de praktijk vaak de Engelse benamingen gebruikt worden, zullen deze ook aangehouden worden in dit onderzoek.

Privacy by design en privacy by default houdt in dat er bij ontwikkeling van nieuw beleid of ontwerp/gebruik van nieuwe systemen vanaf stap 1 al rekening gehouden moet worden met privacy en de bescherming van persoonsgegevens.[[49]](#footnote-49)

De toepassing van privacy by design zorgt er voor dat het ontwerp van beleid en/of systemen een goed beschermingsniveau waarborgt en geeft de mogelijkheid om automatisch de meest privacy-vriendelijke instellingen aan te houden (privacy by default). Het toepassen is verplicht voor alle nieuwe verwerkingen. Voor bestaande verwerkingen geldt dat deze tijdens de evaluatie of vervanging van bestaande systemen ook moeten voldoen aan privacy by design en default.[[50]](#footnote-50)

De genomen maatregelen dienen in ieder geval afgestemd te zijn op:

* Stand van de techniek betreffende de te nemen maatregel;
* Uitvoeringskosten;
* Aard van de verwerking;
* Context van de verwerking;
* Eventuele risico’s voor de rechten en vrijheden van natuurlijke personen.

Daarnaast dienen de genomen maatregelen in lijn te zijn met de beginselen uit de AVG.[[51]](#footnote-51)

### Verwerkersovereenkomst

Art. 28 lid 3 AVG stelt het sluiten van een verwerkersovereenkomst verplicht als een andere partij (verwerker) gegevens verwerkt voor de verwerkingsverantwoordelijke. De verwerker moet voldoende garanties bieden wat betreft deskundigheid en betrouwbaarheid. Daarnaast moet de verwerker ervoor zorgen dat de technische en organisatorische maatregelen voldoen aan de voorschriften uit de AVG.[[52]](#footnote-52) Ook kunnen er bepalingen opgenomen worden in de verwerkersovereenkomst met betrekking tot de aansprakelijkheid van beide partijen.[[53]](#footnote-53)

De verwerkersovereenkomst hoeft, anders dan de naam doet vermoeden, geen apart document te zijn. De afspraken die vastgelegd dienen te worden in een verwerkersovereenkomst, mogen ook als onderdeel toegevoegd worden aan een andere overeenkomst.[[54]](#footnote-54)

#### Verwerker, verwerkingsverantwoordelijke of medeverantwoordelijke?

Om te weten of een verwerkersovereenkomst noodzakelijk is, is het van belang om te weten of u verwerker, verwerkingsverantwoordelijke of medeverantwoordelijke bent.[[55]](#footnote-55)

*Verwerkingsverantwoordelijke*  
Kort gezegd kan er gesteld worden dat er sprake is van een verwerkingsverantwoordelijke, indien deze bepaalt welke persoonsgegevens er verzameld worden, voor welk doel deze verzameld worden en hoe deze verzameld worden, dit is ook terug te zien in het schema in bijlage 1.

Een ander hulpmiddel bij het bepalen of een organisatie verwerkingsverantwoordelijke is, is nagaan of er sprake is van 1 van de 3 onderstaande categorieën:

1. Uitdrukkelijke juridische bevoegdheid

De bevoegdheid, taak of plicht om persoonsgegevens te verwerken is expliciet aan de organisatie opgedragen in de wet.

1. Impliciete bevoegdheid

Er is geen expliciete bevoegdheid, taak of plicht op grond van de wet, maar wel op grond van de gangbare juridische regels en de maatstaven die gelden in het maatschappelijk verkeer.

1. Feitelijke invloed

Hierbij wordt er gekeken of partijen feitelijke invloed uit kunnen oefenen op de verwerking van persoonsgegevens en wordt er gekeken naar de juridische verhouding tussen partijen. Het gaat erom wie daadwerkelijk de beslissingen neemt en daarmee feitelijk bepaalt wat er met de persoonsgegevens gebeurt.[[56]](#footnote-56)

*Verwerker*De organisatie die   
1) ten behoeve van een verwerkingsverantwoordelijke persoonsgegevens verwerkt,   
2) zonder aan het rechtstreekse gezag van de verwerkingsverantwoordelijke onderworpen te zijn,   
is verwerker.

1. Het primaire doel van de dienstverlening, moet gericht zijn op het verwerken van persoonsgegevens ten behoeve van een verwerkingsverantwoordelijke. Als dit niet het geval is en de verwerking van persoonsgegevens slechts een uitvloeisel is van een andere soort dienstverlening, is de organisatie zelf verwerkingsverantwoordelijke en geen verwerker.
2. De verwerker is een organisatie die buiten de verwerkingsverantwoordelijke staat. Als er sprake is van een hiërarchische relatie met de verwerkingsverantwoordelijke, is er dus geen sprake van een verwerker. Dit kenmerkt zich door het feit dat de verwerker geen zeggenschap heeft over het doel en de middelen van de verwerking.[[57]](#footnote-57)

*Medeverantwoordelijke*Naast de verwerker en verwerkingsverantwoordelijke, kan er ook sprake zijn van een medeverantwoordelijke. Wanneer de verwerkingsverantwoordelijk samen met een andere organisatie het doel en de middelen bepaalt voor de verwerking, is er sprake van medeverantwoordelijkheid.

De medeverantwoordelijken hoeven geen verwerkersovereenkomst met elkaar af te sluiten, wel dienen er onderling afspraken gemaakt te worden. De afspraken dienen gericht te zijn op wie op welke manier invulling geeft aan de verplichtingen uit de AVG. Het doel van deze afspraken is dat betrokkenen weten waar zij terecht kunnen om hun rechten uit te oefenen.[[58]](#footnote-58)

#### Inhoud van de verwerkersovereenkomst

Zodra duidelijk is dat er sprake is van een verwerker, dient er een verwerkersovereenkomst afgesloten te worden tussen de verwerkingsverantwoordelijke en de verwerker. In de verwerkersovereenkomst dienen in ieder geval onderstaande zaken aan de orde te komen:

* Het onderwerp en de duur van de verwerking
* De aard en de doeleinden van de verwerking
* Het soort persoonsgegevens en categorieën van betrokkenen
* Taken en verantwoordelijkheden van de verwerker[[59]](#footnote-59)

Daarnaast dient de verwerkersovereenkomst te bepalen dat de verwerker:

* Persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke (art. 28 lid 3 sub a AVG);
* Waarborgt dat de toegang tot de persoonsgegevens beperkt is tot gemachtigde personen die gebonden zijn aan geheimhouding op grond van een overeenkomst of wettelijke verplichting (Art. 28 lid 3 sub b AVG);
* Aan dezelfde beveiligingseisen voldoet als waaraan de verwerkingsverantwoordelijke moet voldoen (Art. 28 lid 3 sub c jo art. 32 AVG);
* Voldoet aan de eisen die er gesteld worden bij het in dienst nemen van een andere verwerker (Art. 28 lid 3 sub d jo lid 2 en 4 AVG);
* De verwerkingsverantwoordelijke zoveel mogelijk ondersteunt bij het vervullen van diens verplichtingen om te voldoen aan verzoeken van betrokkenen (Art. 28 lid 3 sub e AVG);
* De verwerkingsverantwoordelijke zoveel mogelijk ondersteunt bij de beveiliging van de gegevens en de meldplicht datalekken (Art. 28 lid 3 sub f jo art. 32 t/m 36 AVG);
* Na afloop van de overeenkomst alle persoonsgegevens wist of teruggeeft aan de verwerkingsverantwoordelijke en bestaande kopieën verwijdert. Tenzij opslag verplicht is (Art. 28 lid 3 sub g AVG);
* Alle informatie ter beschikking stelt om aan te tonen dat er voldaan is aan de eisen die de AVG stelt aan het inzetten van een verwerker (Art. 28 lid 3 sub h AVG).

### **Datalekken**

Sinds 1 januari 2016 is er op grond van de Wet bescherming persoonsgegevens (Wbp) een meldplicht voor datalekken.[[60]](#footnote-60) Onder de AVG blijft de meldplicht datalekken van kracht, echter wel met strengere eisen met betrekking tot de documentatie en registratie van datalekken. aangevuld met de “meldplicht datalekken”. Onder de AVG komt deze meldplicht, met enkele wijzigingen, terug.

Art. 33 lid 1 jo Art. 4 onder 12 AVG stelt dat er sprake is van een datalek (in de AVG wordt dit “inbreuk in verband met persoonsgegevens” genoemd) als een inbreuk op de beveiliging per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.[[61]](#footnote-61)

#### Datalekregister

Alle datalekken dienen gedocumenteerd te worden in een datalekregister (art. 5 lid 2 en 33 lid 5 AVG). In dit register dienen in ieder geval alle feiten en gevolgen omtrent het datalek geregistreerd te worden.[[62]](#footnote-62) Daarnaast wordt het aangeraden om ook te documenteren welke maatregelen er zijn genomen om de schade te beperken en herhaling te voorkomen. Verder is het aan de verwerkingsverantwoordelijke om te bepalen op welke manier zij invulling geeft aan het datalekregister.[[63]](#footnote-63)

#### Datalek melden

Indien het onwaarschijnlijk is dat een datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, hoeft de inbreuk niet gemeld te worden, alle andere datalekken dienen wel gemeld te worden bij de AP. Het melden van een datalek, dient binnen 72 uur nadat de verwerkingsverantwoordelijke er kennis van heeft genomen te gebeuren. Er wordt hierbij uitgegaan van het moment waarop de verwerkingsverantwoordelijke redelijkerwijs op de hoogte zou moeten zijn.[[64]](#footnote-64)

Of het waarschijnlijk is dat een datalek een (hoog) risico inhoudt, dient de verwerkingsverantwoordelijke zelf te boordelen aan de hand van de volgende factoren:

* De aard, gevoeligheid en hoeveelheid van de gelekte gegevens;
* De moeilijkheidsgraad van identificatie van betrokkenen;;
* De omvang van het datalek;
* De impact op de betrokkene(n);
* Specifieke eigenschappen van de organisatie van de verwerkingsverantwoordelijke (mate van verwerking van persoonsgegevens in de organisatie);
* Overige relevante eigenschappen.[[65]](#footnote-65)

## Verwerking van persoonsgegevens door Opdrachtgever

Voor ik verder in ga op hoe, en welke persoonsgegevens Opdrachtgever verwerkt, is het van belang om een toelichting te geven op het begrip “persoonsgegeven”.

In art. 4 onder 1 van de AVG staat het begrip als volgt uitgelegd: “een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd”.

Er wordt onderscheid gemaakt tussen algemene persoonsgegevens en bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn persoonsgegevens die door hun aard bijzonder gevoelig zijn. Hieronder vallen de volgende gegevens:

* Persoonsgegevens waaruit ras of etnische afkomst blijkt;
* Persoonsgegevens waaruit politieke opvattingen blijken;
* Persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken;
* Persoonsgegevens waaruit het lidmaatschap van een vakvereniging blijkt;
* Gegevens over gezondheid;
* Gegevens met betrekking tot iemands seksueel gedrag of seksuele geaardheid;
* Genetische gegevens;
* Biometrische gegevens met het oog op de unieke identificatie van een persoon.[[66]](#footnote-66)

### Welke persoonsgegevens verzameld Opdrachtgever?

Voorafgaand aan het onderzoek heeft Opdrachtgever al een inventarisatie gedaan van de persoonsgegevens die zij verwerkt. Deze persoonsgegevens hebben ze in twee afdelingen gecategoriseerd: klant- en leveranciersadministratie en personeels- en loonadministratie.

|  |  |
| --- | --- |
| Klant- en leveranciersadministratie | Personeels- en loonadministratie |
| * Bedrijfsnaam | * Naam |
| * Naam contactpersoon | * Adres |
| * Geslacht van de contactpersoon | * Telefoonnummer |
| * Eventuele titels van de contactpersoon | * Geboortedatum |
| * Functie van de contactpersoon | * E-mailadres |
| * Telefoonnummer | * IBAN nummer en BIC bankcode |
| * E-mailadres | * BSN nummer |
| * Bron van de ontmoeting | * Datum in dienst |
| * Verslagen van korte gesprekken/afspraken met de klant | * Burgerlijke staat |
|  | * Gegevens contactpersoon bij ongeval – naam, adres en telefoonnummer |

Om na te gaan of bovenstaande persoonsgegevens inderdaad de enige gegevens zijn die door Opdrachtgever verwerkt worden, heb ik medewerkers en managers van de afdelingen inkoop/verkoop, kwaliteit, financiële administratie, productie en personeelszaken geïnterviewd. Uit deze interviews is gebleken (bijlage 8[[67]](#footnote-67) en Medewerker Personeelszaken, persoonlijke communicatie, 22 mei 2018)[[68]](#footnote-68) dat er niet meer persoonsgegevens verzameld worden dan uit de eigen inventarisatie van Opdrachtgever gebleken is.

### Hoe worden de persoonsgegevens verwerkt?

Binnen Opdrachtgever worden er op verschillende afdelingen persoonsgegevens verzameld van verschillende categorieën betrokkenen.[[69]](#footnote-69) Ik zal in dit onderzoek de twee hoofdcategorieën aanhouden die reeds door Opdrachtgever gebruikt zijn bij de inventarisatie omdat dit op grond van de interviews ook de hoofdcategorieën blijken te zijn: persoonsgegevens van klanten en leveranciers en persoonsgegevens van medewerkers[[70]](#footnote-70).

#### Persoonsgegevens van klanten en leveranciers

Uit het interview met de medewerker en manager inkoop/verkoop (bijlage 8, interview 1) is gebleken dat de persoonsgegevens van klanten en leveranciers voor 90% verzameld worden op beurzen. Contactpersonen van potentiële klanten/leveranciers verstrekken deze persoonsgegevens zelf door het afgeven van een visitekaartje. Via de contactgegevens op dit visitekaartje wordt er vervolgens op de afdeling Inkoop contact opgenomen met de potentiële klant/leverancier, ook worden er nieuwsbrieven verzonden die betrekking hebben op diensten/producten die voor de potentiële klant/leverancier interessant kunnen zijn. Daarnaast worden de visitekaartjes opgeslagen in een fysieke map zodat het mogelijk is om het contact te onderhouden. Deze map ligt, in een afgesloten kast, op de afdeling en alleen medewerkers die voor het uitvoeren van hun werkzaamheden contact op moeten kunnen nemen met klanten/leveranciers hebben hier toegang toe.

Na het eerste contact (na het ontvangen van het visitekaartje op een beurs), dat via e-mail plaatsvindt, worden de gegevens van de potentiële klant/leverancier opgeslagen in een ERP-systeem en een CRM-systeem (een Excel-bestand), met als doel het eenvoudig kunnen onderhouden van het klantencontact. Zowel het ERP-systeem als het CRM-systeem worden door Opdrachtgever zelf beheerd.

De overige 10% van de persoonsgegevens die Opdrachtgever verwerkt van klanten/leveranciers ontvangt zij zodra deze daadwerkelijk klant zijn geworden. Het gaat dan om de persoonsgegevens[[71]](#footnote-71) van andere contactpersonen binnen het bedrijf, voor zover dit noodzakelijk is voor de uitvoering van de overeenkomst.

Zodra er daadwerkelijk zaken gedaan gaan worden met de klant/leverancier wordt er een offerte opgesteld waarin de persoonsgegevens van de juiste contactpersoon/contactpersonen verwerkt worden. Daarna wordt er een overeenkomst afgesloten. De offertes worden opgeslagen in een digitale map waar alle medewerkers die de offerte nodig hebben ter uitvoering van hun werkzaamheden toegang tot hebben.

Alle bewaartermijnen die uit de wet voortvloeien worden voor de persoonsgegevens van klanten/leveranciers in acht genomen door de afdeling Kwaliteit, zo bleek uit een interview met de medewerker en manager van deze afdeling (bijlage 8, interview 3). Echter wordt er op de afdeling inkoop/verkoop volgens de geïnterviewde medewerker en manager helemaal geen rekening gehouden met bewaartermijnen (bijlage 8, interview 1).

#### Persoonsgegevens van medewerkers

De persoonsgegevens van medewerkers[[72]](#footnote-72), worden verwerkt met als doel de uitvoering van de arbeidsovereenkomst.

De verwerking van persoonsgegevens van medewerkers gebeurt volgens de medewerker personeelszaken (medewerker personeelszaken, persoonlijke communicatie, 22 mei 2018) als volgt.

Het werven van sollicitanten vindt voornamelijk digitaal plaats. Op de website van Opdrachtgever worden openstaande vacatures geplaatst waar geïnteresseerden op kunnen reageren, daarnaast is er de mogelijkheid om een open sollicitatie te versturen via de website. Sollicitaties die via de website binnen komen, komen terecht bij de medewerker personeelszaken. Zij bepaalt zelf, of samen met de manager van de afdeling waarvoor de sollicitant gereageerd heeft, of zij de persoon uitnodigt/uitnodigen voor een kennismakingsgesprek. De gegevens van sollicitanten die wellicht in de toekomst nog iets voor Opdrachtgever kunnen betekenen worden zowel digitaal als fysiek bewaard. Voor het bewaren van deze gegevens worden geen bewaartermijnen aangehouden.

Naast het plaatsen van vacatures op haar eigen website, maakt Opdrachtgever ook gebruik van uitzendbureaus. De medewerker personeelszaken geeft aan de uitzendbureaus door welke vacatures er open staan en welke personen zij daarvoor zoeken. Zodra het uitzendbureau een geschikte kandidaat gevonden heeft, wordt dit doorgegeven aan de medewerker personeelszaken van Opdrachtgever. Dit is ook het moment dat er persoonsgegevens in het spel komen; naam en curriculum vitae worden door het uitzendbureau doorgestuurd naar Opdrachtgever. Vervolgens besluit de medewerker personeelszaken of zij de kandidaat wel of niet uit wil nodigen voor een kennismakingsgesprek.

Als de sollicitant aangenomen wordt, wordt er een arbeidsovereenkomst opgesteld waarvoor de persoonsgegevens zoals genoemd in paragraaf 4.2.1. noodzakelijk zijn. Deze gegevens worden direct door de sollicitant verstrekt (in geval van een uitzendbureau, worden deze door de sollicitant aan het uitzendbureau verstrekt). Voor de fiscale gegevens worden de bewaartermijnen aangehouden die in de fiscale wet- en regelgeving terug te vinden zijn. Deze worden, zoals uit het interview met de manager en medewerker van de financiële administratie blijkt (bijlage 8, interview 2), digitaal opgeslagen in systemen van de salarisadministrateur (ADP) en fysiek opgeslagen in afgesloten kasten. Enkel de medewerkers van de financiële administratie hebben toegang tot deze kast, wel is er een reservesleutel in het bezit van de directie.

Verder wordt de arbeidsovereenkomst, inclusief de persoonsgegevens van de werknemer, opgeslagen in een afgesloten kast, waar alleen de medewerker personeelszaken toegang tot heeft. Ook hier geldt weer dat er geen specifieke bewaartermijnen aangehouden worden.

#### Persoonsgegevens delen met derden

Uit de interviews met de medewerkers van verschillende afdelingen (bijlage 8 en persoonlijke communicatie met de medewerker personeelszaken, 24 mei 2018) is gebleken dat de persoonsgegevens die door Opdrachtgever verwerkt worden, met meerdere partijen gedeeld worden:

|  |  |  |
| --- | --- | --- |
| Bedrijfsnaam | Soort dienst | Gedeelde persoonsgegevens[[73]](#footnote-73) |
| ADP | Salarisadministratie | NAW- gegevens en bankgegevens van medewerkers |
| Naam niet bekend | Leasemaatschappij | NAW-gegevens |
| ISSYS | Ondersteuning computerproblemen | Bij computerproblemen kan ISSYS meekijken en is er een mogelijkheid dat zij kennis kunnen nemen van alle persoonsgegevens die de medewerker op zijn computer opgeslagen heeft, daarnaast leveren zij software. |
| VITASYS | Ondersteuning computerproblemen | Bij computerproblemen kan ISSYS meekijken en is er een mogelijkheid dat zij kennis kunnen nemen van alle persoonsgegevens die de medewerker op zijn computer opgeslagen heeft, daarnaast leveren zij software. |
| Protime | Software voor het bijhouden van kloktijden van medewerkers | Mogelijkheid tot kennis nemen van namen van medewerkers als er zich problemen voordoen met de software |
| Naam niet bekend | ARBO dienst | NAW- gegevens van medewerkers |
| Baken 5 | Ondersteuning verzuimadministratie | NAW- gegevens van medewerkers |
| UWV | Arbeidsrechtelijke zaken | NAW-gegevens en BSN-nummer medewerkers |
| Vanhier B.V. | Accountant | NAW-gegevens,  BSN-nummer en bankgegevens |

Daarnaast is in een gesprek met de medewerker personeelszaken (medewerker personeelszaken, persoonlijke communicatie, 8 mei 2018) gebleken dat er reeds een verwerkersovereenkomst afgesloten is met Baken 5.

Verder is uit verschillende gesprekken, met de manager financiële administratie, medewerker personeelszaken en General Manager, gebleken dat ADP en Protime de verwerkersovereenkomst ingebreid hebben in de Algemene Voorwaarden en/of Service Level Agreement (SLA). Met de overige organisaties, is (nog) geen verwerkersovereenkomst afgesloten.

# Resultaten

## De door Opdrachtgever te nemen maatregelen

Uit de interviews (bijlage 8)[[74]](#footnote-74) en uit persoonlijke communicatie met de medewerker personeelszaken (30 april 2018) is gebleken dat Opdrachtgever geen standaard procedures heeft met betrekking tot de bescherming van persoonsgegevens. Omdat het opstellen van een volledig privacybeleid niet mogelijk bleek in het tijdsbestek van dit onderzoek, is er voor gekozen om enkel te onderzoeken welke maatregelen er minimaal genomen moeten worden om aantoonbaar te voldoen aan de AVG.[[75]](#footnote-75)

Een van de grootste veranderingen die de AVG met zich meebrengt is de grotere verantwoordelijkheid van de verwerkingsverantwoordelijke voor de rechtmatige en zorgvuldige omgang met persoonsgegevens, de verantwoordingsplicht van de verwerkingsverantwoordelijke.[[76]](#footnote-76) Het enkel voldoen aan de verantwoordingsplicht, is niet genoeg, Opdrachtgever dient ook aan te kunnen tonen dat zij voldoet aan haar plicht. Om dit aan te kunnen tonen dient zij de volgende maatregelen te nemen: [[77]](#footnote-77)

1. E**en verwerkingsregister opstellen en bijhouden (art. 30 AVG)**Het model verwerkingsregister voor Opdrachtgever, is terug te vinden in bijlage 4. Bij het opstellen van dit model heb ik rekening gehouden met de eisen die gesteld worden aan een verwerkingsregister.[[78]](#footnote-78) Daarnaast heb ik gekozen voor een simpele en duidelijke lay-out zodat er zo min mogelijk kans is op fouten en/of verwarring.

Het is nog niet bekend of er binnen Opdrachtgever al iemand is die als aanspreekpunt zal dienen voor alle privacy gerelateerde zaken en zorg zal dragen voor het up-to-date houden van registers, zoals het verwerkingsregister, en het privacybeleid.

1. **Een privacyverklaring opstellen om betrokkenen te informeren**  
   De privacyverklaring heb ik opgesteld aan de hand van het format van de Metaalunie.[[79]](#footnote-79) Dit format is gebaseerd op twee losse privacyverklaringen, één voor de werknemers en één voor klanten en leveranciers. Ik heb ervoor gekozen om hier één privacyverklaring van te maken zodat er geen verwarring kan ontstaan over het verwijzen naar de juiste privacyverklaring. Daarnaast heb ik getoetst of de privacyverklaring voldoet aan de eisen die gesteld worden aan de informatieplicht.[[80]](#footnote-80)
2. **Indien de grondslagen “toestemming” en/of “gerechtvaardigd belang” gebruikt worden, deze onderbouwen en bewijs van de gevraagde toestemming documenteren**

In de interviews met de medewerkers van verschillende afdelingen (bijlage 8 en persoonlijke communicatie met de medewerker personeelszaken, 24 mei 2018), is naar voren gekomen op welke manier persoonsgegevens verzameld, en verder verwerkt worden binnen de verschillende afdelingen.

Gebaseerd op deze informatie kan er geconcludeerd worden dat de gegevenswerking van Opdrachtgever op drie grondslagen gebaseerd kan worden:

1. Uitvoering van een overeenkomst

* Arbeidsovereenkomst, overeenkomst met klanten/leveranciers

1. Wettelijke verplichting

* Doorgifte aan de Belastingdienst, het UWV, de arbodienst, het pensioenfonds en de Inspectie voor Sociale Zaken en Werkgelegenheid

1. Gerechtvaardigde belangen  
   Opdrachtgever dient te onderbouwen waarom er volgens haar sprake is van een gerechtvaardigd belang bij de verwerking van de persoonsgegevens. De grondslag gerechtvaardigd belang is van toepassing voor de volgende verwerkingen:

* Verzenden van nieuwsbrief;
* Potentiële klanten benaderen;
* Klanten informeren over gewijzigde diensten en producten;
* Doorgifte aan derde partijen die in opdracht van Opdrachtgever werkzaamheden uitvoeren.

Voor al deze verwerkingen geldt dat Opdrachtgever er een gerechtvaardigd belang bij heeft, omdat zij deze verwerkingen uit moet voeren voor een goede bedrijfsvoering en dienstverlening.

Daarnaast verwerkt Opdrachtgever persoonsgegevens in verschillende computerprogramma’s en systemen.[[81]](#footnote-81) Opdrachtgever heeft een gerechtvaardigd belang bij het gebruik van deze programma’s en systemen omdat het gebruik noodzakelijk is voor de bedrijfsvoering.

Tot slot deelt Opdrachtgever persoonsgegevens met haar dochter- en zustermaatschappijen, ook hier geldt dat er sprake is van een gerechtvaardigd belang omdat dit noodzakelijk is om haar diensten uit te kunnen voeren en een optimale dienstverlening te garanderen.

1. **Verwerkersovereenkomsten afsluiten met al haar verwerkers**Zoals in het schema in paragraaf 3.2.2 is weergegeven, deelt Opdrachtgever persoonsgegevens met de volgende bedrijven:

* ADP;
* Leasemaatschappij;
* ISSYS;
* VITASYS;
* Protime;
* Arbodienst;
* Baken 5;
* UWV;
* Vanhier B.V.

Om te weten of het noodzakelijk is om een verwerkersovereenkomst af te sluiten met deze bedrijven, dient er eerst nagegaan te worden of zij verwerker, verwerkingsverantwoordelijke of medeverantwoordelijke zijn[[82]](#footnote-82).

*ADP*

*ADP voert een deel van de salarisadministratie uit voor Opdrachtgever. Het primaire doel van deze dienstverlening is het verwerken van persoonsgegevens van medewerkers van Opdrachtgever, zodat Opdrachtgever kan voldoen aan haar plichten die voortvloeien uit de arbeidsovereenkomst met haar werknemer. Daarnaast is ADP een organisatie die buiten de verwerkingsverantwoordelijke staat. ADP is dus een verwerker.*

*Leasemaatschappij*

*De leasemaatschappij verwerkt persoonsgegevens ten behoeve van Opdrachtgever, echter is het primaire doel van de dienstverlening, het leasen van een auto. De verwerking van persoonsgegevens is dus slechts een uitvloeisel. Daarnaast oefent de leasemaatschappij feitelijk gezien zelf invloed uit over de verwerking van de gegevens. Zij bepaald waar de gegevens voor verwerkt worden en waarom. Er is dus sprake van een verwerker.*

*ISSYS/VITASYS*

*Omdat ISSYS en VITASYS dezelfde soort diensten verlenen aan Opdrachtgever, zullen deze gezamenlijk behandeld worden.*

*ISSYS en VITASYS leveren software aan Opdrachtgever en zijn tevens de bedrijven die helpen in het geval er sprake is van problemen met computers en/of printers. Beide bedrijven staan niet onder gezag van Opdrachtgever en bepalen niet het doel en de middelen van de verwerking. Ook voeren beide bedrijven feitelijk geen invloed uit op de verwerking. Op grond van bovenstaande en de stroomdiagram in bijlage 1, kan er geconcludeerd worden dat beide bedrijven verwerker zijn.*

*Protime*

*Alle werknemers dienen aan het begin en aan het eind van hun werkdag in- en uit te klokken. De registratie hiervan wordt bijgehouden in het programma van Protime. Opdrachtgever stelt zelf het doel en de middelen voor de verwerking vast, Protime heeft hier geen enkele invloed op. Ook staat Protime niet onder het gezag van Opdrachtgever. Verder is het primaire doel van de dienstverlening het verwerken van persoonsgegevens. Alles bij elkaar maakt dat Protime een verwerker is.*

*Arbodienst*

*Opdrachtgever is als werkgever verplicht om zich bij te laten staan door een Arbodienst als de situatie hierom vraagt.[[83]](#footnote-83) Omdat de Arbodienst persoonsgegevens verwerkt op grond van een eigen wettelijke grondslag, is de Arbodienst geen verwerker, maar verwerkingsverantwoordelijke. Echter, zodra de Arbodienst meer taken uitvoert voor Opdrachtgever dan alleen de eigen wettelijke taken, is de Arbodienst wél verwerker. [[84]](#footnote-84) Het is niet bekend of Opdrachtgever andere diensten afneemt van de Arbodienst, daarom wordt de Arbodienst in dit onderzoek gezien als verwerkingsverantwoordelijke.*

*UWV*

*Voor het UWV geldt, net als de Arbodienst dat zij verwerkingsverantwoordelijke is omdat het verstrekken van persoonsgegevens aan het UWV, door Opdrachtgever, wettelijk verplicht is.[[85]](#footnote-85)*

*Baken 5*

*Zoals aangegeven is er met Baken 5 reeds een verwerkersovereenkomst afgesloten. Daardoor zal deze dienstverlener niet verder behandeld worden.*

*Vanhier B.V.*

*Wat betreft de rol van een accountant verschillen de meningen nogal.[[86]](#footnote-86) Zo zegt de Nederlandse Beroepsorganisatie van Accountants dat er gevallen zijn waarin een accountant niet de verwerkingsverantwoordelijke is, maar de verwerker.[[87]](#footnote-87) Afgaande op het schema in bijlage 1 en de criteria voor het beoordelen of er sprake is van een verwerkingsverantwoordelijke, medeverantwoordelijke of verwerker, concludeer ik dat de accountant verwerkingsverantwoordelijke is. Dit omdat de accountant feitelijk gezien degene is die invloed uitoefent over de verwerking. Immers, als Opdrachtgever zou bepalen hoe de accountant te werk moet gaan, is er de mogelijkheid dat de accountant zijn werkzaamheden niet naar behoren uit kan voeren. Daarnaast is de accountant gebonden aan wettelijke plichten die ervoor zorgen dat hij het doel en de middelen van de verwerking bepaald.*

Uit bovenstaande kan geconcludeerd worden dat Opdrachtgever een verwerkersovereenkomst\* af dient te sluiten met ADP, ISSYS, VITASYS en Protime. Voor ADP geldt dat zij zelf de nodige maatregelen[[88]](#footnote-88) hebben genomen om te voldoen aan de plicht van de verwerker.[[89]](#footnote-89)

\* In bijlage 4 is een standaard verwerkersovereenkomst opgenomen die door Opdrachtgever gebruikt kan worden. Ik heb ervoor gekozen om een model overeenkomst van modellen voor de rechtspraktijk[[90]](#footnote-90) te gebruiken, omdat dit een betrouwbare bron is. Ik heb gecontroleerd of de verwerkersovereenkomst inderdaad alle punten bevat die op grond van de AVG vereist zijn[[91]](#footnote-91) en de overeenkomst waar nodig aangepast zodat deze direct door Opdrachtgever gebruikt kan worden.

1. **Een datalekregister opstellen en bijhouden en daarbij een procedure voor datalekken opstellen**

In bijlage 3 is het format datalekregister opgenomen. Hierin kunnen alle feiten rondom een datalek gedocumenteerd worden. Naast het datalekregister, dient Opdrachtgever ook door middel van een standaard datalek procedure aan te tonen welke maatregelen er genomen worden indien er sprake is van een datalek. Vanwege tijdsnood, is ervoor gekozen om deze procedure niet op te nemen in dit onderzoek.

1. **Aangeven hoe er voldaan wordt (gaat worden) aan privacy by design & privacy by default**

Om aan te tonen dat Opdrachtgever voldoet aan privacy by design en privacy by default dient zij de verwerking van persoonsgegevens te minimaliseren, transparant te zijn met betrekking tot de functies en de verwerking van persoonsgegevens, beveiligingskenmerken te creëren en betrokkene in staat te stellen om controle uit te oefenen op de verwerking. Door de genomen maatregelen in een intern beleid te documenteren, is het voor de AP mogelijk om te controleren of er voldaan wordt aan de eisen van privacy by design en privacy by default.[[92]](#footnote-92)

In dit onderzoek is ervoor gekozen om geen intern beleid op te stellen met betrekking tot privacy by design en privacy by default. Mede vanwege het tijdsbestek waarin dit onderzoek afgerond diende te zijn, maar ook omdat ik van mening ben dat privacy by design en privacy by default toegepast dienen te worden op het moment dat Opdrachtgever alle overige punten implementeert.

1. **Beargumenteren waarom het uitvoeren van een DPIA wel/niet noodzakelijk is**

In paragraaf 3.1.3 onder “beschermingseffectbeoordeling/DPIA” is uitgebreid aan bod gekomen wanneer een DPIA wel/niet verplicht is. Bij Opdrachtgever is er geen sprake van:

* Een systematische en uitgebreide beoordeling van persoonlijke aspecten van betrokkenen, die gebaseerd is op geautomatiseerde verwerking (waaronder profilering) en waarop besluiten worden gebaseerd waaraan voor betrokkenen rechtsgevolgen zijn verbonden of die betrokkenen op vergelijkbare wijze wezenlijk treffen;
* Grootschalige verwerking van bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard;
* Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Er kan daarom gesteld worden dat er geen sprake is van een verwerking die mogelijk een hoog risico inhoudt voor betrokkenen, daardoor is het voor Opdrachtgever **niet** verplicht om een DPIA uit te voeren.

# Conclusies

## Beantwoording centrale vraag

De centrale vraag die in dit onderzoek beantwoord diende te worden is: *“Welke aanpassingen dient Opdrachtgever op basis van wetsanalyse, literatuuronderzoek en interviews met medewerkers te maken aan haar huidig privacybeleid om aan te kunnen tonen dat zij voldoet aan de Algemene Verordening Gegevensbescherming?”*

Uit het juridisch kader en de resultaten is gebleken dat er in ieder geval een aantal eisen zijn waar Opdrachtgever aan moet voldoen om aan te tonen dat zij voldoet aan de AVG, dat zij “AVG-proof” is. Het gaat hier om de volgende punten:

1. Een verwerkingsregister opstellen en bijhouden;
2. Een privacyverklaring opstellen om betrokkenen te informeren;
3. De grondslagen toestemming en/of gerechtvaardigd belang onderbouwen, indien van toepassing;
4. Verwerkersovereenkomsten afsluiten;
5. Een datalekregister en datalekprocedure opstellen;
6. Privacy by design en privacy by default in acht nemen;
7. DPIA uitvoeren of beargumenteren waarom dit niet noodzakelijk is.

Omdat er uit de interviews met medewerkers van verschillende afdelingen gebleken is dat er momenteel geen privacybeleid is, is de centrale vraag niet geheel correct meer. Desalniettemin blijft deze vraag wel het uitgangspunt van dit onderzoek en luidt het antwoord als volgt: Opdrachtgever dient alle bovenstaande punten toe te passen en aan de hand hiervan een privacybeleid op te stellen.

Het doel van het onderzoek, *een nieuw privacybeleid op stellen zodat Opdrachtgever aan kan tonen dat zij voldoet aan de verplichtingen uit de AVG*, is gedeeltelijk behaald. Het format verwerkingsregister, de privacyverklaring en het format datalekregister zijn als bijlage toegevoegd en direct bruikbaar. In plaats van een datalek procedure, heb ik ervoor gekozen om een format verwerkersovereenkomst toe te voegen. Ik heb hiervoor gekozen omdat ik van mening ben dat het afsluiten van verwerkersovereenkomsten een hogere prioriteit heeft dan het opstellen van een datalek procedure, mits het datalekregister wel direct in gebruik wordt genomen.

Het opstellen van een heel privacybeleid bleek meer tijd in beslag te nemen dan ik vooraf verwacht had. De door mij opgestelde documenten zijn een goede richting in het opstellen van een nieuw privacybeleid, echter, een echt beleid is het nog niet.

Toch ben ik van mening dat het onderzoek zeer bruikbaar is voor Opdrachtgever omdat ik alle relevante eisen om aantoonbaar te voldoen aan de AVG behandeld heb. Ook denk ik dat ondanks dat ik geen beleid opgesteld heb, het voor Opdrachtgever mogelijk is om zonder er teveel tijd aan kwijt te zijn, een AVG-proof privacybeleid op te stellen aan de hand van de door mij opgestelde standaard documenten en de uitgebreide informatie in het juridisch kader en de resultaten.

# Aanbevelingen

Graag wil ik Opdrachtgever aanbevelen om de door mij opgestelde documenten (verwerkersovereenkomst, datalekregister, verwerkingsregister en privacyverklaring) zo spoedig mogelijk in gebruik te nemen. Voor wat betreft het verwerkingsregister en het datalekregister geldt dat deze ook bijgehouden dienen te worden. Ik adviseer Opdrachtgever om één persoon aan te wijzen die verantwoordelijk zal zijn voor deze taken. Tevens is het verstandig om deze zelfde persoon als aanspreekpunt aan te wijzen voor alle privacy gerelateerde zaken. Daarnaast is het verstandig om alle werknemers op de hoogte te stellen van de privacyverklaring en deze werknemers uit te leggen hoe en wanneer ze deze privacyverklaring dienen te gebruiken.

Verder is het ondanks dat het uitvoeren van een DPIA voor Opdrachtgever niet noodzakelijk is, wel raadzaam om dit toch te doen. Door het uitvoeren van de DPIA kan Opdrachtgever nog beter aantonen dat zij voldoet aan de AVG.

Ook het opstellen van een datalekprocedure en een intern beleid met betrekking tot privacy by design en privacy by default zijn punten die ik Opdrachtgever graag aan wil bevelen, daar ik daar in dit onderzoek niet aan toe ben gekomen.

Tot slot adviseer ik Opdrachtgever om bij de door mij opgestelde documenten aan de hand van dit onderzoek een privacybeleid op te stellen en te implementeren binnen het bedrijf. Daarbij wil ik graag opmerken dat het mij verstandig lijkt om na te gaan of er met alle externe partijen die volgens dit onderzoek verwerkingsverantwoordelijke bleken te zijn, al een verwerkersovereenkomst is afgesloten of dat dit nog dient te gebeuren/niet nodig is.

Als alle in dit onderzoek behandelde punten met betrekking tot de verantwoordingsplicht en het aantoonbaar voldoen aan de AVG door Opdrachtgever verwerkt worden in het privacybeleid, zal zij bij controle van de AP aan kunnen tonen dat zij voldoet aan haar plichten als verwerkingsverantwoordelijke.

# Literatuurlijst

##### Wet- en regelgeving

Algemene Verordening Gegevensbescherming

Richtlijn 95/46/EG

##### Handleidingen en richtlijnen

Article 29 Data protection working party, *Guidelines on Personal data breach notification under Regulation 2016/679*

Groep gegevensbescherming artikel 29, *Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking “waarschijnlijk een hoog risico inhoudt” in de zin van Verordening 2016/679*

Ministerie van Justitie en Veiligheid, *Handleiding Algemene Verordening Gegevensbescherming en Uitvoeringswet Algemene Verordening Gegevensbescherming*

##### Boeken

**Berkvens e.a.**J. Berkvens, J. Reijner, M.J.M.G. van Gerwen, S. Vinken, S. Wiegerinck & S. Wolters, *Checklist Privacy – privacbeleid in 46 checklists,* Berghauser Pont Publishing 2018

**Engelfriet & Kager**A. Engelfriet, L. Meij & P. Kager, *De Algemene Verordening Gegevensbescherming (AVG). Artikelsgewijs commentaar,* IUS Mentis 2017

**Krijgsman e.a.**N. Krijgsman, J. Terstegge & K. Versmissen, *Grip op de AVG. De nieuwe privacywet,* Wolters Kluwer 2017

##### Artikelen

**Bastiaans, Bb 2018/24**S. Bastiaans, “Privacy in een nieuw jasje: een vergelijkging van beschermingsniveau tussen de Wbp en de AVG”, Bb 2018/24

**Bunt, van de & Strijbos, NJB 2018/357**T. van de Bunt & A. Strijbos, “De bewerkersovereenkomst onder de AVG”, *NJB 2018/357,* afl. 7

**Vries de, & Goudsmit, NJB 2016/1077**  
H. de Vries & M. Goudsmit, “Voorsorteren op de Algemene Verordening Gegevensbescherming”, *NJB* 2016/1077, afl. 22, p. 1071-1125

##### Internetbronnen

[www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) “Verantwoordingsplicht”, bezocht op 25 mei 2018

[www.autoriteitspersoonsgegevens.nl](http://www.autoriteitspersoonsgegevens.nl) “Mag u persoonsgegevens verwerken?”, bezocht op 25 mei 2018

[www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) “Wanneer mag u zich baseren op de grondslag uitvoering overeenkomst”, bezocht op 25 mei 2018

[www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) “Hoe weet u of u persoonsgegevens mag verwerken?”, bezocht op 25 mei 2018

[www.vijverbergjuristen.nl](http://www.vijverbergjuristen.nl) zoek op: “Bewerkersovereenkomst naar verwerkersovereenkomst”, bezocht op 27 mei 2018

[www.metaalunie.nl](http://www.metaalunie.nl) “AVG-check”, bezocht op 27 mei 2018

[www.uwv.nl](http://www.uwv.nl) “Uw contact met UWV wijzigt niet door de nieuwe AVG”, bezocht op 4 juni 2018

[www.adp.nl](http://www.adp.nl) zoek op: “Binding Corporate Rules”, bezocht op 7 juni 2018

[www.vangelderadvocaten.nl](http://www.vangelderadvocaten.nl) zoek op: “is een verwerkersovereenkomst met de arbodienst verplicht”, bezocht op 5 juni 2018

[www.europadecentraal.nl](http://www.europadecentraal.nl) zoek op: “privacy by design and by default”, bezocht op 5 juni 2018

[www.nba.nl](http://www.nba.nl) “Reactie NBA op berichtgeving Accountancy Vanmorgen inzake de AVG”, bezocht op 9 juni 2018

[www.accountancyvanmorgen.nl](http://www.accountancyvanmorgen.nl) “AVG en de rol van de accountant: Verwerker, verantwoordelijke of beide? Blijft er onduidelijkheid?”, bezocht op 9 juni 2018

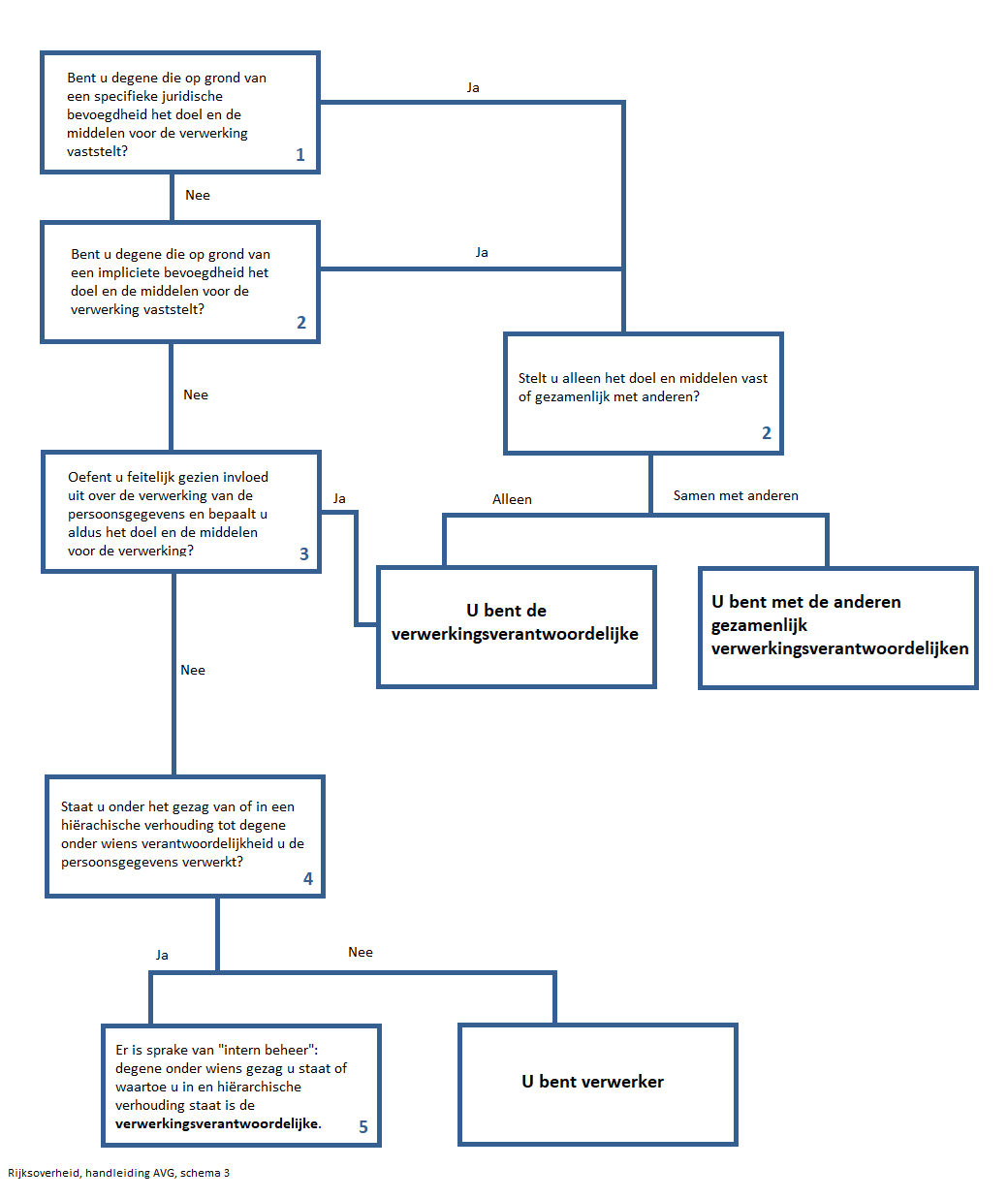
##### Overige

**Modellen voor de Rechtspraktijk**T.J.M. de Weerd, *VIII.5.65 Verwerkersovereenkomst*

5

# Bijlagen

## Schema 1: verwerker of verwerkingsverantwoordelijke?

****

## Schema 2: sancties/boetes AVG

|  |  |
| --- | --- |
| Overtreding | Hoogte van de boete |
| Inbreuk op:[[93]](#footnote-93)   * Art. 8 AVG   Voorwaarden toestemming van kinderen met betrekking tot diensten van de informatie maatschappij   * Art. 11 AVG   Het identificeren van betrokkene   * Artt. 25 t/m 39 AVG   Algemene verplichtingen van de verwerkingsverantwoordelijke   * Art. 41 lid 4   De verplichtingen van het toezichthoudend orgaan   * Artt. 42 en 43 AVG   De verplichtingen van het certificeringsorgaan | Maximaal 10.000.000 Euro of tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.[[94]](#footnote-94) |

|  |  |
| --- | --- |
| Inbreuk op/het niet naleven van:[[95]](#footnote-95)   * Artt. 5 t/m 7 en 9 AVG   Beginselen inzake verwerking van persoonsgegevens   * Artt. 12 t/m 22 AVG   Rechten van betrokkene (o.a. transparantie)   * Artt, 44 t/m 49 AVG   Het doorgeven van persoonsgegevens aan een ontvanger in een derde land of een internationale organisatie   * Hoofdstuk IX AVG   De verplichtingen uit hoofde van krachtens hoofdstuk IX door de lidstaten vastgesteld recht   * Art. 58 lid 1 en 2 AVG  Een bevel of een tijdelijke of definitieve verwerkingsbeperking of een opschorting van gegevensstromen door de toezichthoudende autoriteit en de verlening van toegang. | Maximaal 20.000.000 Euro of tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.[[96]](#footnote-96) |
| Inbreuk op een artikel waarop de AVG zelf geen sanctie stelt. | Een in het nationaal recht bepaalde sanctie[[97]](#footnote-97) |

##### 

## Datalek tabel

|  |  |
| --- | --- |
| **Vraag** | **Antwoord** |
| **Samenvatting incident (feiten en omstandigheden)** |  |
| **Is er sprake geweest van een dreiging of tekortkoming in de beveiliging of zijn er daadwerkelijk persoonsgegevens betrokken bij het incident (verloren gegaan of vernietigd, toegankelijk gemaakt of verstrekt aan een ander die deze gegevens niet zou mogen hebben)?** |  |
| **Als er persoonsgegevens betrokken zijn bij het incident, om hoeveel personen gaat het?** | Minimaal ……. Maximaal ……. |
| **Omschrijf de groep mensen van wie persoonsgegevens betrokken zijn bij het incident.** |  |
| **Wanneer vond het incident plaats?** | **(kies een van de volgende opties en vul aan)**   * Op (datum) * Tussen (begindatum periode) en (einddatum periode) * Nog niet bekend |
| **Wat is de aard van het incident?** | * Lezen (vertrouwelijkheid) * Kopiëren * Veranderen (integriteit) * Verwijderen of vernietigen (beschikbaarheid) * Diefstal * Nog niet bekend |

|  |  |
| --- | --- |
| **Om welk type persoonsgegevens gaat het?** | **(meerdere antwoorden mogelijk)**   * Naam-, adres – en woonplaatsgegevens * Telefoonnummers * E-mailadressen of andere adressen voor elektronische communicatie * Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer) * Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer) * Burgerservicenummer (BSN) * Paspoortkopieën of kopieën van legitimatiebewijzen * Geslacht, geboortedatum en/of leeftijd * Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens) * Overige gegevens, namelijk …. |
| **Welke gevolgen kan het incident hebben voor de persoonlijke levenssfeer van de betrokkenen?** | **(meerdere antwoorden mogelijk)**   * Stigmatisering of uitsluiting * Schade aan de gezondheid * Blootstelling aan (identiteits)fraude * Blootstelling aan spam of phising * Anders, namelijk ….. |
| **Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om het incident aan te pakken en om verdere inbreuken te voorkomen?** |  |
| **Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?** | **(kies één van de volgende opties)**   * Ja * Nee * Nog niet bekend |
| **(Alleen als uw vraag 10 met ja beantwoord heeft)**  **Wanneer heeft u het datalek gemeld aan de betrokkenen, of wanneer gaat u dit doen?** | * Ik heb het datalek aan de betrokkenen gemeld op (datum) * Ik ga het datalek aan de betrokkenen melden op (datum) * Nog niet bekend |
| **(Alleen als uw vraag 10 met ja beantwoord heeft)**  **Wat is de inhoud van de melding aan de betrokkenen?** |  |
| **(Alleen als uw vraag 10 met ja beantwoord heeft)**  **Hoeveel betrokkenen heeft u in kennis gesteld of gaat u in kennis stellen?** |  |

|  |  |
| --- | --- |
| **(Alleen als uw vraag 10 met ja beantwoord heeft)**  **Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken bij het in kennis stellen van de betrokkenen?** |  |
| **(Alleen als uw vraag 10 met nee beantwoord heeft)**  **Waarom ziet u af van het melden van het datalek aan de betrokkenen?** | **(kies één van de onderstaande opties en vul waar nodig aan)**   * De technische beschermingsmaatregelen die ik heb getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten * Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: (vul aan) * Ik heb zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk: (vul aan) * Anders, namelijk: (vul aan) |
| **Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?** | **(kies één van de volgende opties en vul waar nodig aan)**   * Ja * Nee * Deels, namelijk: (vul aan) |
| **(beantwoorden als antwoord vorige vraag “ja” of “deels” was)**  **Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd?** |  |
| **Heeft de inbreuk betrekking op personen in andere EU-landen?** | * Ja * Nee * Nog niet bekend |
| **Heeft uw bedrijf of organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?** | * Ja, namelijk: (vul aan) * Nee |

## Verwerkersovereenkomst

Partijen:

|  |  |
| --- | --- |
| I | [Opdrachtgever], een besloten vennootschap met beperkte aansprakelijkheid, statutair gevestigd te plaats, kantoorhoudende aan de straat nr. X te plaats, 'Verwerkingsverantwoordelijke'; |
| II | [Bedrijfsnaam verwerker], een besloten vennootschap met beperkte aansprakelijkheid, statutair gevestigd te \_\_\_\_\_\_\_\_\_\_, kantoorhoudende aan de \_\_\_\_\_\_\_\_\_\_ nr. \_\_\_\_\_\_\_\_\_\_ te \_\_\_\_\_\_\_\_\_\_, 'Verwerker'. |

Overwegingen:

|  |  |
| --- | --- |
| A | Verwerkingsverantwoordelijke en Verwerker zijn een overeenkomst aangegaan voor het verrichten van de volgende diensten: [diensten]. Deze overeenkomst leidt ertoe dat Verwerker in opdracht van Verwerkingsverantwoordelijke persoonsgegevens verwerkt |
| B | Verwerkingsverantwoordelijke en Verwerker wensen in deze overeenkomst de wederzijdse rechten en verplichtingen voor de verwerking van persoonsgegevens door Verwerker vast te leggen overeenkomstig de toepasselijke privacywetgeving. |

1. Partijen zijn het volgende overeengekomen:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1.1 | De in deze overeenkomst gebruikte woorden of formuleringen hebben de volgende betekenis:   |  |  | | --- | --- | | a | *AVG*: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming); | | b | Betrokkene: degene op wie een persoonsgegeven betrekking heeft; | | c | Onderliggende overeenkomst: de overeenkomst d.d. [DATUM] waarbij Verwerkingsverantwoordelijke aan Verwerker opdracht heeft gegeven om Verwerkingen te verrichten; | | d | Overeenkomst: deze verwerkersovereenkomst inclusief bijlagen daarbij; | | e | Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon,die Verwerker op grond van de onderliggende overeenkomst verwerkt of dient te verwerken, waarvan het soort persoonsgegevens en de categorieën van betrokkenen nader zijn gespecificeerd in bijlage 1; | | f | Privacywetgeving: alle toepasselijke wet- en regelgeving met betrekking tot de verwerking en bescherming van persoonsgegevens, waaronder maar niet beperkt tot de AVG en de Uitvoeringswet AVG; | | g | Uitvoeringswet *AVG*: regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming); | | h | Verwerken/verwerking: alle handelingen of reeks handelingen uitgevoerd op persoonsgegevens of een geheel van persoonsgegevens, al dan niet 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 persoonsgegevens; | |  |  | |

2. Toepasselijkheid

|  |  |
| --- | --- |
| 2.1 | Tenzij Partijen anders schriftelijk zijn overeengekomen, zijn de bepalingen van deze overeenkomst van toepassing op iedere verwerking door verwerker op grond van de onderliggende overeenkomst. |

3. Verwerking door verwerker

Algemeen

|  |  |
| --- | --- |
| 3.1 | Verwerker verwerkt persoonsgegevens ten behoeve van verwerkingsverantwoordelijke, overeenkomstig diens schriftelijke instructies en onder diens verantwoordelijkheid en op de wijze vastgelegd in de onderliggende overeenkomst. |
| 3.2 | Verwerker verwerkt de persoonsgegevens slechts in opdracht van Verwerkingsverantwoordelijke, behoudens afwijkende wettelijke verplichtingen. |
| 3.3 | Verwerker heeft geen zeggenschap over het doel en de middelen voor de verwerking van persoonsgegevens en neemt geen beslissingen over het gebruik van de persoonsgegevens, de verstrekking aan derden en de duur van de opslag van persoonsgegevens. |
| 3.4 | Verwerker stelt de Verwerkingsverantwoordelijke onmiddellijk schriftelijk in kennis indien een instructie naar het redelijk oordeel van Verwerker inbreuk oplevert op de toepasselijke privacywetgeving. |
| 3.5 | Verwerker stelt op eerste verzoek van Verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om de nakoming van in deze overeenkomst neergelegde verplichtingen aan te tonen. |
| 3.6 | Verwerker dient zorg te dragen voor de naleving van de voorwaarden die op grond van de toepasselijke privacywetgeving worden gesteld aan het verwerken van persoonsgegevens. |
| 3.7 | Verwerker verschaft enkel toegang tot de persoonsgegevens aan haar werknemers voor zover dit nodig is voor het verrichten van de diensten op grond van de onderliggende overeenkomst. |
| 3.8 | Verwerker mag de persoonsgegevens enkel buiten de Europese Economische Ruimte verwerken met voorafgaande schriftelijke toestemming van de Verwerkingsverantwoordelijke. |
| 3.9 | Verwerker zal de persoonsgegevens niet langer dan [termijn] verwerken, tenzij Verwerkingsverantwoordelijke hiertoe uitdrukkelijk schriftelijk opdracht heeft gegeven. |

4. Verstrekking persoonsgegevens aan derden

|  |  |
| --- | --- |
| 4.1 | Verwerker zal geen persoonsgegevens aan een derde verstrekken of ter beschikking stellen tenzij op grond van een uitdrukkelijke schriftelijke opdracht van Verwerkingsverantwoordelijke of op bevel van een gerechtelijke of bestuurlijke instantie, op voorwaarde dat Verwerker in dat geval Verwerkingsverantwoordelijke binnen 24 uur na ontvangst van een dergelijk bevel daarvan in kennis stelt om Verwerkingsverantwoordelijke zodoende in staat te stellen daartegen een haar ter beschikking staand rechtsmiddel in te stellen. |
| 4.2 | Indien Verwerker van oordeel is dat zij op grond van een wettelijke verplichting persoonsgegevens ter beschikking dient te stellen aan een daartoe bevoegde instantie zal zij daar niet toe overgaan, dan na overleg met en goedkeuring van Verwerkingsverantwoordelijke. Zij zal Verwerkingsverantwoordelijke zo spoedig mogelijk schriftelijk in kennis stellen van de wettelijke verplichting en daarbij alle relevante informatie verstrekken die Verwerkingsverantwoordelijke redelijkerwijs nodig heeft om de benodigde maatregelen te treffen om te bepalen of verstrekking kan plaatsvinden en, zo ja, onder welke voorwaarden. |

5. Verzoeken van Betrokkenen

|  |  |
| --- | --- |
| 5.1 | Verwerker dient Verwerkingsverantwoordelijke in kennis te stellen van alle verzoeken die rechtstreeks van Betrokkenen zijn ontvangen met betrekking tot de rechten van Betrokkenen op grond van de toepasselijke privacywetgeving, waaronder maar niet beperkt tot verzoeken tot inzage, rectificatie, wissing, beperking van de verwerking of overdracht van de persoonsgegevens. Verwerker geeft aan een dergelijk verzoek alleen gevolg indien Verwerkingsverantwoordelijke Verwerker daartoe schriftelijk opdracht heeft gegeven. |
| 5.2 | Verwerker handelt alle verzoeken om inlichtingen van Verwerkingsverantwoordelijke met betrekking tot de Verwerking van de Persoonsgegevens vlot en behoorlijk af. |

6. Medewerking Verwerker

|  |  |
| --- | --- |
| 6.1 | Verwerker zal de Verwerkingsverantwoordelijke medewerking verlenen bij het doen nakomen van de verplichtingen om: (i) verzoeken van Betrokkenen met betrekking tot de uitoefening van rechten van Betrokkenen op grond van de toepasselijke privacywetgeving te beantwoorden; (ii) passende technische en organisatorische maatregelen te nemen om een op het risico afgestemd beveiligingsniveau te waarborgen; (iii) datalekken te melden aan toezichthouder en de betrokkenen; (iv) een gegevensbeschermingseffectbeoordeling uit te voeren; (v) de toezichthouder te raadplegen voorafgaand aan een verwerking de een hoog risico met zich meebrengt. |

7. Inschakelen derden door Verwerker

|  |  |
| --- | --- |
| 7.1 | Verwerker mag uitsluitend na voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke een derde inschakelen bij de uitvoering van deze overeenkomst, onder de voorwaarden die Verwerkingsverantwoordelijke daarbij stelt. Indien een derde na schriftelijke toestemming van Verwerkingsverantwoordelijke wordt ingeschakeld om ten behoeve van de Verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten, zal Verwerker aan deze andere derde bij overeenkomst minstens dezelfde verplichtingen inzake de Verwerking en bescherming van persoonsgegevens opleggen als de verplichtingen die zijn opgenomen in deze overeenkomst. Verwerker is in alle opzichten verantwoordelijk en aansprakelijk voor het doen en laten van derden die zij in het kader van deze overeenkomst inschakelt. |

8. Geheimhouding

|  |  |
| --- | --- |
| 8.1 | Verwerker zal de persoonsgegevens en andere informatie verkregen van de Verwerkingsverantwoordelijke strikt geheim houden, waarbij zij minstens eenzelfde mate van zorg zal betrachten als die, die zij ten aanzien van de bescherming van haar eigen informatie van zeer vertrouwelijke aard in acht neemt. Verwerker zal de persoonsgegevens of andere informatie verkregen van de Verwerkingsverantwoordelijke niet openbaar maken, distribueren, verstrekken, of op andere wijze bekend maken aan andere personen dan haar werknemers die van de persoonsgegevens of andere informatie verkregen van de Verwerkingsverantwoordelijke kennis moeten kunnen nemen voor hun werkzaamheden voor de Verwerker en zal deze werknemers pas toegang geven tot de persoonsgegevens en andere informatie verkregen van de Verwerkingsverantwoordelijke, nadat zij zijn geïnformeerd over het vertrouwelijke karakter van de Persoonsgegevens en andere informatie verkregen van de Verwerkingsverantwoordelijke. Verwerker legt het in deze overeenkomst bepaalde ook aan haar werknemers op. |

9. Meldplicht datalekken

|  |  |
| --- | --- |
| 9.1 | Verwerker dient Verwerkingsverantwoordelijke onverwijld en in ieder geval uiterlijk binnen 24 uur nadat Verwerker ervan kennis heeft gekregen, in kennis te stellen van iedere inbreuk op de beveiliging (van welke aard dan ook) die (mede) betrekking heeft of kan hebben op de Verwerking van persoonsgegevens. |
| 9.2 | Verwerker dient Verwerkingsverantwoordelijke in ieder geval informatie te verstrekken over het volgende: (i) de aard van de inbreuk, waar mogelijk onder vermelding van de categorieën van Betrokkenen in kwestie en, bij benadering, het aantal Betrokkenen in kwestie; (ii) de (mogelijk) getroffen persoonsgegevens en, bij benadering, het aantal getroffen persoonsgegevens in kwestie; (iii) de vastgestelde en verwachte gevolgen van de inbreuk voor de verwerking van de persoonsgegevens en de daarbij betrokken personen; en (iv) de maatregelen die Verwerker heeft getroffen en zal treffen om de inbreuk aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele negatieve gevolgen van de inbreuk. |
| 9.3 | Verwerker erkent dat Verwerkingsverantwoordelijke onder omstandigheden wettelijk verplicht is om een inbreuk op de beveiliging (van welke aard dan ook) die (mede) betrekking heeft of kan hebben op de persoonsgegevens die Verwerker verwerkt, aan Betrokkenen en/of autoriteiten te melden. Een dergelijke melding door Verwerkingsverantwoordelijke zal nimmer als tekortkoming in de nakoming van deze overeenkomst of onderliggende overeenkomst of anderszins als onrechtmatige handeling worden beschouwd. |
| 9.4 | Verwerker zal alle maatregelen treffen die nodig zijn om de (mogelijke) schade van een inbreuk op de beveiliging te beperken en zal Verwerkingsverantwoordelijke ondersteunen bij meldingen aan Betrokkenen en/of autoriteiten. |

10. Beveiligingsmaatregelen en inspectie

|  |  |
| --- | --- |
| 10.1 | Verwerker zal conform artikel 32 AVG alle passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen, garanderen een passend beveiligingsniveau gelet op de stand van de techniek, de uitvoeringskosten, alsook gelet op de aard, de omvang, context en verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's die verwerking van de persoonsgegevens die de Verwerker verwerkt met zich meebrengen voor de rechten en vrijheden van de Betrokkenen. |
| 10.2 | Verwerker dient Verwerkingsverantwoordelijke te informeren indien een van de beveiligingsmaatregelen wijzigt. |
| 10.3 | Verwerker staat toe dat Verwerkingsverantwoordelijke de naleving van de beveiligingsmaatregelen door Verwerker inspecteert of dat op verzoek van Verwerkingsverantwoordelijke de gegevensverwerkingsfaciliteiten van Verwerker door een door Verwerkingsverantwoordelijke aan te wijzen onderzoeksinstantie worden geïnspecteerdin verband met de verwerkingsactiviteiten die onder deze overeenkomst vallen ('de Inspectie'). De Inspectie wordt uitgevoerd door een onderzoeksinstantie, die naar het redelijk oordeel van Verwerkingsverantwoordelijke neutraal en deskundig is. Verwerkingsverantwoordelijke draagt zorg dat de onderzoeksinstantie verplicht is tot geheimhouding van haar bevindingen tegenover derden. |
| 10.4 | Verwerkingsverantwoordelijke zal alle kosten, vergoedingen en onkosten in verband met de Inspectie betalen, met inbegrip van redelijke door Verwerker gemaakte interne kosten. |
| 10.5 | Verwerkingsverantwoordelijke zal Verwerker een exemplaar van het rapport van de Inspectie verstrekken. |

11. Verplichtingen Verwerkingsverantwoordelijke

|  |  |
| --- | --- |
| 11.1 | Verwerkingsverantwoordelijke is ten aanzien van de Verwerking van Persoonsgegevens krachtens deze overeenkomst de 'Verwerkingsverantwoordelijke' zoals omschreven in artikel 4 sub 7 AVG. |
| 11.2 | Verwerkingsverantwoordelijke gaat ermee akkoord en staat er voor in dat de verwerking van de persoonsgegevens overeenkomstig deze overeenkomst in overeenstemming is met de toepasselijke privacywetgeving. |

12. Aansprakelijkheid

|  |  |
| --- | --- |
| 12.1 | Verwerker is aansprakelijk voor alle schade voortvloeiende uit of verband houdend met het niet-nakomen van deze overeenkomst dan wel handelen in strijd met de toepasselijke privacywetgeving. |
| 12.2 | Verwerker vrijwaart Verwerkingsverantwoordelijke tegen aanspraken van derden, waaronder Betrokkenen, in verband met het toerekenbaar tekortschieten van Verwerker in de nakoming van de overeenkomst of overtreding door Verwerker van de toepasselijke privacywetgeving en zal alle daarmee verband houdende en daaruit voortvloeiende kosten (waaronder mede begrepen kosten van juridische bijstand) en schade van Verwerkingsverantwoordelijke vergoeden. |

13. Beëindiging

|  |  |
| --- | --- |
| 13.1 | De Overeenkomst is voor onbepaalde tijd aangegaan en eindigt op het tijdstip dat de onderliggende overeenkomst eindigt.  Retourneren of vernietigen Persoonsgegevens bij beëindiging Overeenkomst |
| 13.2 | Onverminderd andersluidende schriftelijke opdracht van Verwerkingsverantwoordelijke zal Verwerker in geval van beëindiging van de overeenkomst onverwijld alle aan haar ter beschikking gestelde persoonsgegevens aan Verwerkingsverantwoordelijke retourneren en alle digitale kopieën van persoonsgegevens vernietigen en aan Verwerkingsverantwoordelijke verklaren dat zij dit heeft uitgevoerd. Indien naar het redelijk oordeel van Verwerker een zelfstandige wettelijke verplichting van Verwerker het geheel of gedeeltelijk retourneren of vernietigen van de persoonsgegevens door Verwerker verbiedt of beperkt zal zij Verwerkingsverantwoordelijke zo spoedig mogelijk schriftelijk in kennis stellen van de wettelijke verplichting en daarbij alle relevante informatie verstrekken die Verwerkingsverantwoordelijke redelijkerwijs nodig heeft om te bepalen of vernietiging kan plaatsvinden en, zo ja, onder welke voorwaarden. Indien naar het redelijk oordeel van Verwerkingsverantwoordelijke de wettelijke verplichting (gedeeltelijke) vernietiging van de persoonsgegevens door Verwerker toelaat zal Verwerker daartoe op verzoek van Verwerkingsverantwoordelijke onverwijld overgaan. Is Verwerkingsverantwoordelijke van oordeel dat vernietiging niet mag plaatsvinden, dan zal zij Verwerker daarvan schriftelijk op de hoogte stellen. Verwerker garandeert in dat geval de vertrouwelijkheid van de Persoonsgegevens jegens Verwerkingsverantwoordelijke en zal de persoonsgegevens niet verwerken behalve ter voldoening aan haar bovenbedoelde wettelijke verplichting of na schriftelijke opdracht van Verwerkingsverantwoordelijke. |

14. Overdracht rechten en plichten

|  |  |
| --- | --- |
| 14.1 | Deze overeenkomst en de rechten en verplichtingen uit deze overeenkomst kunnen door Verwerker niet aan derden worden overgedragen zonder de voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke. |

15. Deelbaarheid

|  |  |
| --- | --- |
| 15.1 | Indien één of meer bepalingen van deze overeenkomst niet rechtsgeldig blijkt te zijn, zal de overeenkomst voor het overige van kracht blijven. Partijen zullen over de bepalingen welke niet rechtsgeldig zijn overleg plegen, teneinde een vervangende regeling te treffen die wel rechtsgeldig is en zoveel mogelijk aansluit bij de strekking van de te vervangen regeling. |

16. Toepasselijkheid recht en geschillen

|  |  |
| --- | --- |
| 16.1 | Nederlands recht is van toepassing op deze overeenkomst. |
| 16.2 | Alle geschillen voortvloeiende uit of samenhangende met deze overeenkomst zullen uitsluitend worden voorgelegd aan de bevoegde rechter te \_\_\_\_\_\_\_\_\_\_. |

Aldus is overeengekomen en in tweevoud ondertekend op \_\_\_\_\_\_\_\_\_\_ te \_\_\_\_\_\_\_\_\_\_

voor\_\_\_\_\_\_\_\_\_\_

voor\_\_\_\_\_\_\_\_\_\_

## Privacyverklaring

Opdrachtgever, gevestigd aan adres, Nederland, is verantwoordelijk voor de verwerking van persoonsgegevens zoals weergegeven in deze privacyverklaring.

**Contactgegevens opdrachtgever**

**Persoonsgegevens die wij verwerken**Opdrachtgever verwerkt uw persoonsgegevens doordat u gebruik maakt van onze diensten en/of omdat u deze zelf aan ons verstrekt.

Hieronder vindt u een overzicht van de persoonsgegevens die wij verwerken:

|  |  |
| --- | --- |
| **Klant- en leveranciersadministratie** | **Personeels- en loonadministratie** |
| * Voor- en achternaam contactpersoon | * NAW-gegevens |
| * Geslacht van de contactpersoon | * Telefoonnummer |
| * Telefoonnummer | * E-mailadres |
| * E-mailadres | * IBAN nummer en BIC bankcode |
|  | * BSN nummer |
|  | * NAW-gegevens contactpersoon in geval van nood |

Via het contact- en sollicitatieformulier worden de volgende gegevens verzameld:

* Naam
* E-mailadres
* Telefoonnummer

**Bijzondere en/of gevoelige persoonsgegevens die wij verwerken**Onze website en/of dienst heeft niet de intentie gegevens te verzamelen over websitebezoekers die jonger zijn dan 16 jaar. Tenzij ze toestemming hebben van ouders of voogd. We kunnen echter niet controleren of een bezoeker ouder dan 16 is. Wij raden ouders dan ook aan betrokken te zijn bij de online activiteiten van hun kinderen, om zo te voorkomen dat er gegevens over kinderen verzameld worden zonder ouderlijke toestemming. Als u er van overtuigd bent dat wij zonder die toestemming persoonlijke gegevens hebben verzameld over een minderjarige, neem dan contact met ons op via info@opdrachtgever.nl, dan verwijderen wij deze informatie.

**Verzamelen en gebruiken van persoonsgegevens van sollicitanten, uitzendkrachten/payroll-werknemers, stagiaires en werknemers**Graag maken wij u er op attent dat wij de persoonsgegevens die u ons verstrekt zullen verzamelen en gebruiken omdat dit noodzakelijk is voor het doorlopen van de sollicitatieprocedure of om een (eventuele) arbeidsovereenkomst/stageovereenkomst/uitzendovereenkomst te sluiten en uit te voeren. Daarnaast zijn bepaalde persoonsgegevens nodig voor de nakoming en uitvoering van bepalingen uit de voor ons geldende CAO. Ook verzamelen en gebruiken wij uw persoonsgegevens om aan bepaalde wettelijke verplichtingen te kunnen voldoen. Deze wettelijke verplichtingen hebben bijvoorbeeld te maken met de vaststelling en verschuldigdheid van belastingen en premies voor werknemers.  
  
Gelet op deze noodzaak bent u verplicht om de hiervoor benodigde persoonsgegevens aan ons te verstrekken. Als u ons geen of onvoldoende persoonsgegevens verstrekt, kunnen wij geen sollicitatieprocedure met u doorlopen, een (eventuele) arbeidsovereenkomst/stageovereenkomst/uitzendovereenkomst met u aangaan en uitvoeren of aan onze wettelijke verplichtingen voldoen.  
  
Bent u (payroll-)werknemer of stagiair, dan gebruiken wij uw gegevens voor het opstellen, uitvoeren en beëindigen van de arbeids- en stageovereenkomst of de arbeidsrelatie. Hieronder wordt onder meer verstaan:

* De behandeling van personeelszaken;
* Het vaststellen en uitbetalen van het salaris, vergoedingen en andere geldbedragen; en
* Het vaststellen en betalen van eventuele belastingen, premies en andere fiscale verplichtingen ten behoeve van u als werknemer of stagiair.

Bent u een sollicitant, dan gebruiken wij uw gegevens om met u te kunnen communiceren over het verloop van de sollicitatieprocedure, de beoordeling van uw geschiktheid voor een functie die vacant is of kan komen en de eventuele afhandeling van de door u gemaakte onkosten.

Bent u een uitzendkracht, dan zullen wij de gegevens die wij verkrijgen van het uitzendbureau gebruiken voor de beoordeling van uw geschiktheid voor een functie die vacant is of kan komen en voor de uitvoering van de uitzendovereenkomst.

**Met welk doel en op basis van welke grondslag wij persoonsgegevens verwerken**Opdrachtgever verwerkt uw persoonsgegevens voor de volgende doelen:

* Het afhandelen van uw betaling
* Verzenden van onze nieuwsbrief en/of reclamefolder
* U te kunnen bellen of e-mailen indien dit nodig is om onze dienstverlening uit te kunnen voeren
* U te informeren over wijzigingen van onze diensten en producten
* Om goederen en diensten bij u af te leveren

Opdrachtgever verwerkt ook persoonsgegevens als wij hier wettelijk toe verplicht zijn, zoals gegevens die wij nodig hebben voor onze belastingaangifte.

**Direct marketing**Als u ons daarvoor toestemming heeft gegeven of als wij er een gerechtvaardigd belang bij hebben, zullen wij de door u opgegeven persoonsgegevens bewaren en gebruiken om u in de toekomst persoonlijk per e-mail op de hoogte te brengen van onze bestaande en nieuwe producten en diensten en u hier eventueel een aanbieding voor te doen. Iedere keer dat wij u een reclamemailing sturen, heeft u de mogelijkheid ons te laten weten hier geen prijs meer op te stellen. Zie hiervoor de afmeldlink onderaan iedere mailing.

**Geautomatiseerde besluitvorming**Opdrachtgever neemt niet op basis van geautomatiseerde verwerkingen besluiten over zaken die (aanzienlijke) gevolgen kunnen hebben voor personen. Het gaat hier om besluiten die worden genomen door computerprogramma's of -systemen, zonder dat daar een mens (bijvoorbeeld een medewerker van Opdrachtgever) tussen zit. Opdrachtgever gebruikt de volgende computerprogramma's of -systemen:

* Microsoft Office inclusief Microsoft Outlook, Microsoft Exchange en Microsoft Access en de bijbehorende opslagmogelijkheden voor e-mails en andere bestanden..
* ISAH
* Vantage
* Protime

Wij hebben een gerechtvaardigd belang bij het gebruik van bovenstaande computerprogramma’s en -systemen, omdat het gebruik hiervan noodzakelijk is voor onze bedrijfsvoering.

**Hoe lang we persoonsgegevens bewaren**Opdrachtgever bewaart uw persoonsgegevens niet langer dan strikt nodig is om de doelen te realiseren waarvoor uw gegevens worden verzameld. Wij hanteren de volgende bewaartermijnen voor de volgende (categorieën) van persoonsgegevens:

Sollicitatiegegevens worden tot vier weken na het einde van de sollicitatieprocedure bewaard, tenzij de sollicitant aangeeft dat de gegevens langer bewaard mogen worden, dan worden de gegevens bewaard tot maximaal 1 jaar na einde sollicitatieprocedure. Deze gegevens worden bewaard om de sollicitatieprocedure te kunnen doorlopen.

Personalia worden tot maximaal twee jaar na het einde van de overeenkomst bewaard om uitvoering te geven aan de overeenkomst en te voldoen aan de wettelijke verplichtingen rondom de overeenkomst.

Gegevens die wij via het contactformulier verzamelen worden maximaal vier weken bewaard, tenzij er rede is om de gegevens langer te bewaren.

Fiscale gegevens worden maximaal 7 jaar bewaard om te voldoen aan onze wettelijke verplichting.

**Delen van persoonsgegevens met derden**Opdrachtgever verkoopt uw gegevens niet aan derden. Wel is het is mogelijk dat wij uw persoonsgegevens doorgeven aan andere partijen. Deze andere partijen kunnen overheidsorganen zijn, maar ook partijen die in onze opdracht werkzaamheden uitvoeren of partijen aan wie wij verplicht zijn gegevens te verstrekken in verband met de uitvoering van de (arbeids)overeenkomst. Het gaat om de volgende partijen:

* De Belastingdienst;
* Het UWV;
* Onze arbodienst/bedrijfsarts;
* De Inspectie voor Sociale Zaken en Werkgelegenheid;
* Het Pensioenfonds;
* De verzuimverzekeraar;
* Onze salarisadministrateur.

Soms zal het verstrekken van uw gegevens aan een ander noodzakelijk zijn om te kunnen voldoen aan de wet, zoals het geval is bij doorgifte aan de Belastingdienst, het UWV, de arbodienst/bedrijfsarts, het Pensioenfonds en de Inspectie voor Sociale Zaken en Werkgelegenheid.

In andere gevallen is de doorgifte noodzakelijk om de (arbeids)overeenkomst met u te kunnen uitvoeren. Bij verstrekking van uw gegevens aan onze verzuimverzekeraar hebben wij een gerechtvaardigd belang, namelijk dat wij daardoor aanspraak kunnen maken op een verzekeringsuitkering.

Daarnaast zijn er partijen die in onze opdracht werkzaamheden uitvoeren. Bij deze doorgifte van uw gegevens hebben wij een gerechtvaardigd belang. Deze werkzaamheden zijn uitbesteed vanwege (onder meer) de kennis en expertise die onze salarisadministrateur bezit. Om de (arbeids)overeenkomst met u uit te voeren, heeft de salarisadministrateur uw persoonsgegevens nodig.

Met bedrijven die uw gegevens verwerken in onze opdracht, sluiten wij een verwerkersovereenkomst om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens. Opdrachtgever blijft verantwoordelijk voor deze verwerkingen.  
  
Uw persoonsgegevens worden ook gedeeld met onze dochter- en zusterbedrijven om onze werkzaamheden uit te kunnen voeren en een optimale dienstverlening te kunnen garanderen.

**Cookies, of vergelijkbare technieken, die wij gebruiken**Opdrachtgever gebruikt alleen technische en functionele cookies. En analytische cookies die geen inbreuk maken op uw privacy. Een cookie is een klein tekstbestand dat bij het eerste bezoek aan deze website wordt opgeslagen op uw computer, tablet of smartphone. De cookies die wij gebruiken zijn noodzakelijk voor de technische werking van de website en uw gebruiksgemak. Ze zorgen ervoor dat de website naar behoren werkt en onthouden bijvoorbeeld uw voorkeursinstellingen. Ook kunnen wij hiermee onze website optimaliseren. U kunt zich afmelden voor cookies door uw internetbrowser zo in te stellen dat deze geen cookies meer opslaat. Daarnaast kunt u ook alle informatie die eerder is opgeslagen via de instellingen van uw browser verwijderen.

**Gegevens inzien, aanpassen of verwijderen**U heeft het recht om uw persoonsgegevens in te zien, te corrigeren of te verwijderen. Daarnaast heeft u het recht om uw eventuele toestemming voor de gegevensverwerking in te trekken of bezwaar te maken tegen de verwerking van uw persoonsgegevens door Opdrachtgever en heeft u het recht op gegevensoverdraagbaarheid. Dat betekent dat u bij ons een verzoek kunt indienen om de persoonsgegevens die wij van u beschikken in een computerbestand naar u of een ander, door u genoemde organisatie, te sturen.  
  
U kunt een verzoek tot inzage, correctie, verwijdering, gegevensoverdraging van uw persoonsgegevens of verzoek tot intrekking van uw toestemming of bezwaar op de verwerking van uw persoonsgegevens sturen naar info@opdrachtgever.nl.

Om er zeker van te zijn dat het verzoek tot inzage door u is gedaan, vragen wij u een kopie van uw identiteitsbewijs met het verzoek mee te sturen. Maak in deze kopie uw pasfoto, MRZ (machine readable zone, de strook met nummers onderaan het paspoort), paspoortnummer en Burgerservicenummer (BSN) zwart. Dit ter bescherming van uw privacy. We reageren zo snel mogelijk, maar binnen vier weken, op uw verzoek.

Opdrachtgever wil u er tevens op wijzen dat u de mogelijkheid heeft om een klacht in te dienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens. Dat kan via de volgende link: https://autoriteitpersoonsgegevens.nl/nl/contact-met-de-autoriteit-persoonsgegevens/tip-ons

**Hoe wij persoonsgegevens beveiligen**Opdrachtgever neemt de bescherming van uw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Als u de indruk heeft dat uw gegevens niet goed beveiligd zijn of er aanwijzingen zijn van misbruik, neem dan contact op via [info@opdrachtgever.nl](mailto:info@nijdra.nl)

## Verwerkingsregister

|  |  |
| --- | --- |
| **Verwerkingsactiviteiten ten aanzien van persoonsgegevens** | **Invullen** |
| Voor welk administratief bedrijfsonderdeel worden persoonsgegevens verwerkt |  |
| Naam en contactgegevens verwerkingsverantwoordelijke |  |
| Doel(en) verwerking |  |
| Van welke categorieën personen worden gegevens verwerkt |  |
| Welke categorieën persoonsgegevens worden verwerkt |  |
| Aan welke categorieën ontvangers zijn of zullen de persoonsgegevens worden verstrekt |  |
| Hoe lang gaat u de persoonsgegevens bewaren |  |
| Welke beveiligingsmaatregelen zijn er getroffen |  |

## Vooraf opgestelde interviewvragen

1. Wat is uw functie binnen Opdrachtgever?
2. Wat zijn uw hoofdwerkzaamheden?
3. Van wie verwerkt u persoonsgegevens/van welke groep(en) personen verwerkt u persoonsgegevens?
4. Welke persoonsgegevens verwerkt u?

* Verwerken = verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken etc.

1. Op welke manier verzamelt u deze persoonsgegevens/hoe komt u aan deze persoonsgegevens?
2. Waar bewaart u de door u verzamelde gegevens?
3. Hoe lang bewaart u de door u verzamelde persoonsgegevens?
4. Wie hebben er allemaal toegang tot deze persoonsgegevens?

Hangt samen met:

1. Met welke externe partijen worden de persoonsgegevens gedeeld?
2. Zijn er standaard procedures met betrekking tot het verwerken en beschermen van persoonsgegevens?
3. Wat zou u graag terugzien in de nieuwe privacy procedures voor Opdrachtgever?

## Transcripts

##### Interview 1

##### Interviewer: Rosaline Rodenburg Geïnterviewde: manager en medewerker afdeling Inkoop/Verkoop Opdrachtgever Datum en duur interview: 30 april 2018, 22 minuten Doel interview: inzicht krijgen in de verwerking van persoonsgegevens binnen Opdrachtgever

**Interviewer**: goedemiddag, aller eerst wil ik even aangeven dat ik het interview op zal nemen als jullie dit goed vinden, zodat ik deze kan transcriberen en gebruiken voor mijn onderzoek. Jullie namen zullen niet genoemd worden in mijn onderzoek, omdat dit verder geen toegevoegde waarde heeft, vinden jullie dit goed?

**Medewerker** en **Manager**: ja hoor, prima.

**Interviewer**: ik heb van te voren wat vragen opgesteld, het voornaamste doel van het interview is om inzicht te krijgen in welke persoonsgegevens jullie verwerken en hoe dit gebeurd. Want eh ik heb wel van medewerker X wat lijstjes ontvangen van persoonsgegevens die binnen het bedrijf verwerkt worden, maar eh, ja jullie werken er natuurlijk echt mee. Dus ja, dat is eigenlijk het voornaamste doel.

**Interviewer**: nou eh, dan ga ik beginnen met vraag 1. Wat is jullie functie en wat houdt die in

**Manager**: nou eh op deze afdeling.. eh, ik ben sales manager en hij is accountmanager..

**Interviewer**: ja.. en eh, wat zijn jullie hoofdwerkzaamheden als je een beetje een standaard dag zou beschrijven.

**Medewerker**: nou, het aanbieden van offertes en eh nieuwe klanten zoeken…

**Manager**: en benaderen!

**Medewerker**: daarnaast eh relatie onderhouden.

**Interviewer**: ja eh, dus wel veel contact met de klanten dus?

**Medewerker**: ja, klantcontact ja en vooral mailcontact.

**Interviewer**: ja eh ok.. En eh van wie verwerken jullie persoonsgegevens?

**Manager**: nou eh vooral klanten dus en potentiële klanten.. maar laat ik het zo stellen: hoe wij aan onze persoonsgegevens komen.

**Interviewer**: ja, nouja, verwerken is inderdaad hoe kom je eraan, wat doe je ermee, hoe sla je het op..

**Manager**: ja kijk, wij staan op een beurs en krijgen een visitekaartje, daar staan zijn, of haar persoonlijke gegevens op, bedrijfsgegevens ook natuurlijk. En dan gaan wij aan de slag.. Zo verwerken wij denk ik de gegevens die wij hebben he?

**Medewerker**: ja, daarna ook eh als ze uiteindelijk klant van ons worden, krijgen we ook contact met andere mensen binnen dat bedrijf.

**Manager**: ja, dan krijg je meer kaartjes..

**Medewerker**: of dan krijg je een mail en sla je die contactgegevens op in ons systeem.

**Interviewer**: ja, en die kaartjes krijg je dus van die personen zelf?

**Medewerker**: ja of eh, via de mail die ze ons sturen.

**Interviewer**: ja, maar die mensen geven vrijwillig, uit zichzelf die gegevens?

**Manager**: ja klopt.

**Interviewer**: ja oke..

**Manager**: die worden bij ons dan verder verwerkt, met name dus bedrijfsgegevens en dan eh naam contactgegevens van die persoon, functie van die persoon, wat wij als info hebben gekregen van die personen, als we bijvoorbeeld geen 06 nummer hebben gekregen, dan hebben we die niet en vragen we er ook niet naar.

**Interviewer**: ja, en eh waar slaan jullie die gegevens op?

**Manager**: in ons ERP systeem en in een soort CRM wat wij hebben, dat is een excelbestand.

**Interviewer**: ja, en worden die systemen door jullie zelf beheerd of door een ander bedrijf?

**Manager**: nee door ons .

**Medewerker**: ja

**Interviewer**: dus er is geen externe partij?

**Manager**: nee, dat doen wij allemaal zelf.

**Interviewer**: en eh, nou jullie hebben het ook over veel mailverkeer, hoe doen jullie dat? Het opslaan van e-mailtjes, hoelang worden die bewaard.. waar worden die bewaard?

**Manager**: eh, in onze persoonlijke mailboxen worden die bewaard. In sommige gevallen ook bij offertes, dus eh, in een meer openbare map binnen Opdrachtgever, voornamelijk ??? doet dat, maar wij zien dat ook als verkoop.

**Interviewer**: ja..

**Manager**: ehh, ja ik onderhoud mijn mailbox eigenlijk niet meer, dat wordt gewoon automatisch gedaan, op de achtergrond wordt ie ververst en wordt het naar het archief gebracht en volgens mij na zoveel jaar ben ik hem kwijt.

**Medewerker**: ja, bij mij eh blijft het gewoon in mijn archief staan.

**Manager**: oh wel? Oh.. ik heb wel eens af en toe gaten erin.. maar dat kan je volgens mij gewoon instellen, of het blijft gewoon oneindig in je mailbox.

**Medewerker**: ja, daar zijn instellingen voor in outlook dat je eh bijvoorbeeld mails ouder dan drie jaar automatisch verwijderd.

**Interviewer**: ja dan echt verwijderd, dus ook niet naar het archief?

**Medewerker** en **Manager**: nee.

**Interviewer**: ok ehhh.. even kijken.. onder de AVG is het heel belangrijk dat degene waarvan je de gegevens verwerkt ook echt op de hoogte zijn van eh dat hun gegevens verwerkt worden en met welk doel ze verwerkt worden.. eh, als ik jullie nu zo hoor denk ik het voornaamste is natuurlijk het ontvangen van die visitekaartjes ehh.. ja het geven van visitekaartjes geeft volgens mij al aan dat ze zelf toestemming geven, je kan er vanuit gaan dat ze willen dat je hun contactgegevens gebruikt om contact met ze op te nemen.. Maar wat jij eh verder met die gegevens doet, dat zou je ze wel moeten vertellen.. omdat ze wel toestemming geven om contact te leggen, maar niet voor andere mogelijke doelen.. ehm, ja, doen jullie nu iets om bewust de persoonsgegevens te beschermen?

**Manager** en **Medewerker**: nee, helemaal niet.. maar dat is ook wat ik al eerder aan heb gegeven, moeten wij niet, en dan bedoel ik alle medewerkers, een standaard regel opnemen in onze e-mailhandtekening, wat wij ermee doen en dan eh bijvoorbeeld zie de privacystatement van opdrachtgever op de website.

**Interviewer**: ja, klopt, dat is inderdaad ook mijn idee.. ehm, ik kan me voorstellen dat het voor de ene afdeling lastiger zal zijn om de regels van de AVG mee te nemen in het werkproces.. Hebben jullie een idee wat voor jullie het makkelijkst zou zijn?

**Medewerker**: eh ja, die e-mailhandtekening inderdaad en eh ja een soort van leidraad voor ons, wat moeten we doen en hoe.. op de website staat trouwens al iets over de privacy op de website.

**Interviewer**: ja ok, nou eh het idee is dat ik de standaard documenten op ga stellen die verplicht zijn vanuit de AVG, maar ook dat ik daar inderdaad dus een soort beleid of leidraad bij ga schrijven voor de medewerkers.. eh.. staat er nu al iets op papier wat betreft de omgang met persoonsgegevens? Hoe zorgen jullie er nu voor dat jullie voldoen aan de wet?

**Medewerker**: ja, eh niet. Het is niet geregeld

**Interviewer**: ok niet.. en eh, hoe zijn jullie dan op de hoogte van de wet en regelgeving?

**Medewerker** en **Manager**: ook niet..

**Interviewer**: ok, dus eh, jullie moeten eigenlijk vanaf 0 beginnen..

**Manager**: vanaf 0 beginnen ja.. ja

**Interviewer**: dus bewaartermijnen weten jullie ook niet?

Medewerker en **Manager**: nee, geen idee.

**Manager**: ik heb zelfs cursus gehad van verkoop dat ik formulieren bij moest houden van mijn klanten met wie zijn kinderen zijn, wanneer ze jarig zijn enzo, zodat ik ze een kaartje kan sturen.

**Interviewer**: ja, dat zou ik onder de AVG niet zomaar doen nee.

**Medewerker**: ja en eh, via zo’n visitekaartje, schrijven wij mensen bijvoorbeeld ook in voor onze nieuwsbrief, maar daar moeten ze dus eigenlijk ook akkoord voor geven?

**Interviewer**: ja eh, nieuwsbrieven versturen is nu al geregeld in de telecommunicatiewet, ik zal als ik het red ervoor zorgen dat ik de regels hierover ook opneem in het beleid.

**Manager**: ja, daar moeten we dan voor zorgen.. Maar ik ga niet alles met de hand doen, als er toestemming of iets dergelijks gevraagd moet worden, moet dat wel makkelijk kunnen gebeuren.

**Interviewer**: ja ik ga eh ook nog dingen overleggen met de ICT medewerker, omdat ik zelf natuurlijk niet precies weet wat mogelijk is.. nou eh de laatste vraag: er zijn nu dus nog geen procedures of een standaard beleid, eh, wat is jullie idee als eh wat zou je handig vinden qua inhoud van het beleid.

**Medewerker**: nou, eh gewoon in hapklare brokken, een soort stappenplan.. hoe je je als bedrijf zijnde in kan dekken.

**Interviewer**: ja ik had zelf het idee om eh de basisinformatie die voor iedereen geldt op te nemen in het beleid en dan per onderdeel de aandachtspunten toe te voegen en ook aan te geven wanneer iets met name belangrijk is in welke situatie en duidelijk aangegeven waar wat te vinden is zodat je niet een heel boekwerk door hoeft te bladeren.

**Medewerker**: wordt het een heel boekwerk ja?

**Interviewer**: ehhhh… ja, nou, aan de ene kant wel aan de andere kant niet.. het feit dat jullie nog helemaal niks gedaan hebben met privacywetgeving zorgt er denk ik wel voor dat het in jullie ogen een heel boekwerk zal zijn, omdat voor jullie gewoon álles nieuw is.. en als je in een bedrijf zit waar ze wel al bekend zijn met privacywetgeving en wel al bekend zijn met de wet bescherming persoonsgegevens, de wet die hiervoor gold.. dan is het heel anders, want eigenlijk valt het wel mee hoeveel er veranderd, maar omdat jullie je nu pas bewust bezig gaan houden met privacywetgeving, is het wel heel veel..

**Medewerker**: ja eh, ik ben wel benieuwd naar je rapport, ik zou het wel willen lezen..

**Interviewer**: ja, ik zal sowieso zorgen dat er 1 of 2 exemplaren binnen het bedrijf zijn zodat personen die geïnteresseerd zijn het kunnen lezen.

**Manager**: ja eh, als je nog vragen hebt ofzo dan eh loop je maar even langs hoor, ik zit natuurlijk meestal aan de andere kant, maar medewerker is mijn rechterhand dus daar kan je altijd terecht

**Interviewer**: ja, ik zal tussendoor vast nog wel wat vragen hebben, dankjewel in ieder geval en eh fijne dag nog.

**Manager** en **medewerker**: ja, jij ook bedankt.

##### Interview 2

##### Interviewer: Rosaline Rodenburg Geïnterviewde: manager en medewerker afdeling Financiële administratie Opdrachtgever Datum en duur interview: 2 mei 2018, 16 minuten Doel interview: inzicht krijgen in de verwerking van persoonsgegevens binnen Opdrachtgever

**Interviewer:** goedemorgen, eh, allereerst wil ik vragen of jullie het goed vinden dat ik het interview opneem zodat ik deze kan transcriberen en gebruiken voor mijn onderzoek. Ik zal geen namen noemen maar gewoon medewerker en manager.

**Medewerker**: prima.

**Manager**: ja hoor, is goed.

**Interviewer**: mijn eerste vraag was is zouden jullie toelichting kunnen geven op jullie functie en werkzaamheden?

**Medewerker**: ik maak tussentijdse cijfers, ik verzamel eigenlijk alle cijfers die andere mensen invoeren en ik zet dat in een rapport en zorg dat het klopt.. en eh salarisverwerking, ik krijg van personeelszaken de salarismutaties om te verwerken en dan zet ik dat in het systeem om een salarisstrookje te krijgen.. de financiële administratie, ja..

**Interviewer:** dank je en de vraag die daarmee samenhangt is van welke personen of eigenlijk welke groep personen verzamel je de persoonsgegevens?

**Medewerker:** eigenlijk van alle personeelsleden maar ik sla het niet echt op, manager personeelszaken heeft echt het archief ehh.

**Manager:** nee, maar wij slaan het ook op, want wij hebben hier de salarisstroken staan, de kopieën dus..

**Interviewer:** ja, en welke gegevens zijn dat?

**Manager:** naam, bankrekeningnummer, de NAW-gegevens, de fiscale gegevens en het salaris dat de mensen uitbetaald hebben gekregen de laatste 8 jaren.

**Interviewer:** oké en jullie verzamelden die gegevens dus niet zelf begrijp ik maar die krijg je aangeleverd van de andere afdelingen.

**Medewerker:** ja, klopt.

**Interviewer:** en jullie hebben die gegevens digitaal opgeslagen en op papier?

**Manager:** ja klopt en digitaal staan ze bij onze salarisadministrateur ADP.

**Medewerker:** ja en eh, de papieren dingen gaan in een afgesloten kast op onze afdeling en alleen wij kunnen daarbij.. alleen de directie heeft een reservesleutel.

**Manager:** maar, we hebben ook wel persoonsgegevens, en dan bedoel ik namen van medewerkers opgeslagen in een excelbestand en dit staat op een schijf waar alleen wij bij kunnen.

**Interviewer:** en het bewaren van die gegevens? Houden jullie je aan de bewaartermijnen?

**Manager:** ja, we houden ons aan de fiscale bewaartermijnen.

**Interviewer:** en zijn er los van ADP nog andere partijen waarmee jullie de persoonsgegevens delen?

**Manager:** nee.. alleen ADP.. alle systemen worden ook door ons beheert

**Interviewer:** hebben jullie een standaard beleid of procedures waarmee jullie rekening houden bij de verwerking van persoonsgegevens?

**Medewerker:** nee.. eigenlijk niet.. we hebben wel een keer een seminar gehad bij ADP over de AVG, maar meer niet..

**Manager:** ik heb trouwens wel nog een ding, we hebben natuurlijk ook debiteuren en crediteuren waar we gegevens van contactpersonen van hebben en eh, meestal voert inkoop/verkoop die in, maar soms doen wij dit ook..

**Interviewer:** ok, dus eh, naast de gegevens medewerkers, hebben jullie ook zicht op persoonsgegevens van contactpersonen van crediteuren en debiteuren?

**Mangager:** ja, klopt.

**Interviewer:** en eh, nog even terugkomend op de bewaartermijnen, houden jullie daar ook rekening mee wat betreft het e-mailverkeer?

**Medewerker:** de fiscale gegevens draai ik uit en sla ik op in de kast.. en de mail verwijder ik.

**Manager:** en moeten we nou iets met de privacyverklaring in onze e-mails?

**Interviewer:** ja, nouja, het verwijzen naar de privacyverklaring zou via de e-mailhandtekening kunnen.

**Manager:** ok..

**Interviewer:** nou, gelet op de tijd ga ik afronden.. ik heb nog een laatste vraag, wat zouden jullie graag terug willen zien in een nieuw privacy beleid?

**Medewerker:** nou, als ik twijfel over dingen, dan ga ik dat gewoon eerst navragen voor ik iets doe..

**Manager:** ja, maar eigenlijk doen wij bijna alles al omdat we sowieso aan strengere eisen moeten voldoen..

**Interviewer:** okee..

**Manager:** oh, ik heb hier die verklaring van ADP dat ze aan de hoogst haalbare standaard voldoen..

**Interviewer:** oh, ja, ik zal er zelf ook nog even naar kijken.. nou eh, als er verder geen vragen zijn vanuit jullie wil ik jullie bedanken voor jullie tijd en eh fijne dag nog.

**Manager:** nee, ik heb geen vragen meer..

**Medewerker:** nee, ik ook niet. Jij ook bedankt.

##### Interview 3

##### Interviewer: Rosaline Rodenburg Geïnterviewde: manager en medewerker afdeling Kwaliteit Opdrachtgever Datum en duur interview: 7 mei 2018, 15 minuten Doel interview: inzicht krijgen in de verwerking van persoonsgegevens binnen Opdrachtgever

**Interviewer**: goedemiddag, eh, eerst wil ik vragen of jullie het goed vinden dat ik het interview opneem zodat ik deze kan transcriberen om in mijn onderzoek te kunnen gebruiken. Ik zal in mijn onderzoek geen namen noemen, maar gewoon medewerker 1, 2, 3 omdat dit verder geen toegevoegde waarde heeft..

**Manager**: ja hoor, prima.

**Interviewer**: ok eh, de eerste vraag is wat is jullie functie?

**Medewerker**: ik maak kwaliteitsplannen, eh voorbereiding van wat de klant wil en eh ik zit zelf een beetje in een uniek traject nu want de manager is van plan om over 2,5 jaar met pensioen te gaan dus ik ga een aantal werkzaamheden van hem overnemen.. eh, gericht op de certificering voor milieu en kwaliteit. Ik denk dat dat in een notendop het wel is wat mij betreft.. misschien eh, een mooi ezelsbruggetje naar de manager.

**Manager**: ik heb twee functies, ik ben verantwoordelijk voor eh het klantensysteem en daarnaast ben ik verantwoordelijk voor eh alle procedures binnen Opdrachtgever.

**Interviewer**: ja, eh, waaronder de nieuwe privacy procedures dus?

**Manager**: ja.

**Interviewer**: ok eh, en van welke groep personen verwerken jullie persoonsgegevens?

**Medewerker**: op de meetrapporten staat een naam van de medewerker die dit gemeten heeft en die worden verwerkt in het systeem en die worden opgeslagen..

**Interviewer**: ok.. dus echt alleen namen? Of ook e-mailadressen, telefoonnummers..?

**Medewerker**: nee, niet door mij.. Of eh, gegevens van de contactpersonen van klanten.. dat is gewoon eh, naam, e-mail, dat staat in outlook.. Meer niet he manager?

**Manager**: nee, het is alleen eh, medewerkers die paraferen documenten voor de klant alleen eh, die documenten gaan dus wel naar buiten toe.

**Interviewer**: en de medewerkers zijn hier van op de hoogte?

**Manager**: een deel weet het.. maar ik denk dat we het daar over moeten hebben.. mij verbaasde het dat die documenten naar buiten gaan..

**Interviewer**: en is het echt noodzakelijk dat die documenten naar buiten gaan?

**Manager**: nee..

**Interviewer**: en met welk doel worden ze dan gedeeld?

**Manager**: ja, dat is zo afgesproken.. 15 jaar geleden deed ik deze zelfde functie.. toen heb ik het verboden.. maar klanten willen weten of de personen die de door hun bestelde producten gemaakt hebben wel de juiste opleidingen en certificaten enzo heeft, daarom wordt dit gedocumenteerd en gedeeld..

**Interviewer**: ja, nouja in principe mag dit denk ik wel gewoon, maar alleen als je er een gerechtvaardigd belang bij hebt als bedrijf.. maar het is aan het bedrijf om te kiezen of ze door willen gaan met het delen van die documenten of niet..

**Manager**: ja, kijk voor de kwaliteitsmedewerkers vind ik het logisch en vanzelfsprekend dat zij zulke kwaliteitsdocumenten ondertekenen en dat hun naam daar bij genoemd wordt.. maar voor de productiemedewerkers vind ik het niet passen.

**Interviewer**: ja, je kan inderdaad ook kijken naar of het in de lijn van de arbeidsovereenkomst past, of het bij de hoofdwerkzaamheden past..

**Medewerker**: wat me wel te binnen schiet, we krijgen wel eh, kopen eh van onze toeleveranciers materialen en eh, daar komen ook certificaten bij en daar staan ook wel namen bij van ja eh, voor mij onbekende, waar je dat van inkoopt, die certificaten die sturen wij wel weer rechtstreeks naar onze klant..

**Interviewer**: ja ehhh, dus je ontvangt certificaten met namen van een ander bedrijf?

**Medewerker**: ja, van toeleveranciers.

**Interviewer**: ja, ok. Dat is in principe gewoon de verantwoordelijkheid van degene die het certificaat in eerste instantie deelt, zij verzamelen die persoonsgegevens en delen die..

**Medewerker**: ok, duidelijk.

**Interviewer**: ehm, en de persoonsgegevens die jullie verwerken, verzamelen jullie die zelf?

**Manager**: we vragen ze op aan desbetreffende personen.

**Interviewer**: en waar worden die gegevens opgeslagen?

**Manager**: eh, digitaal, in een Windows omgeving.

**Interviewer**: en het is een beveiligde omgeving?

**Manager**: ja, onbevoegden kunnen er niet zomaar bij.

**Interviewer**: ehmm, en houden jullie rekening met de bewaartermijnen van persoonsgegevens?

**Manager**: ik heb voor al mijn documenten bewaartermijnen waar ik me aan hou, dit zijn dan de termijnen die uit de wet volgen.

**Medewerker**: ja eh, ik volg dezelfde bewaartermijnen.

**Interviewer**: en eh, worden de gegevens die jullie verzamelen gedeeld met externe partijen?

**Manager**: ja, in theorie wel.. in theorie eh worden deze gedeeld met de klanten..

**Medewerker**: ja eh, op de meetrapporten staan namen van de productiemedewerkers

**Interviewer**: en is het toevoegen van de naam van die productiemedewerkers echt noodzakelijk?

**Medewerker**: ja, dat is wel een goede inderdaad..

**Interviewer**: nou, eh, uit het interview heb ik het al een beetje opgemaakt, maar toch de vraag ehm zijn er bepaalde procedures en/of spraken die jullie volgen bij het verwerken van persoonsgegevens?

**Manager**: nee.. nouja, wij houden ons dus wel aan die bewaartermijnen, maar echt een procedure hebben we niet.

**Interviewer**: ok.. en eh dan de laatste vraag alweer.. hebben jullie nog tips voor mij wat betreft een nieuwe beleid?

**Medewerker**: ja eh, gewoon de basis dingen eigenlijk, waar moet ik op letten, waar moet ik me bewust van zijn..

**Manager**: nee eh, ik denk dat ik alles al wel met je besproken heb

**Interviewer**: ok.. hebben jullie zelf nog vragen?

**Medewerker**: nee eh, ik was zelf wel benieuwd naar tips, maar die volgen dan nog wel denk ik

**Interviewer**: ja, en als er dringende vragen zijn kan je ze altijd even stellen.. nou eh, bedankt voor jullie tijd.

**Medewerker**: ja, succes.

**Manager**: ja, ik ben benieuwd.

##### Interview 4

##### Interviewer: Rosaline Rodenburg Geïnterviewde: manager Productie en tevens General Manager Opdrachtgever Datum en duur interview: 3 mei 2018, 19 minuten Doel interview: inzicht krijgen in de verwerking van persoonsgegevens binnen Opdrachtgever

**Interviewer:** goedemiddag, voor we beginnen wil ik vragen of het goed is dat ik het interview opneem zodat ik deze kan transcriberen en gebruiken voor mijn onderzoek.. ehmm, ja, ik zal je naam verder niet noemen in mijn onderzoek omdat dit geen toegevoegde waarde heeft..

**Geïnterviewde:** ja hoor, prima.

**Interviewer:** ok, ja ik heb van tevoren een vragenlijst gemaakt en eh ik wil graag beginnen met een kleine toelichting op jouw functie en bijbehorende werkzaamheden.

**Geïnteviewde:** nou eh, ik ben een van de general managers he, dat klinkt heel mooi in het engels, haha. Ik geef eh functioneel leiding aan de assemblage afdeling, dus ik ben eigenlijk productieleider voor die afdeling en eh samen met mijn man zijn we ook verantwoordelijk voor de hele groepsaansturing, dus voor alle andere afdelingen.

**Interviewer:** ja, ja..

**Geïnterviewde:** dat is zeg maar globaal mijn taak.. de hoofdtaak is echt wel het aansturen van de assemblage en voor de andere taken hebben we gelukkig een aantal managers zitten die verantwoordelijkheden op zich nemen.. maar eh, wij zijn uiteindelijk hoofdverantwoordelijke.

**Interviewer:** hmhm, precies, ja duidelijk.. het interview zal verder gericht zijn op de verwerking van persoonsgegevens, dus eh waar ze vandaan komen en wat ermee gedaan wordt.. ehm, van wie verwerk jij persoonsgegevens?

**Geïnterviewde:** nou eh, ik krijg verlofbriefjes van werknemers, ziekmeldingen, eh werkorders die de fabriek in gaan.. ja eh de gegevens van de werknemers, dus eh, NAW-gegevens, e-mail, dat is het eigenlijk..

**Interviewer:** ja, dus niet veel gegevens maar wel veel doelen?

**Geïnterviewde:** ja eh klopt.

**Interviewer:** en die gegevens verwerk je ook echt allemaal zelf?

**Geïnterviewde** Ehm nou ziekmeldingen geef ik door aan personeelszaken en de werkorders worden geprint, verdeel ik over de afdelingen op de werkvloer en een medewerker tekent die werkorder af, die worden volgens mij voorzien van initialen en eerste letter van de achternaam.. verlofbriefjes worden echt bij mij ingeleverd.. weet niet of je die wel eens gezien hebt zo’n briefje?

**Interviewer:** ja volgens mij wel..

**Geïnterviewde:** ja en eh dit is dus zo’n werkorder en dit is het zo’n verlofbriefje. Ja sommige medewerkers vertellen zelf dat ze griep hebben en de ander zegt weer alleen dat ie ziek is, maar eh daar doen we verder niks mee omdat dat niet mag

**Interviewer:** ja, nouja als ze dat zelf graag willen vertellen.. ehm, je hebt het over het doorgeven van ziekmeldingen aan personeelszaken.. welke persoonsgegevens sla je echt zelf op en hoe?

**Geïnterviewde:** jaaa.. dat heb ik natuurlijk wel, ik laat sowieso alles in mijn mail staan eigenlijk en eh de rest staat op een server dus niet op mijn eigen apparaat.. maar eh die server is wel in eigen beheer..

**Interviewer:** ja ok.. dus je e-mails bewaar je eigenlijk eeuwig?

**Geïnterviewde:** ja, ik bewaar alles totdat de medewerker ICT zegt dat ik mijn mailbox weer eens op moet schonen.

**Interviewer:** ja, mailboxen opschonen is wel een dingetje voor de meeste personen haha..

**Geïnterviewde:** ja en eh, ik krijg natuurlijk wel gegevens van sollicitanten ook in mijn mail en eh nu staan er echt gegevens van 5 jaar geleden nog in denk ik..

**Interviewer:** ja, dat is straks dus inderdaad niet de bedoeling..

**Geïnterviewde:** en eh, kan je dat ook automatisch doen dat verwijderen?

**Interviewer:** ja, dat weet ik eigenlijk niet zeker.. er zijn wel snufjes voor maar wat en hoe precies durf ik niet te zeggen..

**Geïnterviewde:** ja, want ik kan me gewoon voorstellen dat ik dingen van 5 jaar geleden kan vinden.. ik denk dat we binnen het hele bedrijf best wel eens wat beter om mogen gaan met het bewaren van dingen en ook het versturen van e-mails via CC wordt hier echt teveel gedaan.

**Interviewer:** ja, dat is bij veel bedrijven wel een ergernis die CC.. ik heb daar ook niet direct een oplossing voor.. in principe mag het natuurlijk ook gewoon onder de AVG, dus op basis daarvan is er geen probleem.. ehmm.. nu we het toch over rondsturen hebben, een mooi bruggetje naar mijn volgende vraag. Zijn er externe partijen waarmee je persoonsgegevens deelt?

**Geïnterviewde:** ja eh, de accountant, de bedrijfsarts, maar daar zijn al dingen mee geregeld

**Interviewer:** oke..

**Geïnterviewde:** en intern delen mag wel gewoon toch?

**Interviewer:** ja klopt, daarvoor hoef je geen overeenkomsten af te sluiten.

**Geïnterviewde:** oh ja en ik heb natuurlijk te maken met de gegevens van uitzendkrachten, maar die ontvang ik van het uitzendbureau.. dus daar deel ik zelf niet mee maar dat doen zij toch?

**Interviewer:** ja, een uitzendbureau is zelf verwerkingsverantwoordelijke.. Nou eh, ik had eigenlijk nog de vraag of er standaard procedures zijn voor de omgang met persoonsgegevens binnen Opdrachtgever, maar uit het interview en de interviews die ik al heb gehad bleek al dat die er niet zijn.. klopt dat?

**Geïnterviewde:** ja, dat klopt, we hebben tot nu toe eigenlijk nooit echt iets gedaan met privacy enzo..

**Interviewer:** ok, duidelijk.. en ehm, mijn laatste vraag: wat zou je graag terug willen zien in een nieuw privacybeleid?

**Geïnterviewde:** nou eh, hoe we met gegevens omgaan en waar we op moeten letten

**Interviewer:** ja, gewoon de basis dus eigenlijk?

**Geïnterviewde:** ja, inderdaad..

**Interviewer:** heb jij verder nog vragen?

**Geïnterviewde:** ja, ik heb bijvoorbeeld twitter waar ik dingen post van het bedrijf enzo op een beurs bijvoorbeeld en dan plaats ik er een foto van een medewerker bij, mag dit eigenlijk?

**Interviewer:** nou, het plaatsen van foto’s gaat meer richting auteursrecht eigenlijk en dan het portretrecht.. ehm, ja als je zonder opdracht van die medewerker een foto maakt en verspreidt, mag dat in principe gewoon.. de medewerker heeft alleen wel het recht om aan te geven dat hij of zij dit niet wil en dan is het de vraag welke belangen zwaarder wegen.. ehm ja, persoonlijk zou ik als een medewerker het niet wil daar gewoon gehoor aan geven.

**Geïnterviewde:** ja ok, de foto’s worden wel echt bij openbare gelegenheden gemaakt, wat ik al zei bij een beurs bijvoorbeeld, dus ik neem aan dat de medewerker het dan wel goed vindt.

**Interviewer:** ja inderdaad en anders hoor je het wel, nou eh dan ga ik afronden.. bedankt voor je tijd en eh als er vragen zijn hoor ik het wel.

**Geïnterviewde:** ja, hetzelfde geldt voor jou, als je nog dingen moet weten ofzo, gewoon vragen.

**Interviewer:** ja, zal ik doen, nou, fijne vakantie alvast.

1. Rijksoverheid*, handleiding AVG*, p. 62 [↑](#footnote-ref-1)
2. Richtlijn 95/46/EG [↑](#footnote-ref-2)
3. Overweging 6 AVG [↑](#footnote-ref-3)
4. De Vries & Goudsmit, *NJB* 2016/1077, afl. 22, p. 1071-1125 [↑](#footnote-ref-4)
5. <https://www.nijdra.eu/nl/nijdra-group> “Over Nijdra Group” [↑](#footnote-ref-5)
6. Zie bijlage 2 [↑](#footnote-ref-6)
7. Bastiaans, Bb 2018/24, “Privacy in een nieuw jasje: een vergelijking van beschermingsniveau tussen de Wbp en de AVG” [↑](#footnote-ref-7)
8. [www.vijverbergjuristen.nl](http://www.vijverbergjuristen.nl) zoek op: “Bewerkersovereenkomst naar verwerkersovereenkomst”: Waarom deze bron? [↑](#footnote-ref-8)
9. Bijlage 8 en persoonlijke communicatie met medewerkers van alle genoemde afdelingen [↑](#footnote-ref-9)
10. Zie: bijlage 7 [↑](#footnote-ref-10)
11. Overweging 1 AVG [↑](#footnote-ref-11)
12. [www.autoriteitspersoonsgegevens.nl](http://www.autoriteitspersoonsgegevens.nl) “Mag u persoonsgegevens verwerken?” [↑](#footnote-ref-12)
13. Versmissen, Terstegge & Krijgsman 2017, p. 63 [↑](#footnote-ref-13)
14. [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) “wanneer mag u zich baseren op de grondslag uitvoering overeenkomst” [↑](#footnote-ref-14)
15. Versmissen, Terstegge & Krijgsman 2017, p. 60 [↑](#footnote-ref-15)
16. Versmissen, Terstegge & Krijgsman 2017, p. 60 [↑](#footnote-ref-16)
17. [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) “hoe weet u of u persoonsgegevens mag verwerken?” [↑](#footnote-ref-17)
18. Versmissen, Terstegge & Krijgsman 2017, p. 61 [↑](#footnote-ref-18)
19. Versmissen, Terstegge & Krijgsman 2017, p. 61 [↑](#footnote-ref-19)
20. [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) “hoe weet u of u persoonsgegevens mag verwerken?” [↑](#footnote-ref-20)
21. Engelfriet, Meij & Kager 2017, p. 46 [↑](#footnote-ref-21)
22. <https://autoriteitpersoonsgegevens.nl/> “verantwoordingsplicht” [↑](#footnote-ref-22)
23. Rijksoverheid, *Handleiding AVG*, p. 21 [↑](#footnote-ref-23)
24. Rijksoverheid, *handleiding AVG*, p. 51 [↑](#footnote-ref-24)
25. Berkvens e.a. 2018, p. 43 [↑](#footnote-ref-25)
26. Berkvens e.a. 2018, p. 37 [↑](#footnote-ref-26)
27. Omdat dit niet van toepassing is voor Nijdra, is deze niet opgenomen in het standaard verwerkingsregister. [↑](#footnote-ref-27)
28. Rijksoverheid*, handleiding AVG*, p. 57 [↑](#footnote-ref-28)
29. Berkvens e.a. 2018, p. 129 [↑](#footnote-ref-29)
30. Wp 29, gegevensbeschermingseffectbeoordeling, p. 5 [↑](#footnote-ref-30)
31. Wp 29, gegevensbeschermingseffectbeoordeling, p. 7 [↑](#footnote-ref-31)
32. Rijksoverheid, *handleiding AVG*, p. 58 [↑](#footnote-ref-32)
33. <https://autoriteitpersoonsgegevens.nl> “Data protection impact assessment” [↑](#footnote-ref-33)
34. Berkvens e.a. 2018, p. 131 [↑](#footnote-ref-34)
35. <https://autoriteitpersoonsgegevens.nl> “Data protection impact assessment” [↑](#footnote-ref-35)
36. Wp248, p. 7 [↑](#footnote-ref-36)
37. Engelfriet, Meij & Kager 2017, p. 152 [↑](#footnote-ref-37)
38. Rijksoverheid*, handleiding AVG*, p. 75 [↑](#footnote-ref-38)
39. Engelfriet, Meij & Kager 2017, p. 70 [↑](#footnote-ref-39)
40. Rijksoverheid, *Handleiding AVG*, p. 76 [↑](#footnote-ref-40)
41. Rijksoverheid, *Handleiding AVG*, p. 76 [↑](#footnote-ref-41)
42. Berkvens e.a. 2018, p. 95 [↑](#footnote-ref-42)
43. Berkvens e.a. 2018, p. 95 [↑](#footnote-ref-43)
44. Rijksoverheid, *Handleiding* *AVG*, p. 75 [↑](#footnote-ref-44)
45. Rijksoverheid, *Handleiding* *AVG*, p. 75 [↑](#footnote-ref-45)
46. Rijksoverheid, *Handleiding* *AVG*, p. 75 [↑](#footnote-ref-46)
47. Rijksoverheid, *Handleiding* *AVG*, p. 75 [↑](#footnote-ref-47)
48. <https://europadecentraal.nl> “privacy by design and by default” [↑](#footnote-ref-48)
49. Rijksoverheid, *handleiding* *AVG*, p. 61 [↑](#footnote-ref-49)
50. Berkvens e.a. 2018, p. 123 [↑](#footnote-ref-50)
51. Berkvens e.a. 2018, p. 124 [↑](#footnote-ref-51)
52. Overweging 81 AVG [↑](#footnote-ref-52)
53. Van de Bunt & Strijbos, *NJB* 2018/357, afl. 7, p. 479 [↑](#footnote-ref-53)
54. Engelfriet, Meij & Kager 2017 p. 127 [↑](#footnote-ref-54)
55. Versmissen, Terstegge & Krijgsman 2017, p. 28 [↑](#footnote-ref-55)
56. Rijksoverheid, *Handleiding* *AVG*, p. 32 [↑](#footnote-ref-56)
57. Rijksoverheid, *Handleiding AVG*, p. 33 [↑](#footnote-ref-57)
58. Rijksoverheid, *Handleiding* *AVG*, p. 32 [↑](#footnote-ref-58)
59. Overweging 81 AVG [↑](#footnote-ref-59)
60. Rijksoverheid, *Handleiding* *AVG*, p. 64-66 [↑](#footnote-ref-60)
61. Berkvens e.a. 2018, p. 55 [↑](#footnote-ref-61)
62. Wp 250, p. 23 [↑](#footnote-ref-62)
63. Wp 250, p. 23 [↑](#footnote-ref-63)
64. Wp 250, p. 9  
     Berkvens e.a. 2018, p. 57 [↑](#footnote-ref-64)
65. Berkvens e.a. 2018, p. 57 [↑](#footnote-ref-65)
66. Art. 9 lid 1 AVG en overweging 51 AVG [↑](#footnote-ref-66)
67. Relevante passages zijn geel gemarkeerd. [↑](#footnote-ref-67)
68. Ter vervanging van het interview met de medewerker personeelszaken zijn er informele gesprekken gevoerd om informatie te verzamelen. [↑](#footnote-ref-68)
69. Bijlage 8 [↑](#footnote-ref-69)
70. Onder medewerkers wordt verstaan: sollicitanten, uitzendkrachten, stagiaires en werknemers. [↑](#footnote-ref-70)
71. De persoonsgegevens zoals weergegeven in de tabel in paragraaf 4.2.1. [↑](#footnote-ref-71)
72. De persoonsgegevens zoals weergegeven in de tabel in paragraaf 4.2.1. [↑](#footnote-ref-72)
73. Medewerker personeelszaken en General Manager, persoonlijke communicatie, 24 mei 2018 [↑](#footnote-ref-73)
74. Groen gemarkeerd [↑](#footnote-ref-74)
75. Daar het uitvoeren van een dossieronderzoek niet mogelijk was, zijn de te nemen maatregelen enkel gericht op de informatie die ik van medewerkers ontvangen heb en de documenten en fysieke opslagsystemen die mij getoond zijn. [↑](#footnote-ref-75)
76. *Rijksoverheid, Handleiding AVG, hfdst. 5* [↑](#footnote-ref-76)
77. Rijksoverheid, *Handleiding* *AVG*, p. 51 [↑](#footnote-ref-77)
78. Zie par. 3.1.3. onder “Verwerkingsregister” [↑](#footnote-ref-78)
79. [www.metaalunie.nl](http://www.metaalunie.nl) *“AVG-check”* [↑](#footnote-ref-79)
80. Zie par. 3.1.3 onder “iInformatieplicht/Privacyverklaring” [↑](#footnote-ref-80)
81. Zie pag. 3 van privacyverklaring in bijlage [↑](#footnote-ref-81)
82. Hiervoor wordt er gekeken naar de bepalingen zoals genoemd in par. 3.1.3 onder “verwerker, verwerkingsverantwoordelijke en medeverantwoordelijke” en het schema in bijlage 1 [↑](#footnote-ref-82)
83. Op grond van de Arbowet. [↑](#footnote-ref-83)
84. [www.vangelderadvocaten.nl](http://www.vangelderadvocaten.nl) “is een verwerkersovereenkomst met de arbodienst verplicht” [↑](#footnote-ref-84)
85. [www.uwv.nl](http://www.uwv.nl) “uw contact met uwv wijzigt niet door nieuwe avg” [↑](#footnote-ref-85)
86. [www.accountancyvanmorgen.nl](http://www.accountancyvanmorgen.nl) “AVG en de rol van de accountant: Verwerker, verantwoordelijke of beide? Blijft er onduidelijkheid?” [↑](#footnote-ref-86)
87. [www.nba.nl](http://www.nba.nl) “Reactie NBA op berichtgeving Accountancy Vanmorgen inzake de AVG” [↑](#footnote-ref-87)
88. [www.adp.nl](http://www.adp.nl) zoek op “Corporate binding rules” [↑](#footnote-ref-88)
89. In dit onderzoek is ervoor gekozen om zich te richten op de plichten van de verwerkingsverantwoordelijke, de plichten van de verwerker worden daarom niet behandeld. [↑](#footnote-ref-89)
90. Model VIII.5.65 [↑](#footnote-ref-90)
91. Zie par. 3.1.4 [↑](#footnote-ref-91)
92. Rijksoverheid, Handleiding AVG, p. 62  
     overweging 78 AVG [↑](#footnote-ref-92)
93. Art. 83 lid 4 AVG [↑](#footnote-ref-93)
94. Art. 83 lid 4 AVG [↑](#footnote-ref-94)
95. Art. 83 lid 5 AVG [↑](#footnote-ref-95)
96. Art. 83 lid 5 AVG [↑](#footnote-ref-96)
97. Art. 84 lid 1 AVG [↑](#footnote-ref-97)