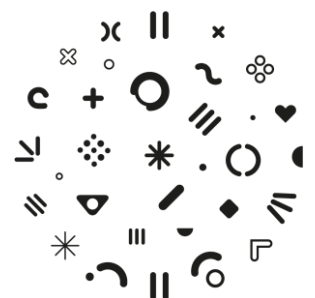




## Whitepaper: De AVG

Privacy is er voor jou. En niet andersom

Datum: 22 maart 2018



Werk is er voor jou.  
En niet andersom



# Inhoud

1. Vooraf
2. Inleiding
3. In 10 stappen
4. Conclusie

# 1. Vooraf

We zien dat de AVG voor organisaties onzekerheid met zich meebrengt. Maar ook in de Wet bescherming persoonsgegevens (Wbp) was de privacywetgeving al streng. De AVG breidt dit iets uit en legt verantwoordelijkheden in enkele gevallen net anders, maar enorm groot zijn de verschillen niet.

Het basis uitgangspunt is dat de privacy van het individu moet worden gerespecteerd. De mens centraal is het uitgangspunt. Als eelloo vinden we dat een goed uitgangspunt. De belangrijkste reden voor stress vormen de hoogte van de boetes. Deze zijn fors hoger dan bij de Wbp, maar bij een goede voorbereiding op deze wetgeving is de kans op boetes niet zo groot.

## 2. Inleiding

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG, internationaal ook wel GDPR genoemd) van toepassing. Deze privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) vervalt hiermee.

Deze nieuwe wet betekent een uitbreiding van de privacyrechten en legt meer verantwoordelijkheden neer bij organisaties. Eelloo krijgt veel vragen over dit onderwerp van klanten. Bijvoorbeeld wat het effect is van deze nieuwe wetgeving op organisaties die persoonsdossiers verwerken voor selectie, ontwikkeling, loopbaan, outplacement en mobiliteit. Een andere vraag die we krijgen is hoe organisaties zich hierop kunnen voorbereiden en hoe eelloo zelf omgaat met deze wetgeving. Welke maatregelen neemt eelloo en welke moeten organisaties zelf nemen?

Deze whitepaper geeft hier voor een groot deel antwoord op. We delen graag onze inzichten. Daar moeten twee kanttekeningen bij worden geplaatst. We zien dat er vanuit Europa op punten nog uitwerking wordt gemaakt van de wetgeving en dat het logischerwijs nog aan jurisprudentie ontbreekt, dus wat de beste manier is om bij deze wetgeving aan te sluiten is nog niet overal bekend. Daarnaast is het voor elke organisatie van belang ook zelf te onderzoeken wat gegeven de eigen specifieke situatie nodig is.

# 3. In 10 stappen

## Waar moet rekening mee worden gehouden?

De Autoriteit Persoonsgegevens biedt een 10 stappenplan dat gevolgd kan worden ter voorbereiding op de AVG:

1. Bewustwording
2. Recht van betrokkenen
3. Overzicht van verwerkingen
4. Data protection impact assessment (DPIA)
5. Privacy by design & privacy by default
6. Functionaris gegevensbescherming
7. Meldplicht datalekken
8. Verwerkersovereenkomsten
9. Leidende toezichthouder
10. Toestemming

### Meer informatie?

De bron van bovenstaande informatie vind je [hier](#).

We gaan in op elk van deze zaken, maar eerst lichten we twee begrippen kort toe die ook in de huidige wetgeving belangrijk zijn: de verwerkingsverantwoordelijke van persoonsgegevens en de verwerker van persoonsgegevens.

### Verwerkingsverantwoordelijke vs. verwerker

In veel gevallen is het onduidelijk wie de eigenaar van persoonsgegevens is. Is dat de persoon zelf, is het een organisatie die gegevens verwerkt en welke dan? De wet spreekt daarom van verantwoordelijkheden.

Er is een verwerkingsverantwoordelijke van persoonsgegevens en er is een verwerker. De verwerkingsverantwoordelijke is die partij die bepaalt wat het doel is van de verwerking van persoonsgegevens en op welke wijze deze persoonsgegevens verwerkt mogen worden. De bewerker is de partij die hier uitvoering aan geeft. In de AVG wordt de term bewerker niet meer gebruikt. Men spreekt van een verwerker, maar het principe is hetzelfde. Bedenk dus steeds wie het doel van de verwerking bepaalt en bespreek dit als dat niet duidelijk is.

Eelloo is veelal verwerker van persoonsgegevens voor haar klanten. De klant bepaalt immers welk assessment er voor een persoon wordt ingezet, welke mobiliteitsoplossingen worden geboden of welke leeromgeving beschikbaar wordt gesteld. Eelloo voert dit uit.

Eelloo gebruikt zelf ook verwerkers. Dit is ook aangegeven in onze contracten. Eelloo gebruikt bijvoorbeeld Detron voor de hosting van de applicaties en de database. Zo ontstaat er dus een keten van verwerkingsverantwoordelijken en verwerkers.

In de onderstaande beschrijving van de 10 stappen komen de begrippen verwerkingsverantwoordelijke en verwerker vaak terug:

## 1. BEWUSTWORDING

Bewustwording start met het in kaart brengen van de impact van de AVG op de organisatie en het maken van beleid. Bij het implementeren van beleid is bewustwording van medewerkers misschien wel de belangrijkste component. Alle medewerkers die te maken hebben met het beleid moeten weet hebben van het beleid en het beleid op juiste wijze toepassen. Dat klinkt gemakkelijk, maar in de praktijk blijkt het vaak dat fouten die ontstaan hun oorzaak vinden in menselijk handelen en dat beleid niet aansluit op de praktijk of andersom.

Eelloo heeft al jaren het ISO27001:2013 certificaat. Dit managementsysteem gaat over informatiebeveiliging en is dus sterk verbonden met de omgang met privacygevoelige gegevens. Bewustwording is een belangrijk onderdeel van dit systeem. Zo doorlopen medewerkers van eelloo jaarlijks e-learnings op het gebied van informatiebeveiliging en privacy en bespreken we gezamenlijk de valkuilen die we zien. Door de gehele organisatie hierbij te betrekken zorgen we dat ook iedereen zich bewust is van de uitdagingen die wij als organisatie ervaren.

Er zijn meerdere manieren om medewerkers bewust te maken van deze privacywetgeving. Het kost tijd om dit op een goede manier te doen. Zoals de Autoriteit Persoonsgegevens (hierna AP) zelf aangeeft: *“Bedenk dat de AP uw organisatie sancties kan opleggen van maximaal 20 miljoen euro of 4% van uw wereldwijde omzet als u zich niet aan de nieuwe privacywetgeving houdt.”* De bewustwordingscomponent kost tijd, maar zorgt er ook voor dat het risico op deze boetes wordt verkleind.

## 2. RECHT VAN DE BETROKKENEN

In de rechten van betrokken veranderen in grote lijnen de volgende zaken:

Daarnaast gelden zagezegd veel rechten die ook in de Wbp al gelden:

- Recht tot vergetelheid
- Recht op dataportabiliteit
- Recht op inzage
- Recht op rectificatie en aanvulling
- Recht op beperking van verwerking
- Recht op een menselijk blik bij besluiten
- Recht op bezwaar
- Recht op duidelijke informatie

Deze rechten worden toegelicht:

### Recht tot vergetelheid

In de Wbp was er al het recht tot correctie en verwijdering van feitelijk onjuiste, onvolledige gegevens of het verwijderen van gegevens die in strijd met de wet worden verwerkt. Het individu kan dit verzoek doen en de verwerkingsverantwoordelijke zal hier gehoor aan moeten geven. In de AVG gaat dit een grote stap verder. Het individu mag vragen om “vergeten” te worden. Dit is niet meer beperkt tot het verwijderen van objectief onjuiste gegevens, onvolledige gegevens of gegevens die niet ter zake doen. De vraag is natuurlijk op welke wijze dit verzoek wordt afgehandeld.

Mocht een kandidaat/medewerker bij eelloo het verzoek doen om “vergeten” te worden dan zal eelloo dit verzoek aan de verwerkingsverantwoordelijke overbrengen. De verwerkingsverantwoordelijke moet dan bepalen of de gegevens mogen worden verwijderd. Als dit bepaald is, zal eelloo de verwerkingsverantwoordelijke ondersteunen bij de uitvoering van het verzoek.

## Wanneer wel verwijderen

Hierbij gelden de volgende stelregels, volgens de AP: *Het recht op vergetelheid geldt niet altijd. Alleen in de volgende situaties in het recht op vergetelheid van toepassing:*

- **Niet meer nodig**  
*De organisatie heeft de persoonsgegevens niet meer nodig voor de doeleinden waarvoor de organisatie ze heeft verzameld of waarvoor de organisatie ze verwerkt.*
- **Onrechtmatige verwerking**  
*De organisatie verwerkt de persoonsgegevens onrechtmatig. Bijvoorbeeld omdat er geen wettelijke grondslag is voor de verwerking.*
- **Intrekken toestemming**  
*De betrokkene heeft eerder (uitdrukkelijke) toestemming gegeven aan de organisatie voor het gebruik van zijn gegevens, maar trekt die toestemming nu in.*
- **Wettelijk bepaalde bewaartermijn**  
*De organisatie is wettelijk verplicht om de gegevens na bepaalde tijd te wissen.*
- **Bezwaar**  
*De betrokkene maakt bezwaar tegen de verwerking. Er geldt op grond van artikel 21 van de AVG een absoluut recht van bezwaar tegen direct marketing. En een relatief recht van bezwaar als de rechten van de betrokkene zwaarder wegen dan het belang van de organisatie om de persoonsgegevens te verwerken.*
- **Kinderen**  
*De betrokkene is jonger dan 16 jaar en de persoonsgegevens zijn verzameld via een app of website ('dienst van de informatiemaatschappij').*

## Wanneer niet verwijderen?

Er kunnen redenen zijn waarom er aan dit verzoek niet direct tegemoet wordt gekomen. De AP noemt hier ook voorbeelden van ([lees meer](#)). Bijvoorbeeld omdat de gegevens vanuit een wettelijke taak of algemeen belang worden verwerkt. Ook is het niet de bedoeling dat iemand door het recht op vergetelheid sporen van crimineel gedrag kan wissen.

Als we dit recht op vergetelheid toepassen op de praktijk, dan kan een verwerkingsverantwoordelijke het recht om een assessmentdossier te verwijderen moeilijk weigeren, maar dat betekent veelal wel dat de opdrachtgever hiervan op de hoogte gesteld zal worden. Het bewaren van basisgegevens is soms wel nodig om aan wettelijke verplichtingen te kunnen voldoen.

Eelloo heeft zich voorbereid op het 'vergeten' van kandidaatsgegevens. Dit doen we op verzoek al enkele jaren. We zorgen ervoor dat het dossier van de kandidaat volledig wordt *gescrambled* zodanig dat niet meer bekend is welke kandidaat het betreft. Desgewenst doen we dit structureel voor alle kandidaten, na de bewaarperiode. Wel kunnen wij in het kader van algemeen belang geanonimiseerde gegevens nog gebruiken om de kwaliteit van ons platform en instrumenten te verbeteren.



### **Recht op dataportabiliteit**

Het recht op dataportabiliteit klinkt wat technisch. Het is het recht om data over te kunnen dragen in een format dat in andere systemen ook te gebruiken is. Dit voorkomt een afhankelijkheid tussen betrokkene en verwerker/ verwerkingsverantwoordelijke. Geen twee systemen zijn gelijk. Het is belangrijk bij de overdraagbaarheid om gegevens in een gestructureerd, veelgebruikt en machineleesbaar format aan te leveren.

Eelloo sluit hierbij aan met CSV-exports en PDF-bestanden. Van één kandidaat of meerdere kandidaten kan het gehele dossier worden geëxporteerd naar een CSV-bestand. Dit kan de verwerkingsverantwoordelijke zelf doen. Daarnaast leveren we PDF-bestanden van het dossier. Een aantal rechten is zagezegd niet nieuw, maar neemt wel een belangrijke plek in bij de AVG:

### **Recht op inzage**

De betrokkene heeft te allen tijde het recht om inzicht te krijgen in zijn dossier.

*Zie AP: vraagt iemand om inzage, dan moet de organisatie diegene op een duidelijke en begrijpelijke manier laten weten of de organisatie zijn persoonsgegevens gebruikt, en zo ja:*

- *Om welke gegevens het gaat;*
- *Wat het doel is van het gebruik;*
- *Aan wie de organisatie de gegevens eventueel heeft verstrekt;*
- *Wat de herkomst is van de gegevens, als deze bekend is.*

We hebben eerder vragen gekregen over aantekeningen, voor bijvoorbeeld de uitvoering van assessments. Inzage in deze werkaantekeningen hoeft niet standaard gegeven te worden. Als deze aantekeningen in het dossier van het kandidaat worden gezet of worden overdragen aan anderen (bijv. per mail aan een collega), dan zal inzage in deze aantekeningen gegeven moeten worden, wanneer hierom wordt gevraagd.

Bij ons is door consultants eenvoudig in te stellen welke informatie zichtbaar is voor kandidaten en welke niet. Doet een kandidaat beroep op zijn recht op inzage, dan kan dus eenvoudig worden ingesteld dat de informatie die eerst alleen voor consultants in te zien was, nu ook voor kandidaten zichtbaar wordt.

### **Recht op rectificatie en aanvulling**

Mocht het zo zijn dat er onjuistheden of fouten in het dossier van de betrokkene staan, dan heeft de betrokkene het recht om deze te laten rectificeren / aan te vullen. Daarbij is het van belang om ook aan te geven aan welke derden deze informatie verstrekt is. Ook aan hen zal deze rectificatie/aanvulling moeten worden doorgegeven.

Het delen van de dossiers is een mogelijkheid in de systemen van eelloo. Hier wordt vaak ook toestemming voor gevraagd aan de kandidaat (in te regelen in het systeem). Hierdoor is het mogelijk om te zien aan wie rectificatie/aanvulling moet worden gemeld.

### **Recht op beperking van verwerking**

De AVG geeft betrokkenen in bepaalde situaties het recht om de verwerking van gegevens te beperken. Hierover zegt de AP het volgende:

## **Criteria recht op beperking van de verwerking**

*Het recht op beperking van de verwerking geldt in situaties die voldoen aan een van de volgende criteria:*

- **Gegevens zijn mogelijk onjuist**  
*Geeft iemand aan dat uw organisatie onjuiste persoonsgegevens gebruikt? Dan mag u deze gegevens niet gebruiken zolang u nog niet heeft gecontroleerd of de gegevens wel kloppen.*
- **Gegevens zijn niet meer nodig**  
*U heeft de persoonsgegevens niet meer nodig voor het doel waarvoor u ze heeft verzameld. Maar de betrokkene heeft de persoonsgegevens nog wel nodig voor een rechtsvordering. Bijvoorbeeld een juridische procedure waarbij hij betrokken is.*
- **De verwerking is onrechtmatig**  
*U mag bepaalde gegevens niet verwerken, maar de betrokkene wil niet dat u de gegevens wist. Bijvoorbeeld omdat hij de gegevens later nog wil opvragen.*
- **Betrokkene maakt bezwaar**  
*Maakt iemand bezwaar tegen het verwerken van zijn persoonsgegevens? Dan moet u stoppen met deze gegevens te verwerken. Tenzij u dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene. Zo lang nog niet duidelijk is of uw gronden zwaarder wegen, mag u de gegevens niet verwerken.*

Ook hier geldt dat bij het beperken van de verwerking, derden op de hoogte gesteld zullen worden, zoals de verwerkingsverantwoordelijke van gegevens. In de praktijk verwachten wij dat dit recht vaak aansluit bij het recht om vergeten te worden en bij het recht voor dataportabiliteit, omdat de te nemen acties hiermee overeenkomen. Het recht tot beperking van verwerking is echter wel een apart recht van betrokkenen, waar organisaties rekening mee moeten houden.

## **Recht op een menselijk blik bij besluiten**

Het is mogelijk dat er op basis van geautomatiseerde rekenregels online beslissingen worden genomen. We zien dit vaker bij grote recruitmenttrajecten. De betrokkene heeft het recht op een menselijke blik bij besluiten. In de praktijk kan dit betekenen dat er opnieuw naar het dossier gekeken zal worden. Als er geen andere gegevens worden aangedragen, dan is de kans groot dat de uitkomst hetzelfde zal zijn, maar het is goed om te weten dat een betrokkene dit verzoek kan indienen.

Er zijn ook situaties te bedenken dat er tot een ander besluit gekomen wordt, bijvoorbeeld als er gronden worden aangedragen die van belang zijn om mee te wegen bij deze persoon (bijv. een persoonlijke beperking) of die van belang zijn voor de situatie (bijv. een overlijden kort voor het assessment). De betrokkene mag altijd vragen om met een menselijke blik naar het dossier te laten kijken.

### **Recht van bezwaar**

Betrokkenen kunnen altijd bezwaar maken tegen verwerking. Hierop moeten betrokken actief worden gewezen.

*De AP: Maakt iemand bezwaar tegen het verwerken van zijn persoonsgegevens? Dan moet u stoppen met deze gegevens te verwerken. Tenzij u dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene. Of die te maken hebben met een rechtsvordering.*

In het privacy statement van eelloo worden betrokkenen al enkele jaren gewezen op het recht tot bezwaar. We zien in onze praktijk dat er op dit recht weinig tot geen aanspraak wordt gemaakt. Mocht iemand bezwaar hebben tegen verwerking dan zullen we de verwerkingsverantwoordelijke hiervan op de hoogte stellen en zullen we de verwerking staken, tenzij verwerkingsverantwoordelijke anders wenst te handelen.

### **Recht op duidelijke informatie**

In de AVG is er een informatieplicht. Het is verplicht om als verwerkingsverantwoordelijke duidelijk, expliciet en in begrijpelijke taal aan te geven op welke wijze gegevens worden verwerkt. In de praktijk is een privacyverklaring/statement hiervoor een geschikt middel. Eelloo heeft al een groot aantal jaren een eigen privacy statement in gebruik waarbij aan deze informatieplicht wordt voldaan.

Het voordeel van dit privacy statement is dat de betrokkenen toestemming geven voor verwerking door eelloo. Echter, eelloo is veelal verwerker van persoonsgegevens en niet de verwerkingsverantwoordelijke. Toestemming op het privacy statement van eelloo betekent niet dat er toestemming wordt verleend voor verwerking door verwerkingsverantwoordelijke. We gaan er vanuit dat de verwerkingsverantwoordelijke hier eigen afspraken over maakt met de betrokkenen. Het is ook overigens mogelijk een privacy statement van de klant te gebruiken in de systemen van eelloo.

### **3. OVERZICHT VAN VERWERKINGEN**

De AVG geeft aan dat er een overzicht moet worden gemaakt van alle verwerkingen van persoonsgegevens. Dit heet ook wel een "Register verwerkingsactiviteiten". Hierin wordt aangegeven welke gegevens worden verwerkt en met welk doel.

We denken hierbij vaak aan kandidaatsgegevens in een assessment-, ontwikkel- of mobiliteitstraject maar bedenk ook dat er andere systemen zijn in de organisatie, denk aan mailadressen voor marketing acties, salescontacten, een customer support systeem of de verwerking van dossiers van eigen medewerkers. Al deze gegevens moeten worden weergegeven op het Overzicht van verwerkingen.

Om het niet nodeloos ingewikkeld te maken voor kleine organisaties wordt er hierbij wel een onderscheid gemaakt tussen organisaties met meer dan 250 medewerkers en organisaties die kleiner zijn. Organisaties met minder dan 250 medewerkers hoeven alleen een register bij te houden als (zie AP):

### **Wanneer u persoonsgegevens verwerkt:**

- *Waarvan de verwerking niet incidenteel is. In de praktijk zijn verwerkingen zelden incidenteel. Denk bijvoorbeeld aan de persoonsgegevens van medewerkers die u verwerkt. Of van uw klanten, cliënten, patiënten of inwoners en/of;*
- *Die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie u persoonsgegevens verwerkt en/of;*
- *Die vallen onder de categorie bijzondere persoonsgegevens. Zoals gegevens over godsdienst, gezondheid en politieke voorkeur of strafrechtelijke gegevens. Bent u verplicht om een register van verwerkingsactiviteiten op te stellen? Dan moet u dit register kunnen verstrekken wanneer de Autoriteit Persoonsgegevens daar om vraagt.*

#### **Meer informatie?**

De bron van bovenstaande informatie vind je [hier](#).

Eelloo heeft een register opgesteld voor de eigen verwerking van gegevens. Over het algemeen zullen klanten van eelloo ook een eigen register moeten bijhouden omdat de verwerking niet incidenteel is. Dit zijn twee verschillende registers, omdat er sprake is van andere rollen in de verwerking van gegevens tussen de klant (vaak de verwerkingsverantwoordelijke) en eelloo (de verwerker) en de verwerkers van de klant hele andere kunnen zijn dan de verwerkers van eelloo.

#### **4. DATA PROTECTION IMPACT ASSESSMENT (DPIA)**

Er zijn 9 criteria die bepalen of er een DPIA moet worden uitgevoerd. Wie zich in het HRM werkveld bevindt zal veel te maken hebben met beoordelen van mensen op basis van persoonskenmerken. Dit is het eerste criterium en vaak zijn er meerdere criteria van toepassing. Er moet dus een DPIA worden uitgevoerd. Een DPIA is een vorm van risicoanalyse waarbij door de eigen organisatie wordt ingeschat hoe groot het risico is van de verwerking van persoonsgegevens. Verwerking is alleen gerechtvaardigd als risico's in kaart zijn gebracht en afdoende maatregelen worden getroffen, zodat de privacy van de betrokkene(n) niet nodeloos in gevaar komt. Bij twijfel kan de AP worden geraadpleegd.

#### **Raadpleeg de AP.**

Meer informatie over bovenstaande vind je [hier](#).

#### **5. PRIVACY BY DESIGN & PRIVACY BY DEFAULT**

*Privacy by design* betekent dat er bij het ontwerp van producten en diensten al wordt nagedacht over de verwerking van persoonsgegevens en hoe deze gegevens beschermd kunnen worden. Hierbij speelt ook dat gegevens niet langer worden bewaard dan nodig.

*Privacy by default* houdt in dat er al standaard technische en organisatorische maatregelen worden getroffen om de persoonsgegevens die niet noodzakelijk zijn niet te verwerken. Het is mogelijk om heel veel gegevens te verwerken die voor het doel van verwerking strikt genomen niet nodig zijn. Vanuit privacy oogpunt is het dan af te raden deze gegevens te verwerken.

Eelloo houdt in het ontwerp van haar software veel rekening met privacy van betrokkenen. Zo is er een persoonsdossier ontwikkeld waarbij kandidaten te allen tijde zelf kunnen inloggen en eigen gegevens kunnen raadplegen, is er standaard een beperking op de bewaartermijn van dossiers.

Deze bewaartermijn kan worden ingesteld per klant en staat standaard op een 1 jaar. Er worden door eelloo ook sterke technische en organisatorische maatregelen getroffen. Hierdoor is het resultaat van technische security tests (waaronder penetratietests) elk jaar erg positief en hebben wij al jaren het ISO27001:2013 certificaat. Voor meer details over de maatregelen die eelloo neemt, verwijzen we naar Service level, Techniek en beveiliging:

#### Onze maatregelen.

Meer details over de maatregelen die eelloo neemt vind je [hier](#).

## 6. FUNCTIONARIS GEGEVENSBESCHERMING

Een functionaris gegevensbescherming (FG) (of data protection officer) is een persoon die zorgdraagt voor beschikbaarheid en beveiliging van gegevens die de organisatie verwerkt en die naleving van de wetgeving binnen de organisatie monitort en bij afwijkingen optreedt ([lees meer](#)).

Het is een rol die binnen de Overheid en publieke organisaties verplicht is en die ook verplicht is bij organisaties die op grote schaal gegevens verwerken. Wie bijzondere persoonsgegevens verwerkt (over ras of geloof bijv.) is ook verplicht een FG te benoemen. Veel van onze klanten zullen een FG moeten benoemen. Voor een FG hoeft geen nieuwe medewerker te worden aangesteld. Een FG is een rol die ook bij bestaande medewerkers kan worden belegd. Eelloo heeft al jaren een FG, dit vormt een onderdeel van de ISO27001:2013 standaard.

## 7. MELDPLICHT DATALEKKEN

Gaat er wat mis en komt data breder beschikbaar dan zou moeten (bewust of onbewust), dan moet de verwerkingsverantwoordelijke hiervan melding maken bij de Autoriteit Persoonsgegevens. Er is een stappenplan voor meldingen te vinden op:

#### Stappenplan.

Het stappenplan voor het maken van meldingen vind je [hier](#).

Grotendeels is deze meldplicht gelijk aan de meldplicht van de Wbp. Het is iets uitgebreider omdat ook datalekken die zich in de eigen organisatie hebben voorgedaan, moeten worden gemeld bij de AP. Eelloo zal waar mogelijk ondersteunen om de benodigde informatie aan te leveren voor een juiste en tijdige melding.

## 8. VERWERKERSOVEREENKOMSTEN

Er moeten duidelijke afspraken worden gemaakt over de verwerking van gegevens. Dit wordt gedaan in een verwerkersovereenkomst (in de Wpb heette dit nog een bewerkersovereenkomst). In de Wbp was het aan de verwerkingsverantwoordelijke van gegevens om te bepalen of er een bewerkersovereenkomst moest worden afgesloten. In de AVG is de verwerkersovereenkomst verplicht. Het is aan de verwerkingsverantwoordelijke om zo'n overeenkomst af te sluiten bij het inschakelen van verwerkers.

Eelloo heeft al jaren een dergelijke standaardovereenkomst. Deze is in verband met de AVG licht gewijzigd. Met alle opdrachtgevers zullen we proactief een verwerkersovereenkomst sluiten. Daarnaast heeft eelloo een verwerkersovereenkomst met toeleveranciers die persoonsgegevens verwerken. Hierbij is Detron van belang om te noemen, omdat Detron de hostingpartij is van het platform dat eelloo ontwikkelt. Detron is daarmee subverwerker van alle opdrachtgevers van eelloo. Dit is ook aangegeven in onze contracten.

## 9. LEIDENDE TOEZICHTHOUDER

Dit is van belang voor organisaties die internationaal opereren. Het is dan van belang om te weten welke de leidende toezichthouder is ([lees meer](#)). De leidende toezichthouder op de werkzaamheden van eelloo is de Autoriteit Persoonsgegevens.

## 10. TOESTEMMING

Om gegevens te verwerken moet er toestemming zijn van de betrokkenen van wie er persoonsgegevens worden verwerkt. Dit vindt binnen het platform van eelloo al enkele jaren plaats middels het akkoord op het privacy statement. Hierin is expliciet, duidelijk en begrijpelijk vastgelegd op welke wijze gegevens worden verwerkt. Alleen nadat de gebruiker zelf het vinkje zet voor verwerking wordt met verwerking van zijn/haar gegevens gestart.

In de AVG moet de toestemming net zo gemakkelijk in te trekken zijn als hij is gegeven. Dat kan ook, omdat de toestemmingsvraag direct ook kan worden geweigerd. Mocht een kandidaat zijn toestemming gedurende een assessment (of ander traject) de toestemming willen intrekken dan wordt er in feite een verzoek tot verwijdering gedaan. Dat verzoek wordt als een verwijderverzoek in behandeling genomen.

## 4. Conclusie

Er zijn met de overgang van de Wbp naar de AVG zeker een aantal punten die expliciete maatregelen en aandacht vragen van partijen in ons werkveld. Wanneer ze gestructureerd tegen het licht van de eigen situatie worden gehouden, zal meestal blijken dat ze goed zijn in te voeren en ook een logische herkomst hebben. In een wereld waar werk er is voor mensen en niet andersom, is het niet meer dan logisch dat mensen zelf de controle hebben over hun werk-, of loopbaangerelateerde data. Dit is dé reden waarom eelloo binnen de eigen organisatie en bij het ontwikkelen van het platform *privacy by default* en *privacy by design* hoog in het vaandel heeft staan. We hopen hiermee een goede basis te vormen voor het privacybeleid van onze klanten. We hopen dat deze whitepaper organisaties handvatten biedt om te voldoen aan de AVG eisen.

### Vragen?

Neem bij vragen gerust contact op met een eelloo contactpersoon of support via [support@eelloo.nl](mailto:support@eelloo.nl), 088- 100 47 00.

# eelloo

**Bezoekadres**

Fort bij 't Hemeltje  
Fortweg 9  
3992 LX Houten

T 088 100 47 00  
support@eelloo.nl  
www.eelloo.nl

**Postadres**

Postbus 2411  
3502 MC Utrecht

KVK 30 13 67 88  
BTW NL8049 13 328 B01  
Bank NL82 RABO03692 64 290