

VSNU

28 januari 2019

Auteurs:  
M.J. Bonthuis  
M. Domingus

# Code gebruik persoonsgegevens in wetenschappelijk onderzoek

Handreiking voor onderzoekers,  
ondersteuners, faculteitsdecanen  
en bestuurders.





## INHOUDSOPGAVE

<b>1</b>	<b>Waarom gegevensbescherming belangrijk is .....</b>	<b>7</b>
1.1	Verantwoordingsplicht .....	8
1.2	Rollen en verantwoordelijkheden.....	8
1.3	De (U)AVG & wetenschappelijk onderzoek.....	10
1.4	Gedragcode voor de sector .....	11
<b>2</b>	<b>Juridisch kader .....</b>	<b>13</b>
2.1	De Declaration of Helsinki (WMA).....	13
2.2	De (Europese) Algemene Verordening Gegevensbescherming (AVG) .....	13
2.2.1	Uitzonderingen voor wetenschappelijk onderzoek .....	13
2.3	De UAVG.....	16
2.4	De WHW .....	16
2.5	De WMO .....	16
<b>3</b>	<b>Stappenplan Onderzoek &amp; Gegevensbescherming.....</b>	<b>18</b>
3.1	Stap 0: Rollen en verantwoordelijkheden bepalen .....	18
3.2	Stap 1: Minimaliseer de identificeerbaarheid van persoonsgegevens.....	22
3.3	Stap 2: Toestemming en wijze van verwerken .....	28
3.4	Stap 3: Categorie betrokkene .....	31
3.5	Stap 4: Omvang van de verwerking .....	34
3.6	Stap 5: Opslag .....	36
3.7	Stap 6: FAIR principes.....	37
<b>4</b>	<b>Wat kan de universiteit doen?.....</b>	<b>39</b>
4.1	Organisatorische maatregelen .....	39
4.2	Technische maatregelen .....	41
4.3	Juridische maatregelen .....	41
4.4	Monitoren van ontwikkelingen binnen de universiteit .....	43
<b>5</b>	<b>Bijlagen.....</b>	<b>44</b>
	Bijlage 1 EUR voorbeeld: Overeenkomst Gezamenlijke Verwerkingsverantwoordelijken, Joint Controller Agreement.....	44
	Bijlage 2 EUR voorbeeld: Informed Consent formulier.....	44
	Bijlage 3 EUR voorbeeld: Dataclassificatie .....	44
	Bijlage 4 EUR voorbeeld: registratie van onderzoek in het register van verwerkingen .....	44



## VOORWOORD

De context van wetenschappelijk onderzoek is leidend voor deze gedragscode, daarom is een generieke praktische aanpak beschreven die kan worden toegepast op zowel bestaand als toekomstig onderzoek. De gedragscode bevat een instrument waarmee alle betrokkenen de vertaalslag kunnen maken per specifiek onderzoekscenario naar de maatregelen die onderzoekers, ondersteuners, faculteitsdecanen en de CvB van de instelling vanuit het juridische kader zullen nemen. Uitgebreide voorbeelden van de toepassing van deze scenario's en de maatregelen die daarbij passen, zijn daarnaast ook te vinden in de online module Privacy in Onderzoek<sup>1</sup>.

### **Geen uitgebreide handleiding en juridische uitleg**

Deze gedragscode geeft dus niet een pasklaar antwoord op alle vragen voor elke specifieke onderzoekssituatie, maar beperkt zich tot een vertaling van de principes uit de AVG naar praktische handvatten die toepasbaar zijn in specifieke onderzoekscenario's. Hierdoor weten onderzoekers, ondersteuners, faculteitsdecanen en bestuurders met deze handreiking welke beslissingen zij moeten nemen gedurende het onderzoeksproces, wat hierbij de afwegingen zijn en wat de onderliggende logica is. Hierdoor kan zorgvuldig met persoonsgegevens gewerkt worden, maar ook beter worden ingeschat in welke gevallen aanvullende expertise nodig is. Het eerste aanspreekpunt voor de ondersteuning is bij de instellingen doorgaans geregeld vanuit onderzoeksondersteuning (data stewards), de privacy organisatie (privacy officers) en de Functionaris voor de Gegevensbescherming (FG).

Deze gedragscode geeft nadere invulling aan de eerste norm van de Gedragscode wetenschappelijke integriteit 2018, namelijk de verantwoorde balans tussen de privacy rechten van individuen en het belang van het kunnen doen van innovatief onderzoek:

*1. Houd bij de bepaling van onderwerp en inrichting van het onderzoek rekening met de belangen van wetenschap en/of samenleving.*

### **Persoonsgegevens, verwerker of verantwoordelijke**

De eerste vraag voor onderzoekers/ instellingen is of er sprake is van verwerking van persoonsgegevens (wat onder een 'verwerking' kan worden beschouwd wordt hierna uitgelegd) zij volgens de Algemene Verordening Gegevensbescherming (hierna: AVG) en wie daarvoor verantwoordelijk is. Persoonsgegevens<sup>2</sup> zijn gegevens die direct of indirect herleidbaar zijn tot een (levend) individu. In onderzoekscontext gaat het om de identifiers (direct) en quasi identifiers (indirect). Het gaat er vervolgens om wie verantwoordelijk is voor het vaststellen van het doel en de middelen van de verwerking van persoonsgegevens. Deze entiteit is de verwerkingsverantwoordelijke. Daarnaast is het van belang om te bepalen voor welke verwerking de onderzoeker/instelling optreedt in opdracht van een verantwoordelijke. De onderzoeker/instelling opereert dan als verwerker. Tenslotte dienen onderzoekers/ instellingen die vanuit hun rol als verantwoordelijke (derde) partijen in hun

<sup>1</sup> De module is hier te vinden: [https://maken.wikiwijs.nl/117199/Privacy\\_in\\_Onderzoek](https://maken.wikiwijs.nl/117199/Privacy_in_Onderzoek).

<sup>2</sup> Zie ook op de website van de Autoriteit Persoonsgegevens: <https://www.autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens> De AVG spreekt van persoonsgegevens en bijzondere categorieën van persoonsgegevens. Zie voor dit laatste nadere toelichting in hoofdstuk 2.



opdracht persoonsgegevens verwerken (verwerkers) in kaart te krijgen, evenals eventuele sub-verwerkers.

Er is in dit kader een model (uitklapplaat of rolverdeler ppt) ontwikkeld dat op twee vragen antwoord geeft, te weten:

- voor welke verwerkingen van persoonsgegevens ben ik/is mijn organisatie verantwoordelijke of verwerker?
- welke derde partijen verwerken in opdracht van mij (als verantwoordelijke) persoonsgegevens (als verwerker of ontvanger)?

Zo kunnen onderzoekers/instellingen bepalen met welke partijen een verwerkerovereenkomst afgesloten moet worden en met welke niet, bijvoorbeeld omdat het om een verstrekking tussen twee verantwoordelijken gaat.

### **Samenhang met cursusmodule**

Het uitgangspunt van deze gedragscode is dat we een lerend model voorstaan in de sector. Deze gedragscode is hierbij een hulpmiddel om het gesprek over gegevensbescherming met onderzoekers en onderzoeksondersteuners te stimuleren. Daarbij hoort ook dat we vormen vinden om met elkaar concrete casuïstiek te bespreken en daarvan te leren. Om die reden is parallel aan deze code, gewerkt aan een online module Privacy in Onderzoek, die door universiteiten opgenomen kan worden in een elektronische leeromgeving. De module is zo opgezet dat universiteiten zelf workshops kunnen organiseren met onderzoekers.

### **Meer lezen**

In de aanloop naar de invoering van de AVG zijn er talloze publicaties verschenen die de wet uitleggen. Ook is er specifiek voor onderzoek cursusmateriaal ontwikkeld.

- Voor een uitgebreide toelichting van de AVG verwijzen we naar de Handleiding Algemene Verordening Gegevensbescherming van het Ministerie van Justitie en Veiligheid (<https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming>)
- Door de RUG is een MOOC (<https://www.futurelearn.com/courses/general-data-protection-regulation>) ontwikkeld over de AVG
- Op de website ([https://www.edugroepen.nl/sites/RDM\\_platform/Bewustwording/Productenoverzicht.aspx](https://www.edugroepen.nl/sites/RDM_platform/Bewustwording/Productenoverzicht.aspx)) van het Landelijk Coördinatiecentrum Research Data Management komen steeds meer tools beschikbaar, zoals het Maturity Model, privacy reference cards, een routekaart PIA, een flowchart hergebruik zorggegevens en diverse modelformulieren informed consent.
- Bart van der Sloot, De Algemene Verordening Gegevensbescherming in gewone mensentaal. Amsterdam University Press, 2018. (<https://www.aup.nl/nl/book/9789462989290/de-algemene-verordening-gegevensbescherming-in-gewone-mensentaal>)
- Ethics and data protection. 14 November 2018. Dit document is op verzoek van de Europese Commissie (DG Onderzoek en Innovatie) opgesteld door een panel van deskundigen en heeft tot doel de bewustwording in de wetenschappelijke gemeenschap te vergroten, met name met begunstigden van EU-onderzoeks- en innovatieprojecten. ([http://ec.europa.eu/research/participants/data/ref/h2020/grants\\_manual/hi/ethics/h2020\\_hi\\_ethics-data-protection\\_en.pdf](http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf))



- De instrumenten die nodig zijn om aan de AVG te voldoen zijn nog volop in ontwikkeling. In Bijlage 1 van deze code is een aantal voorbeelden opgenomen van juridische contracten. Deze zijn niet voor alle situaties bruikbaar en moeten goed getoetst worden door de experts binnen de eigen instelling.



# 1 Waarom gegevensbescherming belangrijk is

De bescherming van persoonsgegevens (informationele privacy) is vooral in het nieuws vanwege de dreiging van hoge boetes als organisaties niet aan de regels voldoen. Gegevensbescherming is echter al veel langer onderdeel van de beroepscode van wetenschapsbeoefenaars. In de 'Nederlandse Gedragscode Wetenschapsbeoefening' uit 2014 werden al principes benoemd die relevant zijn voor gegevensbescherming (p. 5):

*Iedere wetenschapsbeoefenaar toont respect voor mensen en dieren die betrokken zijn bij wetenschappelijk onderwijs en onderzoek. Onderzoek met mensen is principieel slechts mogelijk als zij op basis van deugdelijke informatie toestemming hebben gegeven, de risico's gering zijn, en de privacy van de betrokkenen afdoende wordt beschermd.*

In de nieuwe Gedragscode wetenschappelijke integriteit 2018 staat onder het principe 'Verantwoordelijkheid' (p. 10):

*Verantwoordelijkheid houdt onder andere in dat men zich rekenschap geeft van het feit dat men als onderzoeker niet solistisch opereert, en daarom rekening houdt met de legitieme belangen van bij het onderzoek betrokken personen en dieren, van eventuele opdrachtgevers en financiers, en van de omgeving.*

Verder wordt bij 'Normen voor goede onderzoekspraktijken' genoemd (p. 12):

*Houd rekening met belangen van (proef)personen, (proef)dieren en de risico's voor de onderzoekers en de omgeving, waarbij in ieder geval alle relevante wet- en regelgeving in acht wordt genomen.*

## **Andere redenen om persoonsgegevens te beschermen**

Een goede en ethische omgang met persoonsgegevens is op zichzelf waardevol, maar er zijn nog andere redenen<sup>3</sup> waarom gegevensbescherming van belang is voor onderzoekers en universiteiten:

- Goed datamanagement en verantwoorde, ethische omgang met onderzoeksdata, wordt steeds meer een eis voor projectaanvragen bij bijvoorbeeld NWO en bij Europese subsidies<sup>4</sup>.
- Consortiumpartners kunnen eisen dat uw organisatie haar datamanagement goed op orde heeft en anders de samenwerking stoppen.
- Goede en ethische omgang met data kan de betrouwbaarheid van het onderzoek en de onderzoeksresultaten vergroten.
- Een goede en ethische omgang met data kan het vertrouwen van burgers en onderzoeksobjecten in de wetenschap vergroten.
- Een schending van de wettelijke regels kan leiden tot reputatieschade en negatieve media aandacht.
- Een schending van de wettelijke regels kan leiden tot boetes die kunnen oplopen tot 20 miljoen euro per schending van de Algemene Verordening Gegevensbescherming.

<sup>3</sup> Zie ook: A Researcher's Privacy Reference Card. Why. ([hdl.handle.net/1765/111052](https://hdl.handle.net/1765/111052))

<sup>4</sup> Zie ook: Ethics and data protection ([http://ec.europa.eu/research/participants/data/ref/h2020/grants\\_manual/hi/ethics/h2020\\_hi\\_ethics-data-protection\\_en.pdf](http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf))



## 1.1 Verantwoordingsplicht

De AVG is gebaseerd op privacy principes en vergemakkelijkt en waarborgt het vrije verkeer van persoonsgegevens binnen de EU, door het harmoniseren van de regelgeving binnen de EU. Hiermee wordt beoogd de interne markt te versterken, met name door publiek-private gedreven innovatie, waarbij universiteiten een belangrijke rol spelen. Het recht op gegevensbescherming is geen absoluut recht, maar een grondrecht naast andere rechten. Het doen van onderzoek en bijdragen aan innovatie in publiek-private samenwerkingen wordt gestimuleerd vanuit de AVG. De AVG eist tegelijkertijd dat bij de verwerkingen van persoonsgegevens in onderzoek adequate maatregelen worden getroffen, die instellingen in staat stellen om aan te tonen dat zij handelen in overeenstemming met de AVG.

De AVG legt dus een verantwoordingsplicht bij instellingen om aan te tonen dat op een goede manier invulling wordt gegeven aan een adequate verwerking van persoonsgegevens. De instelling beschermt bij deze verwerkingen de (informatie) privacyrechten en vrijheden van de betrokkenen bij wetenschappelijk onderzoek. Zo moet de instelling kunnen aantonen dat een verwerking voldoet aan de privacy principes van rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid<sup>5</sup>.

Instellingen zijn verplicht verantwoording af te leggen over de gegevensverwerkingen bv. wanneer de Autoriteit Persoonsgegevens daar om vraagt. Hierbij zal worden gekeken naar de mate waarin de instelling passende en gedocumenteerde technische en organisatorische maatregelen heeft genomen om de persoonsgegevens te beschermen. Bijvoorbeeld door het toepassen van de principes van privacy by design en privacy by default<sup>6</sup>.

## 1.2 Rollen en verantwoordelijkheden

De AVG onderscheidt twee rollen in het kader van het beschermen van persoonsgegevens, de verwerkingsverantwoordelijke en de verwerker. Ze worden hieronder toegelicht:

### *Verwerkingsverantwoordelijke*

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; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

### *Verwerker*

Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

---

<sup>5</sup> Zie ook: <http://www.privacy-regulation.eu/nl/artikel-5-beginselen-inzake-verwerking-van-persoonsgegevens-EU-AVG.htm>.

<sup>6</sup> Zie AVG recital 78: "Ter bescherming van de rechten en vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens zijn passende technische en organisatorische maatregelen nodig om te waarborgen dat aan de voorschriften van deze verordening wordt voldaan. Om de naleving van deze verordening aan te kunnen tonen, moet de verwerkingsverantwoordelijke interne beleidsmaatregelen nemen en maatregelen toepassen die voldoen aan met name de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen. (...)". Bron: <http://www.privacy-regulation.eu/nl/r78.htm>.



De verantwoordelijke blijft verantwoordelijk voor de implementatie van de AVG. De instelling die in opdracht van een verantwoordelijke persoonsgegevens verwerkt (zoals bijvoorbeeld het analyseren van bepaalde gegevens ten behoeve van een specifiek onderzoek of het faciliteren van een (externe) opslag-faciliteit) kan dan als verwerker worden aangemerkt (art 28 AVG). De verantwoordelijke dient een verwerkerovereenkomst af te sluiten met iedere verwerker. De AVG geeft in het algemeen aan welke onderwerpen in een verwerkersovereenkomst vastgelegd dienen te worden (art 28 (3) AVG).

Voor de context van onderzoek zullen die voorwaarden meer toegesneden moeten worden op de eisen van onderzoek en de erkende uitzonderingen. Zo is bijvoorbeeld aangegeven dat de persoonsgegevens na afloop van de overeenkomst vernietigd dienen te worden of teruggegeven. Bij onderzoek zal er een specifieke afspraak uitgewerkt moeten worden, zoals het voor een vastgelegde periode opslaan van gepseudonimiseerde gegevens bij de instelling, zodat verificatie van de resultaten van het onderzoek mogelijk is.

Het kan ook zijn dat de private partij en de onderzoeksinstelling als gezamenlijke verantwoordelijken (art 26 AVG) dienen te worden aangemerkt. Beide verantwoordelijken zijn dan gebonden aan de eisen van de verordening, al kan de verantwoordelijkheid van de wetenschappelijke partner wel een specifieke invulling krijgen. In dat geval dienen partijen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze verordening vast te stellen, met name met betrekking tot de uitoefening van de rechten van de betrokkenen en hun respectieve verplichtingen om de in de artikelen 13 en 14 AVG bedoelde informatie te verstrekken.

De verantwoordelijkheid van de instelling om te voldoen aan de AVG leidt er ook toe dat rollen en verantwoordelijkheden binnen organisaties bij het gebruik van persoonsgegevens helder moeten zijn. Waar senior management (in dit geval het College van Bestuur/faculteitsdecaan) voorheen aan de onderzoeker kon vragen: "Ben je klaar voor de AVG?", is de nieuwe vraag die gesteld wordt: "Heb ik je voldoende in de gelegenheid gesteld om te voldoen aan de AVG?".

De concrete rolverdeling bij het voldoen aan de AVG is verdeeld over drie niveaus:

- 1. Universiteit (CvB):** voorziet in de noodzakelijke algemene voorzieningen om onderzoekers in staat te stellen te voldoen aan de regels: beleid, richtlijnen, infrastructuur en gekwalificeerde staf die onderzoekers ondersteunen. Het College van Bestuur draagt de verantwoordelijkheid voor het scheppen van de algemene noodzakelijke voorwaarden voor verantwoorde omgang met persoonsgegevens. Hiertoe stelt zij privacybeleid vast, stelt zij relevante handreikingen vast, ziet zij erop toe dat een passende infrastructuur beschikbaar is en dat er een adequate onderzoeksondersteuning is die voorziet in ondersteuning, training en advisering gedurende de gehele levenscyclus van persoonsgegevens waar zij verantwoordelijke van is.
- 2. Faculteitsdecaan:** voorziet in aanvullende noodzakelijke en discipline-specifieke voorzieningen om onderzoekers in staat te stellen te voldoen aan de regels: beleid, richtlijnen, infrastructuur en gekwalificeerde staf die onderzoekers ondersteunen. De decaan van een faculteit stelt vast of de door het CvB gerealiseerde algemene



noodzakelijke voorwaarden voor verantwoorde omgang met persoonsgegevens passend zijn voor het onderzoek aan zijn/haar faculteit. Waar nodig zal de decaan erop toezien dat aanvullende specifieke noodzakelijke voorwaarden voor verantwoorde omgang met persoonsgegevens passend zijn voor het onderzoek aan zijn/haar faculteit worden gerealiseerd.

- 3. Onderzoekers:** volgen privacy principes en gebruiken de voorzieningen die privacy ondersteunen (beleid, richtlijnen, infrastructuur en gekwalificeerde staf die onderzoekers ondersteunen). De onderzoeker maakt optimaal gebruik van de algemene en eventueel specifieke voorzieningen en middelen om verantwoord onderzoek te kunnen doen en ziet toe op de goede gang van zaken in zijn/haar onderzoek, conform de privacy principes. Daarnaast heeft de onderzoeker een eigen verantwoordelijkheid voor het onderzoeksontwerp, het documenteren van de omgang met onderzoeksgegevens en de verantwoorde toepassing van de onderzoeksmethodiek. De doorwerking van ethische gedragscodes hierbij wordt erkend in de AVG. Een vorm van peer assessment - al dan niet door een wettelijk erkende ethische commissie- vormt een eerste afweging van de bescherming van de rechten van betrokkenen. Onderzoeksfinanciers vragen in het kader van dergelijke assessments ook aantoonbare bewustheid van passende maatregelen voor de bescherming van de gegevens. In deze gedragscode wordt er vanuit gegaan dat voor ieder onderzoek een onderzoeksprotocol moet worden opgesteld die is goedgekeurd door een hoofdonderzoeker (Principal Investigator).

### **1.3 De (U)AVG & wetenschappelijk onderzoek**

De Algemene Verordening Gegevensbescherming (AVG) die op 25 mei 2018 in werking trad, en ook de aanpalende (concept) Uitvoeringswet AVG, beschrijven algemene principes die geborgd dienen te worden om persoonsgegevens te beschermen in het kader van wetenschappelijk onderzoek.

Hoe kan het wetenschappelijk onderzoek zo ingericht worden dat de voortgang van het onderzoek zo weinig mogelijk hinder ondervindt? En waarbij tegelijk optimaal recht wordt gedaan aan de rechten en vrijheden van personen betrokken bij het onderzoek, zoals beschreven en bedoeld in de (uitvoeringswet) Algemene Verordening Gegevensbescherming en eventuele overige/ nationale wet- en regelgeving? Hoe kunt u weten of en wanneer u passende organisatorische en technische maatregelen moet treffen om persoonsgegevens op passende wijze te beschermen binnen uw onderzoek en wat de aard van deze maatregelen is?

De gedragscode richt zich voor al op wetenschappelijk onderzoek met persoonsgegevens:

- die specifiek voor dit doel worden verzameld (vragenlijsten, cohort-onderzoek etc.);
- die voor wetenschappelijk onderzoek worden hergebruikt (dossieronderzoek), dan wel
- met betrokkenen waar de verantwoordelijke al een (arbeids-)relatie mee heeft (ook wel 'eigen' betrokkenen) genoemd.

Voor het medisch-/gezondheidswetenschappelijk onderzoek en onderzoek met humaan materiaal zijn specifieke regelingen voorhanden/ in de maak. Zo wordt door de COREON (Federa) een gedragscode gezondheidsonderzoek ontwikkeld en is er een Europese



gedragscode research in ontwikkeling. Deze twee gebieden blijven buiten beschouwing bij deze gedragscode, maar sluiten er qua uitgangspunten wel op aan.

Deze gedragscode biedt helderheid en duidelijkheid met betrekking tot deze vragen voor het ontwerp, de uitvoering, de ondersteuning en de beoordeling van wetenschappelijk onderzoek. Deze code heeft de vorm van een gedragscode voor de sector, zoals beschreven in art.40 lid 2 van de AVG.

#### **1.4 Gedragscode voor de sector**

De Algemene Verordening Gegevensbescherming biedt de mogelijkheid aan "verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen" om een gedragscode op te stellen, teneinde de toepassing van de verordening nader toe te lichten<sup>7</sup>.

Om twee redenen is een nadere uitleg van verwerkingen van persoonsgegevens in wetenschappelijk onderzoek nodig, namelijk:

- een praktische toelichting op het zorgvuldig en rechtmatig verwerken van persoonsgegevens in wetenschappelijk onderzoek momenteel feitelijk ontbreekt en
- de AVG en de Uitvoeringswet AVG (UAVG) nadere bepalingen kennen die specifiek gelden voor onderzoek; de zogenaamde vrijstellingen/ uitzonderingen voor onderzoek.

De gedragscode omgang met persoonsgegevens biedt praktische handvatten voor:

- a behoorlijke en transparante verwerking in wetenschappelijk onderzoek;
- b de uitoefening van de rechten van personen, betrokkenen bij wetenschappelijk onderzoek;
- c de gerechtvaardigde belangen van de onderzoeker in de context van wetenschappelijk onderzoek;
- d de verzameling van persoonsgegevens;
- e de pseudonimisering van persoonsgegevens;
- f behoorlijke informatieverstrekking aan en transparantie naar betrokkenen en het publiek in algemene zin;
- g behoorlijke informatieverstrekking aan en transparantie naar minderjarigen, de bescherming van de privacyrechten van deze minderjarigen, en de wijze waarop de toestemming wordt verkregen van de personen die de ouderlijke verantwoordelijkheid voor kinderen dragen;
- h passende technische en organisatorische maatregelen ter beveiliging van de verwerking van persoonsgegevens en deze persoonsgegevens zelf;
- i behoorlijke informatieverstrekking en transparantie na een geconstateerd datalek (van onder andere persoonsgegevens) richting de Autoriteit Persoonsgegevens en betrokkenen;
- j de doorgifte van persoonsgegevens aan derde landen of internationale organisaties.

De gedragscode geeft aan hoe de rechten en vrijheden van individuen (data subjecten / betrokkenen), betrokken bij wetenschappelijk onderzoek vanuit één of meerdere van de Nederlandse universiteiten, te beschermen, door passende bescherming van (bijzondere) persoonsgegevens van deze individuen.

---

<sup>7</sup> Zie voor de letterlijke tekst Artikel 40 EU-AVG "Gedragscodes" (bron: <http://www.privacy-regulation.eu/nl/artikel-40-gedragscodes-EU-AVG.htm>).



Daar waar privacybescherming veelal gericht is op het individu, kan door het bekend worden van de resultaten van wetenschappelijk onderzoek ook meer bekend worden over risico's voor bepaalde groepen in de samenleving. Ook al zou de individuele privacy goed beschermd zijn, kan de zogenaamde 'groepsprivacy' worden aangetast. Mogelijk kunnen onderzoeksresultaten leiden tot stigmatisering/ discriminatie van groepen die zo een verhoogd risico lopen. Alle actoren zouden ook met dit aspect rekening moeten houden.

Artikel 40 AVG kent de verplichting om een gedragscode voor te leggen aan de bevoegde toezichthoudende autoriteit, in dit geval de Autoriteit Persoonsgegevens (hierna: AP). De AP heeft echter niet de bevoegdheid om toezicht te houden op gegevensverwerkingen ten behoeve van academische doeleinden. In de concepttekst UAVG is er een uitzondering gemaakt voor de bepalingen omtrent certificering en gedragscodes. Hiermee blijven de relevante artikelen in de AVG onverkort van toepassing. De AVG zegt o.a. dat toezicht op een goedgekeurde gedragscode enkel kan geschieden door een orgaan dat over passende deskundigheid tot het onderwerp van de gedragscode bezit (artikel 41 AVG).

Toezicht op de VSNU Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek is op dit moment mogelijk door de KNAW. Artikel 1.5 WHW beschrijft de KNAW als organisatie die werkzaam is op het gebied van wetenschappelijk onderzoek en een die de uitwisseling van informatie en gedachten bevordert. Niet alleen is er dus een wettelijke aanknopingspunt, ook bezit de KNAW de relevante deskundigheid en kennis op het gebied van wetenschapsbeoefening om toezicht te houden op de naleving van de gedragscode.

Een gedragscode (art 40 (2) (b) AVG) binnen de instelling kan de verordening nader toelichten met het oog op de gerechtvaardigde belangen die door verwerkingsverantwoordelijken in een specifieke context worden behartigd. Het zou nuttig zijn als in gedragscodes bijvoorbeeld voor het veld van direct marketing en smartmeter data, ook zou worden ingegaan op deze invulling. Voor onderzoek binnen organisaties zou dit bijdragen aan de transparantie. Voor onderzoek bij andere instellingen voorkomt het een ketenprobleem. De wetenschappelijke instellingen, die betrokken worden bij onderzoek, hebben belang bij de samenwerking en het hergebruik van de data, maar zij zijn niet primair de verantwoordelijke. Een oplossingsrichting zou zijn dat de instellingen in een gedragscode of via een andere procedure vaststellen welke maatregelen als passende waarborgen bij verdere verwerking voor specifieke onderzoek scenario's minimaal afgesproken worden.



## 2 Juridisch kader

Het juridisch kader is gebaseerd op internationale, Europese en nationale wet- en regelgeving, op een praktische manier uitgewerkt in deze gedragscode.

### 2.1 De Declaration of Helsinki (WMA)

De verklaring van Helsinki gaat in op de ethische aspecten van wetenschappelijk onderzoek met identificeerbare personen en waarin de noodzaak van een onderzoeksprotocol (art. 21,22), toetsing door een ethische commissie (art. 23) vertrouwelijke omgang en privacy (art. 24).

### 2.2 De (Europese) Algemene Verordening Gegevensbescherming (AVG)

Het begrip "wetenschappelijk onderzoek" wordt in de AVG niet specifiek gedefinieerd. De European Data Protection Board (EDPB, voorheen de Artikel 29 werkgroep/ WP29) vat wetenschappelijk onderzoek op als een "onderzoeksproject dat opgezet wordt in overeenstemming met de relevante methodologische en ethische normen van de sector, conform goede praktijken."

In deze gedragscode wordt dan ook uitgegaan van wetenschappelijk onderzoek door of namens een hoofdonderzoeker die gelieerd is aan een wetenschappelijke instelling die een onderzoeksprotocol heeft goedgekeurd. Het protocol beschrijft onder andere de onderzoeksvraag, de methodologie en hoe deze de omvang van de benodigde gegevens rechtvaardigt.

#### 2.2.1 Uitzonderingen voor wetenschappelijk onderzoek

In dit gedeelte worden de belangrijkste uitzonderingen van de AVG voor onderzoek aangestipt. Toestemming van betrokkenen vormt een belangrijke grondslag voor rechtmatige verwerking van persoonsgegevens (artikel 6 AVG). Dat geldt ook voor onderzoek. Echter, specifieke wetgeving, een overeenkomst, het algemene belang of de gerechtvaardigde belangen van de verantwoordelijke of een derde kunnen ook een grondslag voor onderzoek vormen.

Er zijn in de AVG uitzonderingen voor wetenschappelijk onderzoek, te weten op de beginselen van doelbinding en dataminimalisatie. Soms is het dus toegestaan om zonder toestemming van betrokkene persoonsgegevens te verwerken voor wetenschappelijk onderzoek (artikel 6 (1) (f) AVG; grond 47). Bij verder (her-)gebruik voor onderzoek van persoonsgegevens, die met een andere grondslag zijn verkregen, is wel een aanvullende compatibiliteitstest vereist (artikel 6 (4) AVG; Grond 50). Het beginsel dat persoonsgegevens niet langer bewaard worden dan noodzakelijk is voor het doel van de verwerking kent een uitzondering met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden (art 5 (1) (e) AVG).

Bijzondere persoonsgegevens (gegevens omtrent gezondheid, strafrechtelijk verleden, ras/ethniciteit, geloofsovertuiging, politieke voorkeur, seksuele voorkeur) mogen onder omstandigheden voor onderzoek verwerkt worden, mits er passende technische en organisatorische maatregelen zijn genomen. Dan mag afgezien worden van de invulling van bepaalde rechten van betrokkenen, als dat noodzakelijk is voor het onderzoek (artikel 89



AVG). Dat kan per lidstaat nader ingevuld worden. In de Uitvoeringswet AVG is dit voor Nederland uitgewerkt (art. 44 UAVG).

Ook wordt in de Nederlandse uitvoeringswetgeving een nieuwe uitzondering in de AVG (artikel 85 AVG) voor academische expressies geïmplementeerd, waarmee beoogd wordt ruimte te scheppen voor een afweging tussen de vrijheid van meningsuiting en de bescherming van persoonsgegevens.

In een ontsnappingsclausule voor doorgifte naar derde landen (landen buiten de EU/ EER) wordt wetenschappelijk onderzoek genoemd. Met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden dient rekening gehouden te worden met de gerechtvaardigde verwachting van de maatschappij dat er sprake is van kennisvermeerdering (49 (1) AVG; grond 113).

In het navolgende worden de belangrijkste uitzonderingen uitgelegd.

### **Het gerechtvaardigde doel voor verdere verwerking voor onderzoek**

Twee belangrijke principes uit de AVG die onlosmakelijk met elkaar verbonden zijn, zijn 'doelbinding' en 'rechtmatige grondslag'. De twee worden samen het gerechtvaardigd doel genoemd en worden hieronder toegelicht.

#### *Doelbinding*

De AVG vereist dat persoonsgegevens mogen worden verwerkt voor het doel waarvoor ze zijn verkregen. Persoonsgegevens die een instelling al heeft verwerkt, kunnen volgens Artikel 5 (1) b AVG ook worden gebruikt voor wetenschappelijk onderzoek, ook al zijn zij daar in eerste instantie niet voor bedoeld. De verordening noemt nadrukkelijk de mogelijkheid van verdere verwerking (verenigbaar gebruik) voor het doel van wetenschappelijk onderzoek:

*"...de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1<sup>8</sup>, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd".*

Het verenigbare gebruik moet wel rekening houden met de verwantschap tussen het primaire doel en het doel van wetenschappelijk onderzoek, de context waarin de gegevens zijn verwerkt, de verhouding tussen verantwoordelijke en betrokkene, de aard van de gegevens (gewoon, bijzonder etc.), de mogelijke gevolgen voor de betrokkenen (zie ook: groepsprivacy). Hoe dichter het primaire doel en het doel van wetenschappelijk onderzoek bij elkaar liggen hoe sneller men mag aannemen dat er sprake is van verenigbaarheid gebruik. Daarnaast zullen ten alle tijden het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

#### *Rechtmatige grondslag*

De hoofdregel voor een rechtmatige verwerking is dat organisaties die persoonsgegevens verwerken een rechtmatige grondslag moeten hebben. Artikel 6 AVG geeft aan welke 6 grondslagen er voor verwerkingen in het algemeen mogelijk zijn. Een verwerking voor wetenschappelijk onderzoek is toegestaan als:

---

<sup>8</sup> <http://www.privacy-regulation.eu/nl/89.htm>.



- er toestemming van de betrokkene is of;
- als de verwerking noodzakelijk is voor het gerechtvaardigde belang of;
- als de verwerking noodzakelijk is voor het algemeen belang.

Artikel 23 lid 1 AVG biedt de mogelijkheid om op nationaal niveau met een specifieke wettelijke bepaling verdere verwerking voor wetenschappelijk onderzoek toe te staan. Artikel 41 van de Wet op het Centraal bureau voor de statistiek is een voorbeeld van zo'n wettelijke grondslag voor verwerking van persoonsgegevens voor onderzoek. Het CBS is bevoegd om - mits er voldaan is aan maatregelen bij het CBS en de verzoeker- persoonsgegevens te verstrekken of toegankelijk te maken aan universiteiten in de zin van de Wet op het Hoger en Wetenschappelijk onderwijs (WHW) of andere bij wet ingestelde instellingen voor het doel van statistisch of wetenschappelijk onderzoek.

De ruimte voor verdere verwerking biedt mogelijkheden (i) voor wetenschappelijk onderzoek door de verantwoordelijke zelf en (ii) om namens de verantwoordelijke of als derde onderzoek te doen met voor een ander doel verzamelde persoonsgegevens. Het eerste geval kan bijvoorbeeld spelen bij persoonsgegevens van studenten, die de universiteit primair voor het onderwijs verwerkt. De onderzoeker heeft, als hij onderhandelt over een publiek-private samenwerking en meedenkt over de invulling van de onderzoeksopzet bij de verdere verwerking ook een eigen belang dat het onderzoek kan worden gedaan. In de richtlijnen voor wetenschapsbeoefening dient de decaan zorg te dragen dat er op facultair niveau overzicht is over de verwerking van persoonsgegevens bij dit soort onderzoek en dat deze verwerking met passende maatregelen en transparantie voor betrokkenen is omkleed.

Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens in eerste instantie zijn verzameld, verstrekt de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie (art. 13 lid 3 AVG). Of de persoonsgegevens nu wel of niet van de betrokkene zelf worden verkregen, de verordening schrijft altijd voor dat betrokkenen goed geïnformeerd worden (art 13 en 14 AVG).

### **De uitvoeringswet en de vrijheid van meningsuiting en informatie (art 85 AVG)**

Artikel 85 AVG vraagt de lidstaten om het recht op gegevensbescherming overeenkomstig de verordening in overeenstemming te brengen met het recht op de vrijheid van meningsuiting en van informatie, daaronder begrepen de verwerking voor journalistieke doeleinden en van academische, artistieke of literaire uitdrukkingsvormen. Artikel 85 lid 2 AVG noemt een aantal hoofdstukken in de verordening en verplicht lidstaten om te voorzien in uitzonderingen of afwijkingen van de verordening voor deze categorieën van gegevensverwerkingen. Belangrijk is dat uitzonderingen op artikel 89 AVG ook mogelijk zijn omdat dit artikel onder een van de genoemde hoofdstukken valt. In de UAVG staat dat in het licht van de harmonisatie van terminologie de academische en journalistieke gegevensverwerkingen op een lijn worden geplaatst.

### **Wetenschappelijk onderzoek met bijzondere persoonsgegevens**

Bijzondere persoonsgegevens zijn gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het



oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, of gegevens over strafrechtelijke verleden (UAVG).

Er dienen passende maatregelen getroffen te worden om te waarborgen dat de persoonlijke levenssfeer van de deelnemers niet onevenredig wordt geschaad. Binnen de AVG wordt onderscheid gemaakt tussen gewone persoonsgegevens en bijzondere persoonsgegevens.

Het verbod om bijzondere gegevens te verwerken is niet van toepassing voor zover (art. 9 lid 2 onder j AVG):

- het wetenschappelijk onderzoek een algemeen belang dient,
- de verwerking voor het betreffende onderzoek of de betreffende statistiek noodzakelijk is,
- het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning vergt.

### **2.3 De UAVG**

Artikel 27 van de UAVG werkt de uitzondering op het verbod voor het verwerken van bijzondere persoonsgegevens bij onderzoek uit voor die gevallen dat geen toestemming van betrokkenen kan worden verkregen (art 89 AVG). Daarbij is gekozen voor een beleidsneutrale invulling, die zo dicht mogelijk aansluit bij het voorheen geldende recht (waaronder de Wet bescherming persoonsgegevens).

### **2.4 De WHW**

De WHW vult de ruimte voor ongebonden wetenschappelijk onderzoek en de verwevenheid van onderwijs en onderzoek als essentiële elementen van de universiteit in. Universiteiten en hogescholen hebben niet alleen betekenis, omdat ze hoger opgeleiden leveren maar ook omdat ze functioneren als kennisinstelling waar onderwijs, onderzoek, innovatie en maatschappelijke dienstverlening nauw met elkaar verweven zijn.

### **2.5 De WMO**

Gedragswetenschappelijk, paramedisch en verpleegkundig onderzoek vallen in bepaalde gevallen onder de wet medisch wetenschappelijk onderzoek met mensen (WMO), uitgezonderd daar waar het om het experimenteren van enkel psychologische, opvoedkundige of sociale aard gaat. Om voor wetenschappelijk onderzoek in de zin van de WMO aangemerkt te worden moeten de in de definitie genoemde elementen aanwezig zijn: het moet gaan om wetenschappelijk onderzoek waarbij mensen aan handelingen worden onderworpen of een bepaalde gedragswijze opgelegd krijgen. Dossieronderzoek valt daar dus niet onder. De WMO gaat spelen in gevallen waarbij het onderzoek aanmerkelijk ingrijpt in het dagelijks leven. De WMO vereist een schriftelijke toestemming voor dergelijk wetenschappelijk onderzoek.



Zolang passende waarborgen zijn ingesteld, de verwerking behoorlijk, rechtmatig en transparant is en in overeenstemming met de normen voor gegevensminimalisering en individuele rechten, kunnen andere rechtsgronden dan toestemming, zoals artikel 6, lid 1, onder e) of f) AVG worden gebruikt. Op grond van de uitzondering van artikel 9, lid 2, geldt dit ook voor bijzondere categorieën gegevens. Voor de drie te onderscheiden rollen in de AVG betekent dit het volgende.

De **verantwoordelijke instelling (CvB)** zal er erop moeten toezien dat de faciliteiten om (de uitzonderingen op) het vragen (en weer in kunnen trekken) van toestemming voorhanden zijn. Daarnaast dient de instelling onderzoekers te faciliteren in het kunnen rechtvaardigen van het wetenschappelijk onderzoek, met name daar waar het een uitzondering op de grondslag toestemming betreft.

De **faculteitsdecaan** zal er erop moeten toezien dat (de uitzonderingen op) het vragen (en weer in kunnen trekken) van toestemming zijn geïmplementeerd.

Voor **onderzoekers** betekent dit het volgende. Voor het **verwerken van persoonsgegevens** ten behoeve van wetenschappelijk onderzoek, dan wel het hergebruik van bestaande persoonsgegevens, is één van de drie rechtsgronden, zoals hierboven benoemd (toestemming, gerechtvaardigd belang, algemeen belang), vereist. Hierbij geldt dat toestemming de zwakste rechtsgrond is van de drie, omdat toestemming altijd kan worden ingetrokken. Een beroep op de andere twee rechtsgronden is niet aan de onderzoeker, maar aan het oordeel van de FG, die hierover richtlijnen kan opstellen binnen de instelling. Een beroep op gerechtvaardigd belang of algemeen belang kent verplichtingen in termen van heldere communicatie vooraf (bijvoorbeeld in een privacy statement, waarin de aard van de verwerking en het doel van de verwerking helder wordt toegelicht), en passende technische en organisatorische borging van de bescherming van de betreffende persoonsgegevens.

Voor het **verwerken van bijzondere (categorieën van) persoonsgegevens** ten behoeve van wetenschappelijk onderzoek, dan wel het hergebruik van bestaande bijzondere persoonsgegevens, zal in beginsel door de onderzoeker toestemming van de betrokkene moeten worden gevraagd, tenzij dit onmogelijk blijkt of een onevenredige inspanning vergt. De onderzoeker zal moeten onderbouwen waarom een andere grondslag is gekozen, bijvoorbeeld omdat het onderzoek zelf geschaad wordt (covert research), de risico's voor betrokkenen beperkt zijn en achteraf transparantie wordt gerealiseerd door heldere communicatie over doel en opzet van het onderzoek. Indien toestemming de rechtmatige grondslag is, zal de onderzoeker de betrokkene de mogelijkheid moeten bieden om de toestemming weer in te trekken en geeft de onderzoeker hieraan gehoor, rekening houdend met de geldende uitzonderingen zoals deze gelden voor onderzoek. Zo kan om redenen van reproduceerbaarheid en wetenschappelijke integriteit, na intrekking van de toestemming, wel verdere verwerking van nieuwe gegevens van het individu worden gestaakt, maar kunnen de persoonsgegevens verwerkt tot het moment van intrekken van toestemming, die legitiem zijn verkregen en verwerkt, blijven worden verwerkt. Dit dient van tevoren aan de mogelijke deelnemers van onderzoek helder gecommuniceerd te worden.

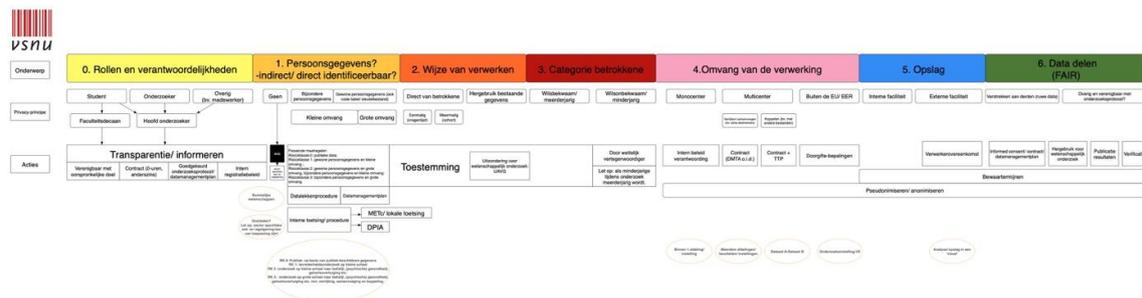


### 3 Stappenplan Onderzoek & Gegevensbescherming

In onderstaand figuur is weergegeven welke overwegingen en maatregelen bij welk soort onderzoek een rol spelen. Iedere onderzoeker kan gebruik maken van dit middel om de noodzakelijk acties die moeten worden genomen te inventariseren. Het middel bevat 6 onderdelen, te weten:

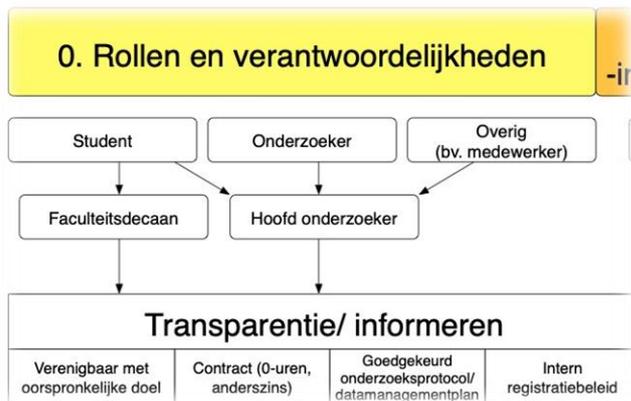
- 0 Rollen en verantwoordelijkheden
- 1 Identificeerbaarheid van persoonsgegevens
- 2 Toestemming en wijze van verwerken
- 3 Betrokkenen
- 4 Omvang van de verwerking
- 5 Opslag van gegevens
- 6 Hergebruik/ FAIR-principes.

Het middel dient op alle onderdelen van boven naar beneden te worden gelezen, vervolgens kan de onderzoeker kiezen welke opties van toepassing zijn op het betreffende onderzoek en ziet de onderzoeker de benodigde acties.



#### 3.1 Stap 0: Rollen en verantwoordelijkheden bepalen

De eerste vraag die beantwoord moet worden is wie welke rol en verantwoordelijkheid heeft. We gaan er bij deze methode vanuit dat het goedgekeurd onderzoek betreft uitgevoerd door (of namens) een academische instelling die daarvoor (mede-)verantwoordelijke is. Als niet helder is welke rol de instelling/ onderzoeker heeft is de verantwoording in het kader van gegevensbescherming niet haalbaar. Voor het definiëren van de rollen kan gebruik gemaakt worden van de AVG-rolverdelers.



Bovenste laag: Over het algemeen kan wetenschappelijk onderzoek binnen een instelling uitgevoerd worden door een:

- student,
- onderzoeker of een
- overige medewerker.

Middelste laag: Dergelijke functies vallen vaak onder supervisie van een hoofdonderzoeker of in het geval van een zorginstelling een hoofdbehandelaar. Er dient een keuze te worden gemaakt wie de hoofdonderzoeker is en dus verantwoordelijk voor de gegevensbescherming binnen het onderzoek.

Onderste laag: De acties die de instelling moet nemen zijn: informeren van betrokken over wetenschappelijk onderzoek (algemeen via bv. de website en specifiek via folders/ mailing/ brieven).

Overige acties kunnen zijn dat:

- er een (0-uren) aanstelling bij de organisatie moet zijn;
- een door de hoofdonderzoeker goedgekeurd onderzoeksprotocol moet zijn;
- het onderzoek intern geregistreerd moet worden.

### **Meer lezen over transparantie bij verwerking van persoonsgegevens voor onderzoek?**

Artikel 13 lid 3 en artikel 14 lid 4 AVG werken het beginsel om een behoorlijke en transparante verwerking te waarborgen verder uit. Om welke informatie het gaat, is samengevat in grond 63 AVG:

*"Elke betrokkene dient het recht te hebben, te weten en te worden meegedeeld voor welke doeleinden de persoonsgegevens worden verwerkt, (indien mogelijk) hoe lang zij worden bewaard, wie de persoonsgegevens ontvangt, welke logica er ten grondslag ligt aan een eventuele automatische verwerking van de persoonsgegevens en, ten minste wanneer de verwerking op profilering is gebaseerd, wat de gevolgen van een dergelijke verwerking zijn..."*

Er is een uitzondering op de informatieverplichting aan betrokkenen in het geval dat het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen. Dat is bijvoorbeeld het geval bij verwerking met het oog op archivering (in het algemeen belang) grootschalig wetenschappelijk of historisch onderzoek of statistische doeleinden. Dan moet wel voldaan zijn aan de voorwaarden en waarborgen genoemd in artikel 89 AVG



(dataminimalisatie door pseudonimisering). Het kan ook zijn dat de verplichting om informatie aan betrokkenen te verstrekken het doel van die verwerking onmogelijk dreigt te maken of ernstig in gevaar dreigt te brengen. In dergelijke gevallen neemt de verwerkingsverantwoordelijke passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het publiek beschikbaar maken<sup>9</sup> van informatie over het onderzoek.

Het beginsel van transparantie in de AVG zou de gedachte kunnen doen postvatten dat het vereist is om persoonsgegevens te bewaren alleen om betrokkenen te kunnen informeren over hun rechten, ook als dat voor de verwerking niet nodig is. Dat is niet het geval. Artikel 11 AVG biedt een regeling voor verwerking waarvoor identificatie niet is vereist. Voor veel onderzoek is het dan ook niet altijd nodig om identificeerbare gegevens te verwerken. Het principe van dataminimalisatie brengt dan met zich mee dat zo snel mogelijk met gepseudonimiseerde gegevens wordt gewerkt. Zo mogelijk wordt dat aan betrokkenen gemeld. Maar de AVG blijft dan wel gelden. Dat is anders als met geanonimiseerde gegevens gewerkt kan worden. Aangezien de gegevens niet meer herleidbaar zijn naar een natuurlijke persoon betekent dat deze gegevens niet onder de scope van de AVG meer vallen. Let wel, van strikt geanonimiseerde gegevens is zelden sprake.

---

<sup>9</sup> De praktische invulling van het openbaar maken zou bijvoorbeeld een mededeling in de krant kunnen zijn met een link naar een website of informatie, die vindbaar wordt gemaakt op de projectwebsite en via het bij de instelling gangbare systeem voor wetenschappelijke informatie. Als er een wetenschappelijke instelling bij het onderzoek is betrokken, zou het uit praktisch oogpunt het handigst zijn als die instelling de verantwoordelijkheid op zich neemt om de openbaarmaking te verzorgen.



### Stap 0: rollen en verantwoordelijkheden per functie

De **instelling (CvB)** dient ervoor zorg te dragen dat het (interne) beleid en regels om wetenschap onderzoek te kunnen doen voorhanden is, zoals bijvoorbeeld:

- het (eigen) onderzoek dient ten alle tijden door of namens een hoofdonderzoeker uitgevoerd te worden;
- de onderzoekers zijn (contractueel) gebonden aan de instelling;
- al het onderzoek dient intern geregistreerd te zijn;
- deelnemers zijn geïnformeerd over het (her-)gebruik van (bijzondere) persoonsgegevens ten behoeve van wetenschappelijk onderzoek;
- er een interne gedragscode is opgesteld en goedgekeurd.

De **faculteitsdecaan** dient ervoor zorg te dragen dat het (interne) beleid en regels om wetenschap onderzoek te kunnen doen binnen de faculteit geïmplementeerd is, zoals bijvoorbeeld:

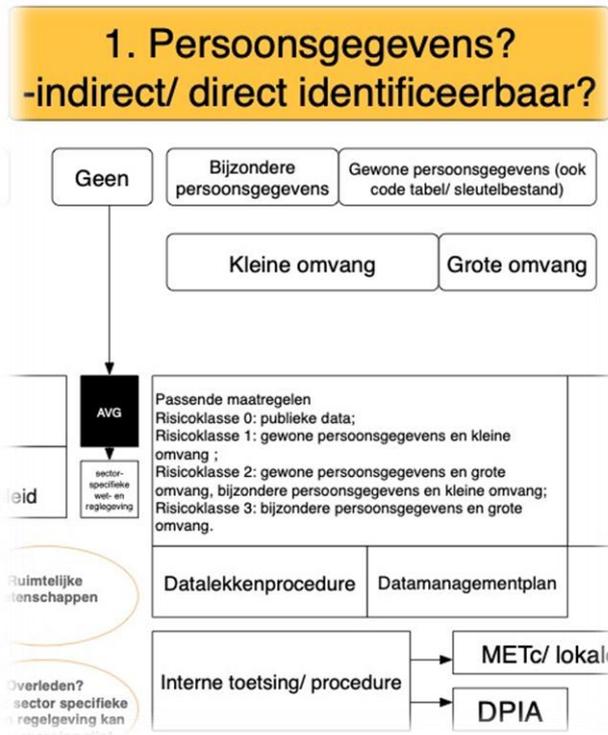
- een procedure voor of door hoofdonderzoekers uit te kunnen voeren;
- onderzoekers (contractueel) te binden aan de instelling, bv. op basis van een 0-uren contract;
- al het onderzoek te (doen) registreren;
- er op toeziet dat de interne gedragscode wordt gevolgd.

De **onderzoeker** dient ervoor zorg te dragen dat het (interne) beleid en regels om wetenschap onderzoek na te leven, met in acht genomen:

- dat het (eigen) onderzoek ten alle tijden door of namens een hoofdonderzoeker uitgevoerd moet worden;
- dat onderzoekers (contractueel) gebonden zijn aan de instelling;
- al het onderzoek te registreren;
- deelnemers hebben geïnformeerd over het (her-)gebruik van (bijzondere) persoonsgegevens ten behoeve van het specifieke wetenschappelijk onderzoek;
- volgt de interne gedragscode.



### 3.2 Stap 1: Minimaliseer de identificeerbaarheid van persoonsgegevens



De eerste vraag die gesteld moet worden is er of er sprake is van verwerking van (gevoelige, bijzondere) persoonsgegevens<sup>10</sup>. Oftewel dat gekeken wordt in welke mate persoonsgegevens<sup>11</sup> herleidbaar naar een natuurlijke persoon zijn. Een verwerking kan zowel direct als indirect herleidbare gegevens bevatten.

Direct herleidbare gegevens zijn bijvoorbeeld: naam, adres, geboortedatum, telefoonnummer, burgerservicenummer, verzekeringsnummer, studentnummer, DNA-profiel. Met deze gegevens kan een natuurlijke persoon uniek worden onderscheiden van andere personen.

Met indirect herleidbare gegevens is een natuurlijke persoon nog niet geïdentificeerd, maar unieke identificatie is zonder onredelijke inspanning mogelijk. Deze "identifiers" zijn zelf geen unieke identificatiegegevens maar voldoende gecorreleerd aan een natuurlijke persoon. Voorbeelden zijn bijvoorbeeld: geslacht, etniciteit, woonplaats, gegevens van bepaalde gebeurtenissen, medische kenmerken. Herleidbaarheid kan in dit geval vaak plaatsvinden door meerdere identifiers te combineren.

#### Meer lezen over herleidbaarheid?

Over wat indirect herleidbaar is, bestaan veel misverstanden. Wat vaak (onterecht) gedacht wordt, is dat met het verwijderen van direct identificerende kenmerken (zoals naam,

<sup>10</sup> "Personal Data" (GDPR\*, Article 4).

<sup>11</sup> Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.



geboortedatum e.d.) een verwerking als anoniem kan worden beschouwd. Deze gegevens kunnen echter nog steeds indirect herleidbaar zijn<sup>12</sup>. Ook gepseudonimiseerde gegevens kunnen indirect herleidbaar zijn. Gepseudonimiseerde gegevens zijn echter niet altijd te beschouwen als een persoonsgegeven (Breyer-zaak), maar ook niet zonder meer anoniem. Een deugdelijke de-identificatie (het onherleidbaar maken van gegevens aan natuurlijke personen) hangt van een aantal factoren af. Deze factoren worden hier uitgewerkt.

In rechtsoverweging 26 van de AVG staat hierover:

*"...Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken. Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen..."*

De volgende actoren kunnen worden onderscheiden bij het proces van de-identificeren:

- het bronbestand die ook veelal van de verantwoordelijke is van de (bijzondere) persoonsgegevens;
- de Trusted Third Party (TTP): de organisatie die de brongegevens aan de bron pseudonimiseert;
- de ontvanger.

Voor iedere actor in het proces kan een eigen conclusie worden getrokken in hoeverre de gegevens als persoonsgegeven (direct/ indirect herleidbaar) dan wel als geanonimiseerd kunnen worden beschouwd, waarbij van belang is:

- hoe uniek zijn gegevens in de dataset, oftewel zijn de gegevens afzonderlijk te isoleren? We noemen dit ook wel 'singling out'. Hoe hoger de mate van isolatie is, hoe sneller aangenomen moet worden dat de gegevens indirect herleidbaar zijn;
- zijn vervolgens de unieke gegeven te koppelen aan een (andere) dataset die direct identificerende gegevens bevat, zodat herleiding naar een natuurlijke persoon mogelijk is?

Voor de mate van koppelbaarheid (*linkability*) is van belang of de actor redelijkerwijs in staat is de gegevens te 'koppelen', hetgeen minder snel aannemelijk is als de pseudonimisering door een organisatie onafhankelijk van de organisatie die het bronbestand in bezit heeft plaatsvindt. De objectieve factoren (kosten en tijd) maken dat het (redelijkerwijs) niet mogelijk is de gegevens bij een onafhankelijk derde partij te koppelen. Dat is wezenlijk anders als de pseudonimisering intern heeft plaatsgevonden, dan wel als de sleutel bij een (onafhankelijke) derde ligt maar de organisatie er voor bepaalde doelen beschikking over kan hebben (bv. voor opsporingsdoeleinden).

Re-identificatie kan dus redelijkerwijs voorkomen worden als er sprake is van:

- een verwaarloosbare 'singling out'; de gegevens zijn niet te isoleren in de set; OF

---

<sup>12</sup> Zie ook: El Emam, K., & Arbuckle, L. (2014). Anonymizing Health Data: Case Studies and Methods to Get You Started. O'Reilly Media, Inc.



- de gegevens zijn door de actor niet te 'linken' aan direct identificeerbare gegevens, bijvoorbeeld doordat de sleutel bij een onafhankelijke derde ligt én deze redelijkerwijs (op basis van wettige middelen) niet voor de actor beschikbaar is. We hanteren hiermee voor wetenschappelijk onderzoek een zogenaamde materiele interpretatie van het begrip 'herleidbaarheid'.

#### **Een voorbeeld**

*Een ip-adres is voor een Internet Service Provider een persoonsgegeven, aangezien dit gegeven te 'linken' is aan het bestand met abonnees. Voor een organisatie die hier geen toegang toe heeft, zal dit redelijkerwijs niet makkelijk te 'linken' zijn aan direct herleidbare gegevens.*

*Het is dus van belang of de verantwoordelijke beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie die bij de internetprovider van deze persoon berust. Geen enkele provider zal NAW-gegevens verstrekken wanneer een websitehouder louter uit nieuwsgierigheid wil weten welke bezoeker er achter een bepaald IP-adres schuil gaat. Naar verwachting zullen onder die omstandigheden IP-adressen dan (dus) ook niet te beschouwen als persoonsgegevens (aangezien de middelen voor identificatie ontbreken).*

In beide gevallen is dus de vraag of door singling out, dan wel linkability (of een combinatie van beide) indirecte herleidbaarheid optreedt. We spreken dan van re-identificatie.

#### **Re-identificatie bij koppeling**

Een tweede veelvoorkomend misverstand is dat het koppelen van twee of meer geanonimiseerde bestanden op weinig bezwaren stuit. Echter, zal in het nieuwe (samengestelde) bestand de kans op singling out en linkability (re-identificatie) opnieuw moeten worden bekeken, er ontstaan immers weer geheel nieuwe combinaties. Het doen van onderzoek met (persoons-)gegevens kan dan ook niet als een statische toestand worden gezien aangezien de gevoeligheid onder andere wordt bepaald door de context waarin het gegeven zich bevindt.

De grote vraag is dus steeds in hoeverre een natuurlijke persoon (indirect) herleidbaar is in een verwerking. Zelfs als alle direct identificeerbare persoonskenmerken zijn verwijderd, bestaat er een gerede kans dat met een combinatie van andere gegevens toch iemand herleidbaar/identificeerbaar is. Om dat risico in te kunnen schatten, zijn speciale technieken en software beschikbaar, die met hulp van statistische technieken de mate van herleidbaarheid kunnen berekenen (k-anonymity). Voorbeelden zijn de software Eclipse<sup>13</sup> van Privacy Analytics of Amnesia<sup>14</sup> van het Institute for the Management of Information Systems Research Center "Athena". Nadat is vastgesteld in welke mate de verwerking direct/indirect herleidbare gegevens bevat, kunnen een aantal bewerkingen worden uitgevoerd om de verwerking te pseudonimiseren, de-identificeren of volledig anoniem te maken.

<sup>13</sup> <https://privacy-analytics.com/software/privacy-analytics-eclipse/>.

<sup>14</sup> <https://amnesia.openaire.eu/>.



**Actie: verkleinen van kans op herleidbaarheid**

Eén van de belangrijkste maatregelen die onderzoekers kunnen nemen, is het verkleinen van de kans dat gegevens tot natuurlijke personen herleidbaar zijn. Belangrijk is om allereerst vast te stellen in welke mate de gegevens (direct of indirect) herleidbaar zijn.

Wanneer een onderzoeker persoonsgegevens verwerkt, kan daarbij de mate van herleidbaarheid worden bepaald, door uit te gaan van de volgende niveaus van herleidbaarheid, waarbij de verwerking:

- 1 direct herleidbare persoonsgegevens bevat – waarin expliciete kenmerken zijn opgenomen, zonder poging om deze te verbergen of te vervangen door indirecte identifiers;
- 2 potentieel identificeerbare gegevens bevat – waarbij een poging is gedaan om direct identificeerbare kenmerken te verbergen. Bijvoorbeeld door een e-mailadres gedeeltelijk te hashen of een nummer te vervangen door een code.
- 3 geen direct/indirect tot natuurlijke personen herleidbare gegevens bevat – data waarin kenmerken ontbreken waarmee personen kunnen worden herleid.

**A VISUAL GUIDE TO PRACTICAL DATA DE-IDENTIFICATION**

Produced by **FUTURE OF PRIVACY FORUM** PFF.org

What do scientists, regulators and lawyers mean when they talk about de-identification? How does anonymous data differ from pseudonymous or de-identified information? Data identifiability is not binary. Data lies on a spectrum with multiple shades of identifiability.

**SSN**

**DEGREES OF IDENTIFIABILITY**  
Information containing direct and indirect identifiers.

**PSEUDONYMOUS DATA**  
Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact.

**DE-IDENTIFIED DATA**  
Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.

**ANONYMOUS DATA**  
Direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification.

	EXPLICITLY PERSONAL	POTENTIALLY IDENTIFIABLE	NOT READILY IDENTIFIABLE	KEY CODED	PSEUDONYMOUS	PROTECTED PSEUDONYMOUS	DE-IDENTIFIED	PROTECTED DE-IDENTIFIED	ANONYMOUS	AGGREGATED ANONYMOUS
<b>DIRECT IDENTIFIERS</b> Data that identifies a person without additional information or by linking to information in the public domain (e.g., name, SSN)	INTACT	PARTIALLY MASKED	PARTIALLY MASKED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
<b>INDIRECT IDENTIFIERS</b> Data that identifies an individual indirectly. Helps connect pieces of information until an individual can be singled out (e.g., DOB, gender)	INTACT	INTACT	INTACT	INTACT	INTACT	INTACT	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
<b>SAFEGUARDS and CONTROLS</b> Technical, organizational and legal controls preventing employees, researchers or other third parties from re-identifying individuals	NOT RELEVANT due to nature of data	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	NOT RELEVANT due to nature of data	NOT RELEVANT due to high degree of data aggregation
<b>SELECTED EXAMPLES</b>	Name, address, phone number, SSN, government-issued ID (e.g., Jane Smith, 123 Main Street, 555-555-5555)	Unique device ID, license plate, medical record number, cookie, IP address (e.g., MAC address 68:AB:4D:35:45:03)	Same as Potentially identifiable except data are also protected by safeguards and controls (e.g., hashed MAC addresses or legal representations)	Clinical or research datasets where only certain regions key (e.g., Jane Smith, diabetes, Hgb 13.1, gHb = Cxk123)	Unique, artificial pseudonyms replace direct identifiers (e.g., HIPAA Limited Datasets John Doe = S1T7 1M619Z) (unique sequence not used anywhere else)	Same as Pseudonymous, except data are also protected by safeguards and controls	Data are suppressed, generalized, perturbed, swapped, etc. (e.g., CFA 3.2 = 3.0-3.5, gender: female = <gender=male>)	Same as De-identified, except data are also protected by safeguards and controls	For example, noise is calibrated to a data set to hide whether an individual is present or not (differential privacy). 5.6% of Washington, DC residents are women	Very highly aggregated data (e.g., statistical data, census data, or population data that 5.6% of Washington, DC residents are women)

Bron: Jules Polonetsky, Omer Tene, and Kelsey Finch, Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification, 56 Santa Clara L. Rev. 593 (2016). Available at: <https://digitalcommons.law.scu.edu/lawreview/vol56/iss3/3>

**Manieren om kans op herleidbaarheid te verlagen**

*Minimaliseren* - er voor zorgen dat precies gedefinieerd wordt welke persoonsgegevens een onderzoeker nodig heeft, en welke niet al dan niet met geautomatiseerde verwijderingscripts.



*Generaliseren van data* - Bij deze bewerking wordt de data in een 'record' vervangen door een minder precieze waarde. Bijvoorbeeld: een geboortedatum wordt vervangen door een leeftijdscategorie. 1 mei 1977 wordt (in 2019): 42

*Onderdrukken van deel van de data* - Hierbij worden bepaalde 'records' vervangen door een "NULL" waarde, of worden 'records' met minder dan 5 of 10 waarnemingen verwijderd. De postcode 3515 AB wordt dan: 3515.

*Subsampling* - In plaats van de volledige set met data, wordt een random deel van de dataset bewaard en de rest verwijderd.

*Scheiden van data* - het scheiden van databases, en het opslaan van data op verschillende verspreide systemen helpt ook om gegevens te beschermen. Door berekeningen te maken op data over verschillende databases heen is er geen centrale opslag. Het beperken van de toegang en encryptietechnieken zijn hier ook goede maatregelen.

*Sleutelbestand* - "Keycoded data" zijn data waarin direct identificeerbare kenmerken zijn vervangen door een code/ sleutel, zodat ongewenste of onbedoelde re-identificatie voorkomen wordt. Degenen die het sleutelbestand in handen hebben, kunnen indien gewenst alsnog de oorspronkelijke gegevens zien.

*Pseudonimiseren* - In een gepseudoniseerd bestand zijn alle directe persoonskenmerken verwijderd of veranderd, maar indirecte persoonskenmerken zijn intact. Aan deze bestanden kan extra beveiliging worden toegevoegd.

*Data de-identificeren* - Als ook de indirecte persoonskenmerken worden verwijderd, is sprake van geïdentificeerde data. Direct en indirect herleidbare kenmerken zijn ofwel verwijderd ofwel zodanig aangepast, dat er geen directe link meer te leggen is tussen informatie over de persoon en de persoon zelf.

*Anonimiseren* - Bij anonimiseren gaat het de-identificeren nog een stap verder: met wiskundige en technische bewerkingen wordt de data zodanig bewerkt dat re-identificatie niet meer mogelijk is. Voor een succesvolle anonimisering zijn diverse technieken en methoden ontwikkeld. K-anonymity en differential privacy zijn de twee belangrijkste vormen. Ze zorgen ervoor dat data bruikbaar blijft voor analyse en waarbij de gegevens beschermd worden.

*Aggregeren* - Bij het aggregeren van data zijn gegevens van meerdere personen samengevoegd. Aanvullende maatregelen zijn dan niet meer nodig. In veel gevallen zijn persoonsgegevens niet nodig, en kun je volstaan met geanonimiseerde en geaggregeerde informatie. Bij het publiceren van data en archivering is het anonimiseren van data door aggregatie een belangrijke methode, om te voorkomen dat er herleidbaarheid tot personen ontstaat.

Bij de verwerking van direct identificerende gegevens dient voor zover mogelijk een gescheiden bestand te worden aangelegd van de communicatiegegevens van de deelnemers en een bestand van onderzoeksgegevens. De koppeling tussen beide geschiedt volgens een inhoudsloos administratienummer. Het communicatiebestand dient (binnen 6 maanden) te



worden verwijderd zodra het voor het doel van het onderzoek niet meer nodig is daarover te beschikken.

**Stap 1: minimaliseer de identificeerbaarheid van persoonsgegevens per functie**

De **instelling (CvB)** dient ervoor zorg te dragen dat het (interne) beleid en regels om passende maatregelen (dataminimalisatie; pseudonimiseren, anonimiseren e.d.) te kunnen doen voorhanden is, zodat onderzoekers en ondersteuners ten alle tijden onderzoek kunnen doen met passende maatregelen. Daarbij dient rekening gehouden te worden met de mate van isolatie van gegevens en de mogelijkheid om te kunnen koppelen (singling out, linkability).

De **faculteitsdecaan** dient ervoor zorg te dragen dat het (interne) beleid en regels om passende maatregelen (dataminimalisatie; pseudonimiseren, anonimiseren e.d.) te kunnen implementeren, zoals bijvoorbeeld:

- een procedure om door onderzoekers gegevens te minimaliseren;
- er op toeziet dat de maatregelen worden gevolgd.

De **onderzoeker** dient ervoor zorg te dragen dat het (interne) beleid en regels om passende maatregelen (dataminimalisatie; pseudonimiseren, anonimiseren e.d.) te kunnen nemen, met in acht genomen:

- dat het (eigen) onderzoek ten alle tijden passende maatregelen moet hebben (anonimiseren, pseudonimiseren, scheiden van communicatiebestand etc.);
- volgt de procedures.



### 3.3 Stap 2: Toestemming en wijze van verwerken



Artikel 6 (1) AVG geeft aan dat een verwerking rechtmatig is als de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden. Toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, bijvoorbeeld een (schriftelijke) verklaring, met elektronische middelen, of een mondelinge verklaring, waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt (grond 32 AVG). Daarnaast gelden ook altijd de informatieplichten van artikel 13 AVG.

Voor gevallen waarin de doeleinden voor gegevensverwerking binnen een wetenschappelijk onderzoeksproject aanvankelijk niet kunnen worden gespecificeerd, staat de AVG als uitzondering toe dat het doel op een meer algemeen niveau kan worden omschreven. Gezien de strenge eisen die door artikel 9 AVG worden gesteld betreffende de verwerking van bijzondere categorieën gegevens, merkt de EDPB (voorheen Artikel 29 Werkgroep) in haar opinie op dat in het geval bijzondere categorieën gegevens worden verwerkt op basis van uitdrukkelijke toestemming, op de toepassing van de flexibele aanpak van overweging 33 AVG een striktere interpretatie van toepassing is een hoge mate van controle vereist. Persoonsgegevens die door hun aard bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden, verdienen dan ook specifieke bescherming aangezien de context van de verwerking ervan significante risico's kan meebrengen voor de grondrechten en de fundamentele vrijheden (grond 51 AVG). Het verbod op verwerking van bijzondere persoonsgegevens heeft geen betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt. De Engelse tekst is hier duidelijker. Er staat dat de persoonsgegevens 'manifestly made public', wat beter vertaald zou kunnen zijn met 'onloochenbaar door betrokkene openbaar gemaakt zijn'. Wel zal er meer aandacht moeten komen voor de manier waarop in dit soort specifieke gevallen bij onderzoek invulling kan worden gegeven aan de informatie aan betrokkenen op grond van artikel 13 en 14 AVG.

#### Brede en/of gespecificeerde toestemming

De AVG lijkt een zekere mate van flexibiliteit te verschaffen voor de mate van specificering en granulariteit van toestemming in het kader van wetenschappelijk onderzoek. Het is vaak niet mogelijk op het ogenblik waarop de persoonsgegevens worden verzameld, het doel van de gegevensverwerking voor wetenschappelijke onderzoeksdoeleinden volledig te omschrijven. Daarom moet de betrokkenen worden toegestaan toestemming te kunnen



geven voor bepaalde terreinen van het wetenschappelijk onderzoek waarbij erkende ethische normen voor wetenschappelijk onderzoek in acht worden genomen. Betrokkenen moeten de gelegenheid krijgen om hun toestemming alleen te geven voor bepaalde onderzoeksterreinen of onderdelen van onderzoeksprojecten, voor zover het voorgenomen doel zulks toelaat. Ten eerste moet worden opgemerkt dat de verplichtingen ten aanzien van de eis van specifieke toestemming niet buiten toepassing laat. Dit betekent dat wetenschappelijke onderzoeksprojecten in beginsel alleen persoonsgegevens op basis van toestemming mogen omvatten als een dergelijk project een goed omschreven doel heeft.

Het is belangrijk dat in het geval toestemming wordt gebruikt als de rechtsgrond voor de verwerking, dat de betrokkene ook een mogelijkheid moet hebben om deze toestemming weer in te kunnen trekken. De EDPB merkt op dat het intrekken van toestemming zou kunnen leiden tot ondermijning van bepaalde soorten wetenschappelijk onderzoek waarvoor aan personen gekoppelde gegevens nodig zijn, de AVG is echter duidelijk dat toestemming moet kunnen worden ingetrokken en dat verwerkingsverantwoordelijken hiernaar moeten handelen—voor wetenschappelijk onderzoek geldt geen uitzondering op deze eis. Wanneer een verwerkingsverantwoordelijke een verzoek tot intrekking ontvangt, moet hij in beginsel de persoonsgegevens meteen wissen als hij de gegevens wil blijven gebruiken voor (toekomstige) onderzoeksdoeleinden.

In bijlage 2 is een voorbeeld van een Toestemmingsformulier opgenomen die voldoet aan de AVG. Let wel, toestemming is afhankelijk van de verstrekte informatie. Toestemming zal dan ook altijd in dat licht moeten worden gezien.



In de U-AVG geldt een uitzonderingsgrond (art. 24 U-AVG), waardoor het mogelijk is om uitdrukkelijke toestemming achterwege te laten indien het vragen ervan onmogelijk blijkt of een onevenredige inspanning vergt. Bij de uitvoering moet dan wel voorzien worden in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Deze uitzondering geldt echter niet voor onderzoek dat onder de reikwijdte van de WMO valt.

### **Stap 2: Toestemming en wijze van verwerken per functie**

De **instelling (CvB)** dient ervoor zorg te dragen dat het (interne) beleid en regels om de uitzondering op toestemming te bepalen, toestemming te vragen, dan wel bezwaar te maken voorhanden is, zodat onderzoekers en ondersteuners ten alle tijden onderzoek kunnen doen met een rechtmatige grondslag.

De **faculteitsdecaan** dient ervoor zorg te dragen dat het (interne) beleid en regels om de uitzondering op toestemming te bepalen, toestemming te vragen te kunnen implementeren, zoals bijvoorbeeld:

- Beleid/ procedures om te bepalen voor welk soort onderzoek toestemming nodig is en wanneer daarvan kan worden afgeweken;
- Procedure voor betrokkenen om (al dan niet schriftelijk) toestemming te geven/ bezwaar te maken, gegeven toestemming weer in te trekken etc. middels een standaard formulier.

De **onderzoeker** dient ervoor zorg te dragen dat het (interne) beleid en regels om de uitzondering op toestemming te bepalen, toestemming te vragen wordt gevolgd, zoals bijvoorbeeld:

- Beleid/ procedures om te bepalen voor welk soort onderzoek toestemming nodig is en wanneer daarvan kan worden afgeweken;
- Procedure voor betrokkenen om (al dan niet schriftelijk) toestemming te geven/ bezwaar te maken, gegeven toestemming weer in te trekken etc. middels een standaard formulier.



### 3.4 Stap 3: Categorie betrokkene

In welke mate de technische en organisatorische maatregelen adequaat zijn, bij de verwerking van persoonsgegevens, heeft ook een relatie met de individuen van wie de persoonsgegevens worden verwerkt. De AVG stelt hogere eisen aan de verwerking van persoonsgegevens van kwetsbare groepen en minderjarigen.



#### *Kwetsbare groepen*

Van betrokkenen, die vanuit cultureel, maatschappelijk, sociaal, of anderzijds, als kwetsbaar kunnen worden aangemerkt zal een wettelijk vertegenwoordiger de toestemming moeten geven.

#### *Minderjarigen*

Voor wat betreft wetenschappelijk onderzoek met (bijzondere) persoonsgegevens worden jongeren vanaf 16 jaar in de AVG en de WMO gelijkgesteld met volwassenen. Zij kunnen zelfstandig toestemming geven voor een bepaalde behandeling (zoals toestemming geven voor wetenschappelijk onderzoek, deze intrekken dan wel bezwaar maken), instemming van de ouders is niet nodig. Bij kinderen jonger dan 12 jaar beslissen alleen de ouders daarover. Aan jonge kinderen moet wel op een begrijpelijke wijze worden uitgelegd wat er gaat gebeuren. Zijn de kinderen tussen de 12 en 16 jaar dan moeten zowel ouder als kind afzonderlijk toestemming geven voor deelname aan wetenschappelijk onderzoek, danwel het bezwaar maken daartegen.

Van belang is dat, hoewel de AVG de mogelijkheid biedt aan lidstaten om de leeftijdsgrens naar 13 te verlagen, er in Nederland bij het verwerken van gegevens van kinderen tot 16 jaar, toestemming nodig is van de ouders of verzorgers.

#### **Rechten van betrokkenen**

Wanneer persoonsgegevens overeenkomstig artikel 89, lid 1 AVG, met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt, heeft de betrokkene het recht om met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens, tenzij de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang. De verwerkingsverantwoordelijke moet kunnen aantonen dat zijn belangen zwaarder wegen dan de belangen, de grondrechten en de fundamentele vrijheden van de betrokkene.



Betrokkenen hebben bijvoorbeeld het recht op inzage om te weten welke gegevens van hen verwerkt worden, met welk doel die verwerkt worden en waar die gegevens vandaan komen. Artikel 12 AVG stelt dat betrokkenen op begrijpelijke wijze op hun rechten moet worden gewezen en dat de verwerkingsverantwoordelijke de uitoefening van de rechten moet faciliteren. In het voorafgaande zagen we al dat bij verwerking voor onderzoek de nationale wetgever soms specifieke en soms algemenere uitzonderingen op deze rechten mogelijk heeft gemaakt bij onderzoek. Ook de AVG noemt twee direct werkende uitzonderingen.

Artikel 16 t/m 20 regelen de rechten op rectificatie en wissing van gegevens. Artikel 17 bepaalt bijvoorbeeld dat de betrokkene het recht heeft op wissing van de gegevens als ze niet meer nodig zijn voor het doel van de verwerking of als de betrokkene zijn toestemming heeft ingetrokken. Artikel 17 (3) (d) AVG geeft aan dat de rechten van artikel 17 AVG (recht op gegevenswissing) niet gelden als dat nodig is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89 , lid 1 AVG, voor zover het bedoelde recht de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen.

In artikel 21 (6) AVG en in grond 69 AVG wordt specifiek genoemd dat het recht van bezwaar ook bij onderzoek geldt, tenzij er sprake is van wetenschappelijk onderzoek dat noodzakelijk is voor de uitvoering van een taak van algemeen belang:

Specifiek voor verwerkingen voor wetenschappelijke doeleinden bij instellingen of diensten voor wetenschappelijk onderzoek noemt de concepttekst van de UAVG een mogelijke uitzondering op bepaalde rechten van betrokkenen (Art. 42 UAVG). Indien een verwerking wordt verricht door instellingen of diensten voor wetenschappelijk onderzoek of statistiek, en de benodigde voorzieningen zijn getrokken om te verzekeren dat de persoonsgegevens uitsluitend voor statische of wetenschappelijke doeleinden worden gebruikt, kan de verantwoordelijke de artikelen 15, 16 en 18 van de AVG buiten toepassing laten. Het gaat dan om het recht van inzage van de betrokkene, het recht op rectificatie en het recht op beperking van de verwerking.



### Stap 3: Categorie betrokkene per functie

De **instelling (CvB)** dient ervoor zorg te dragen dat het (interne) beleid en regels om betrokkenen hun rechten uit te kunnen laten oefenen voorhanden is, zodat onderzoekers en ondersteuners ten alle tijden onderzoek kunnen doen met inachtneming van de rechten van alle soorten betrokkenen.

De **faculteitsdecaan** dient ervoor zorg te dragen dat het (interne) beleid en regels om betrokkenen hun rechten uit te kunnen laten oefenen geïmplementeerd is, zodat onderzoekers en ondersteuners ten alle tijden onderzoek kunnen doen met inachtneming van de rechten van alle soorten betrokkenen, bijvoorbeeld door:

- een procedure incl. een goedgekeurd model voor inzage, correctie, verwijdering, terugkoppeling etc.;
- er op toeziet dat de procedures/formats worden gevolgd/gebruikt.

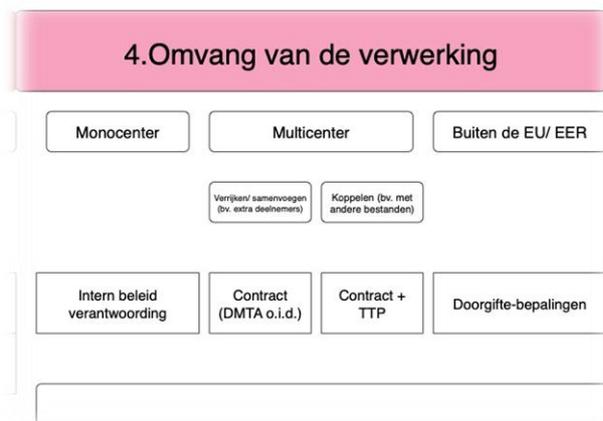
De **onderzoeker** dient ervoor zorg te dragen dat het (interne) beleid en regels om betrokkenen hun rechten uit te kunnen laten oefenen bekend is en gevolgd wordt, bijvoorbeeld door:

- een procedure incl. een goedgekeurd model voor inzage, correctie, verwijdering, terugkoppeling etc.;
- gebruikt gemaakt is van procedures/formats.



### 3.5 Stap 4: Omvang van de verwerking

Bij de verwerking met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens binnen een en dezelfde instelling zal aan het interne (verantwoordingsbeleid) moeten voldoen.



#### *Multicenter en verwerkers*

Wanneer meerdere instellingen (multicenter) betrokken zijn bij een onderzoeksprotocol kan er worden vanuit gegaan dat er meerdere verwerkingsverantwoordelijken verantwoordelijk zijn. Als er meerdere verwerkingsverantwoordelijken betrokken zijn bij een onderzoeksprotocol (multicenter) zullen partijen in een overeenkomst aspecten van de AVG en datamanagement vast moeten leggen. Er kan sprake zijn van het verrijken van de verwerking, bv. door een protocol uit te voeren binnen verschillende instellingen met een vergelijkbare doelgroep. Ook kan er sprake zijn van koppeling.

Het kan ook zijn dat bepaalde verwerkingsactiviteiten zijn uitbesteed aan een derde partij, dan is sprake van een verwerker. Met verwerkers zal een verwerkerovereenkomst afgesloten moeten worden. Dit geldt zowel voor het mono- als multicenteronderzoek.

#### *Koppelen van gegevens uit verschillende verwerkingen*

Mag koppeling van gegevens uit verschillende registers ten behoeve van wetenschappelijk onderzoek volgens de AVG? Ja, wetenschappers verwerven dankzij registeronderzoek essentiële kennis over de wisselwerking op lange termijn, bijvoorbeeld van een aantal sociale factoren, zoals werkloosheid en onderwijs met andere levensomstandigheden.

Onderzoeksresultaten die door middel van registers worden verkregen leveren solide kennis van hoge kwaliteit op die een maatschappelijke impact en relevantie kennen, bijvoorbeeld doordat deze kunnen worden gebruikt om een op kennis gebaseerd beleid te ontwikkelen en te implementeren, de levenskwaliteit van een deel van de bevolking te verbeteren, en sociale diensten efficiënter te maken. Daarom mogen persoonsgegevens worden gebruikt voor wetenschappelijke onderzoeksdoeleinden, met inachtneming van de passende voorwaarden en waarborgen voor de bescherming van de privacyrechten en vrijheden van de personen betrokken bij dit onderzoek.



Om tegemoet te komen aan het principe van dataminimalisatie zal gebruik gemaakt kunnen worden van een Trusted Third Party (zie persoonsgegevens: anonimiserings/pseudonimisering).

#### *Grensoverschrijdende verwerking*

Wanneer gegevens worden doorgegeven aan landen buiten de Europese Unie (EU) (zogenaamde derde landen), dient dit in het privacystatement worden opgenomen. Een derde land is een land buiten de EU (exclusief Noorwegen, IJsland en Liechtenstein). Gegevens mogen alleen doorgegeven worden aan derde landen als het betreffende land een passend beschermingsniveau heeft. De Europese Commissie geeft een adequaatheidsbesluit aan derde landen die een passend beschermingsniveau hebben. Klik hier @@@ voor de landen die een passend beschermingsniveau hebben.

#### **Stap 4: Omvang van de verwerking per functie**

De **instelling (CvB)** dient ervoor zorg te dragen dat:

- er vastgesteld (intern) beleid en regels zijn om mono-centeronderzoek te kunnen verantwoorden;
- er contracten afgesloten kunnen worden met instellingen die mee- en of samenwerken aan het onderzoek (multicenter);
- er verwerkerovereenkomsten afgesloten kunnen worden met derde partijen die in opdracht gegevens verwerken;
- er een TTP-voorziening is wanneer bestanden moeten worden gekoppeld.

De **faculteitsdecaan** dient ervoor zorg te dragen dat:

- het vastgestelde (interne) beleid en regels om monocenter-onderzoek te kunnen verantwoorden is geïmplementeerd;
- er een procedure binnen de faculteit is geïmplementeerd waardoor er contracten afgesloten kunnen worden met instellingen die mee- en of samenwerken aan het onderzoek (multicenter);
- er een procedure binnen de faculteit is geïmplementeerd waarmee verwerkerovereenkomsten afgesloten kunnen worden met derde partijen die in opdracht gegevens verwerken;
- er een procedure is geïmplementeerd wanneer TTP-voorziening nodig is (bv. wanneer bestanden moeten worden gekoppeld).

De **onderzoeker** dient ervoor zorg te dragen dat het (interne) beleid en regels om monocenter-onderzoek is verantwoord;

- er contracten afgesloten zijn met instellingen die mee- en of samenwerken aan het onderzoek (multicenter);
- er verwerkerovereenkomsten afgesloten zijn met derde partijen die in opdracht gegevens verwerken.
- er gebruik is gemaakt van een TTP wanneer bestanden worden gekoppeld.



### 3.6 Stap 5: Opslag

Onderzoekers zullen de bestanden op de interne faciliteit moeten plaatsen. Er kan ruimte zijn om voor een externe faciliteit te kiezen. De opslag is een verwerkingsactiviteit en met de derde partij zal een verwerkerovereenkomst afgesloten moeten worden.



Het kan raadzaam om bij de verwerking van direct identificerende gegevens de communicatiegegevens van de deelnemers te scheiden van een bestand met onderzoeksgegevens. De koppeling tussen beide geschiedt volgens een inhoudsloos administratienummer. Het communicatiebestand dient (binnen 6 maanden) te worden verwijderd zodra het voor het doel van het onderzoek niet meer nodig is daarover te beschikken.

#### Stap 5: Opslag per functie

De **instelling (CvB)** dient ervoor zorg te dragen dat:

- er vastgesteld (intern) beleid en regels zijn om gegevens intern op te slaan;
- er verwerkerovereenkomsten afgesloten kunnen worden met derde partijen die in opdracht gegevens verwerken (opslaan);

De **faculteitsdecaan** dient ervoor zorg te dragen dat:

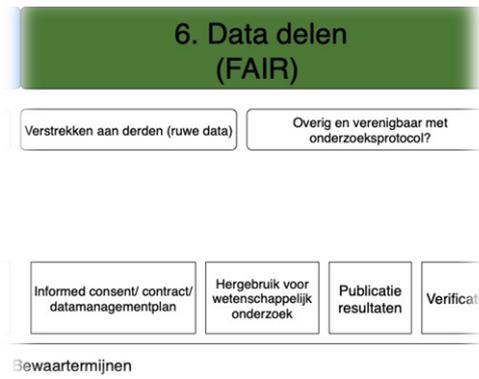
- het vastgestelde (interne) beleid en regels om gegevens intern op te slaan is geïmplementeerd;
- er een procedure binnen de faculteit is geïmplementeerd waarmee verwerkerovereenkomsten afgesloten kunnen worden met derde partijen die in opdracht gegevens verwerken (opslaan);

De **onderzoeker** dient ervoor zorg te dragen dat:

- gegevens zijn opgeslagen in de interne faciliteit;
- er verwerkerovereenkomsten zijn afgesloten zijn met derde partijen die in opdracht gegevens verwerken (opslaan).



### 3.7 Stap 6: FAIR principes



Zoals in de Gedragscode wetenschappelijke integriteit 2018 staat benoemd onder *normen voor goede onderzoekspraktijken*:

*11. Maak de onderzoeksgegevens en de onderzoeksdata na afloop van het onderzoek zoveel mogelijk publiek beschikbaar. Leg, als onderzoeksgegevens en/of de onderzoeksdata niet voor het publiek beschikbaar gemaakt kunnen worden, de valide redenen<sup>15</sup> daarvoor vast.*

Onder die valide redenen valt onder andere de bescherming van persoonsgegevens<sup>16</sup>:

*Optimal reuse of research data*

*14. UNDERLINES that research data originating from publicly funded research projects could be considered as a public good, and ENCOURAGES the Member States, the Commission and stakeholders to set optimal reuse of research data as the point of departure, whilst recognising the needs for different access regimes because of Intellectual Property Rights, personal data protection and confidentiality, security concerns, as well as global economic competitiveness and other legitimate interests. Therefore, the underlying principle for the optimal reuse of research data should be: "as open as possible, as closed as necessary".*

Dit kan ertoe leiden dat delen van een onderzoek, om redenen van het borgen van de privacyrechten van de bij het onderzoek betrokkenen, niet publiek beschikbaar kunnen worden gemaakt. In een data management plan, kan, in de ontwerpfase van een onderzoek, vaak per werkpakket worden aangegeven of de onderzoeksgegevens na het onderzoek al dan niet publiek beschikbaar kunnen worden gemaakt. Dit is voor de financiering van onderzoek bijvoorbeeld geen bezwaar.

In het algemeen kan voor onderzoeksdata die voor een groot deel uit (bijzondere categorieën van) persoonsgegevens bestaan worden vastgesteld dat de (statistische) waarde van de onderzoeksgegevens afneemt, naarmate deze (sterk) wordt gepseudonimiseerd of

<sup>15</sup> Valide redenen, waaronder vertrouwelijkheid, kunnen worden gevonden in: Europese Raad, Raadsconclusies: The transition towards an Open Science system, paragraph 14 (Brussel, 27/05/2016, 9526/16, via: [data.consilium.europa.eu/doc/document/ST-9526-2016-INIT/en/pdf](http://data.consilium.europa.eu/doc/document/ST-9526-2016-INIT/en/pdf)).

<sup>16</sup> ibidem, pagina 8



geanonimiseerd. Het publiek beschikbaar maken van geanonimiseerde onderzoeksgegevens lijkt dan ook minder zinvol.

In een data archief zoals bijvoorbeeld dat van DANSeasy<sup>17</sup> kan echter op verschillende manieren toegang worden verleend aan verschillende doelgroepen. Zo kan ervoor worden gekozen dat wanneer iemand toegang wenst tot de onderzoeksdata, deze zich wendt tot de hoofdonderzoeker om toegang tot de onderzoeksgegevens te vragen, het doel van het onderzoek en het gebruik van de betreffende onderzoeksgegevens toe te lichten, en kan het hergebruik van de betreffende onderzoeksgegevens bijvoorbeeld zijn voorbehouden aan onderzoekers, of meer specifiek, onderzoekers uit een bepaalde discipline. Op deze manier kan adequaat en zorgvuldig gehoor worden gegeven aan het uitgangspunt voor de toegang tot onderzoeksdata: "as open as possible, as closed as necessary".

---

<sup>17</sup> DANSeasy is het data archief van DANS (Data Archiving and Networked Services, een instituut van KNAW/NWO): <https://easy.dans.knaw.nl/ui/home>



## 4 Wat kan de universiteit doen?

Naast een aantal verplichtingen die de AVG met zich meebrengt, kan de universiteit ook het een ander doen om te zorgen dat onderzoekers, onderzoeksondersteuners en bestuurders voldoen aan de principes van de AVG. Het gaat om maatregelen op 3 terreinen:

- 1 Organisatorisch
- 2 Technisch
- 3 Juridisch

Dit hoofdstuk bevat een aantal strategieën die universiteiten toepassen om te voldoen aan de AVG.

### 4.1 Organisatorische maatregelen

#### *Visie, beleid*

De implementatie van het borgen van privacyrechten binnen de instelling betreft het organisatorisch borgen van een nieuwe structurele verantwoordelijkheid van de universiteit. Deze taak hangt samen met de missie en strategie van de instelling en is daar een vast onderdeel van. Deze visie deelt de instelling via haar externe communicatie (website, privacy statement, jaarverslag, etc.) met haar medewerkers, studenten, gasten en partners. In de privacyvisie van de instelling kan bijvoorbeeld tot uitdrukking komen dat privacy wordt gezien als een corporate responsibility<sup>18</sup> voor allen, maar waarbij ook specifieke rollen en verantwoordelijkheden zijn belegd en eenieder weet wat de eigen verantwoordelijkheid is, hoe deze vorm te geven, met welke middelen, en bij wie ondersteuning kan worden gevonden.

In het beleid wordt ook aangegeven hoe personen hun privacyrechten kunnen uitoefenen, bijvoorbeeld via een inzageverzoek en hoe de processen, rollen en verantwoordelijkheden achter het borgen van deze privacyrechten zijn belegd. Vaak wordt in privacybeleid een relatie gelegd met beleid op het gebied van (cyber)security en informatiebeveiliging. Dit kan bijvoorbeeld blijken door de implementatie van een dataclassificatie met bijbehorende merkingen (zie bijvoorbeeld Bijlage 3). Vanuit bijvoorbeeld jaarlijks gepubliceerde dreigingsbeelden<sup>19</sup> kan worden ingeschat of de genomen organisatorische en technische maatregelen nog steeds adequaat zijn.

#### *Rollen en verantwoordelijkheden*

Bij de implementatie van het borgen van privacyrechten binnen de instelling zijn verschillende vormen van samenwerking cruciaal; zowel tussen faculteiten en centrale diensten als tussen de centrale diensten onderling. Hierbij is de afbakening van de rollen en verantwoordelijkheden van belang om te borgen dat de afgesproken taken ook worden uitgevoerd, gemonitord en de plan - do - check - act cyclus voor de verschillende verwerkingen invulling krijgt. Samenwerking tussen de ondersteunende diensten maakt dat de gekozen stappen juridisch correct zijn, technisch goed worden gefaciliteerd of afgedwongen en passen binnen de principes en architecturen van de instelling. Vaak is er

<sup>18</sup> Zie bijvoorbeeld de white papers over Accountability-Based Privacy Governance van het Centre for Information Policy Leadership (CIPL): <http://www.informationpolicycentre.com/cipl-white-papers.html>.

<sup>19</sup> Zie bijvoorbeeld het jaarlijkse SURF cyberdreigingsbeeld 2017:

<https://www.surf.nl/nieuws/2017/12/cyberdreigingsbeeld-2017-toont-belangrijkste-dreigingen.html>.



sprake van centrale verantwoordelijkheden (FG, CISO, CIO, ICT, Legal, Academische Zaken, Research Services, instellingsbrede commissies (ethische commissie, wetenschappelijke integriteit)) en facultaire verantwoordelijkheden (decaan, directeuren onderzoek en -bedrijfsvoering, afdelingshoofden, ethische commissies, onderzoeksondersteuning (data stewards, privacy officers)). Onderlinge afstemming, het gezamenlijk leertraject via centrale en facultaire privacy en security awareness en trainingsprogramma's dragen bij aan de kwaliteit van de samenwerking en de resultaten van deze samenwerking. Het verschil in de rollen en verantwoordelijkheden van het CvB, de FG, de privacy organisatie moet voor de gehele organisatie duidelijk zijn. Wie communiceert c.q. rapporteert waarover naar wie, wie legt de AVG uit, wie doet formele externe communicatie en hoe zien de interne escalatie paden er uit?

#### *Ondersteuningsstructuur binnen de instelling*

De implementatie van het borgen van privacyrechten binnen de instelling geschiedt vanuit een privacy organisatie, samengesteld vanuit medewerkers van de centrale stafdiensten en de faculteiten. Hierbij wordt afgesproken hoe de samenwerking plaatsvindt en hoe deze in processen en met informatie- en ICT-middelen wordt gefaciliteerd. Hoe vindt bijvoorbeeld de interactie plaats tussen de data stewards (research data management), de ethische commissies of de internal review boards, de privacy officers, de research funding staff, de technical transfer office staff, contractmanagement, de controllers en de projectleiders onderzoek? Dit dient op zo'n manier te gebeuren dat het onderzoek soepel wordt gefaciliteerd en niet gehinderd. In de samenwerking tussen collega's van centrale stafdiensten en faculteiten kan voorts goed en effectief opvolging worden gegeven aan de verzoeken van individuen (inzageverzoeken, verzoek om correctie, verzoek om verwijdering, etc.) omdat de registraties waarin verwerkingen plaatsvinden van deelnemers aan het onderzoek mogelijk in centrale en decentrale registraties plaatsvinden. Voor de kwaliteit van de dienstverlening geldt de aanbeveling de medewerkers in de privacy organisatie adequaat te scholen en door middel van een erkende certificering, bijvoorbeeld het CIPP/e certificaat van het IAPP<sup>20</sup>, aantoonbaar over de juiste basiskennis te laten beschikken.

#### *Bewustwording*

Aan de basis van het kunnen nemen van de eigen verantwoordelijkheid binnen de instelling staat een basisniveau aan kennis en van correct gedrag. Dit betreft kennis van persoonsgegevens, wat verwerkingen zijn en de leidende privacy principes. In het gedrag geldt dat de onderzoekers en onderzoeksondersteuners weten wat ze in verschillende contexten moeten doen en waarom, welke middelen zij veilig kunnen inzetten en hoe zij risico-inschattingen kunnen doen met betrekking tot privacy en security. Naast een generiek basisniveau identificeert de instelling bepaalde risicogebieden voor wat betreft de verwerkingen van persoonsgegevens, vanwege de aard van het onderzoek (vaak onderzoek naar kwetsbare groepen, vaak verwerking van bijzondere categorieën van persoonsgegevens) en traint deze specifieke doelgroep in de toepassing van de juiste middelen (beveiligde samenwerkingsplatforms, technieken om data te pseudonimiseren of anonimiseren, vastgelegde procedures en organisatorische maatregelen) en het gebruik van de juiste documenten (informed consent, privacy statement, verwerkersovereenkomst, Non Disclosure Agreement, etc.). Belangrijk aspect van bewustwording is het meten van het

---

<sup>20</sup> Zie: <https://iapp.org/certify/cippe/>.



kennisniveau en gedrag, zodat waar nodig bijgestuurd kan worden. Als mensen weten wat ze op welke manier moeten doen volgen de privacy verbeterende processen vanzelf.

De Autoriteit Persoonsgegevens (AP) biedt instrumenten die u kunnen helpen om de AVG na te leven, zoals de website [hulpbijprivacy.nl](https://hulpbijprivacy.nl) en de AVG-regelhulp, maar ook guidelines die zijn opgesteld samen met de andere privacytoezichthouders in Europa.

#### *Samenwerking*

Nederland kent een hoge organisatiegraad, waarin deskundigen elkaar in verschillende gremia ontmoeten om effectief samen te werken en kennis en best practices te delen. Voorbeelden hiervan zijn het FG-netwerk binnen de VSNU, de SCIPR groep vanuit SURF en het Landelijk Coördinatiepunt Research Datamanagement (LCRDM). Samenwerking tussen de instellingen maakt dat de sector leert en in volwassenheid in privacy bevorderend gedrag groeit.

## **4.2 Technische maatregelen**

#### *Privacy by Design and Privacy by Default*

Het concept van Privacy by Default verplicht organisaties de privacy van hun gebruikers te beschermen door de instellingen en functies van de producten of diensten standaard (by default) op de meest privacy-vriendelijke stand te zetten. Voor onderzoekers betekent dit bijvoorbeeld standaardinstellingen bij online opslag van gegevens, of end-to-end encryptie waarvan de sleutel bij pseudonimisering alleen bij de (hoofd-)onderzoeker bekend is.

#### *Veilige en betrouwbare systemen*

Zoals gezegd moet u zorgen dat uw technische systemen om data te verwerken veilig en betrouwbaar zijn. U kunt hier bijvoorbeeld ook denken aan Privacy by Design, waarbij u uw technisch systeem op een privacy-vriendelijke manier inricht.

#### *Tooling en hulpmiddelen*

Niet al het onderzoek maakt gebruik van persoonsgegevens of bijzondere persoonsgegevens. Maar voor onderzoekers die wel deze gegevens verwerken zal het welkom zijn dat zij zich op een makkelijke manier en op het juiste niveau kunnen informeren over hun rol als onderzoeker bij het borgen van privacy in wetenschappelijk onderzoek. Vervolgens zal de onderzoeker, ondersteund door deskundigen binnen de instelling, rekening houdend met deze kennis, invulling willen geven aan het borgen van privacy binnen onderzoek door gebruik te maken van bijvoorbeeld instrumenten, beslisbomen, tooling, infrastructuur, contracten en overeenkomsten. Voorbeelden van opleidingen en trainingen, informatiemateriaal, beleid, instructiemateriaal en case beschrijvingen, passend bij de verschillende wetenschappelijke disciplines, zullen een welkome inspiratiebron zijn voor alle betrokkenen. Onderzoekers en onderzoeksondersteuners worden uitgenodigd om deze voorbeelden in kaart te brengen en voor elkaar beschikbaar te maken.

## **4.3 Juridische maatregelen**

#### *Verwerkingsregister*

Onder de AVG geldt een verantwoordingsplicht, wat inhoudt dat de universiteit moet kunnen aantonen dat zij in overeenstemming met de AVG handelt. Het bijhouden van een register



van verwerkingsactiviteiten is onderdeel van de verantwoordingsplicht. De AVG stelt echter dat voor categorieën van verwerkingen geldt dat een register dient te zijn aangelegd. Voor onderzoek geldt dus ook dat niet voor elk individueel onderzoek een beschrijving van (de keten van) verwerkingen hoeft te worden geregistreerd, maar dat registratie van een categorie van verwerkingen volstaat. Dit voorkomt onnodige bureaucratie voor zowel de onderzoeker als de privacy-organisatie. Onderzoek als keten van verwerkingen is als verwerking te onderscheiden van bijvoorbeeld een verwerking 'inschrijven studenten'; voor dit laatste geldt dat het een vastgesteld terugkerend proces is waarbij vele medewerkers betrokken zijn. Voor onderzoek geldt dat een onderzoeker vaak verantwoordelijk is voor verschillende onderzoeksprojecten die qua typen verwerkingen vaak niet veel verschillen.

Ter illustratie: de basis voor een registratie van onderzoek zou er uit kunnen zien als Bijlage 4. Hiermee wordt voldaan aan de verplichting (cf. artikel 30) van de AVG. Onderzoek zal overeenkomsten vertonen op basis van de aard van de persoonsgegevens, de aard van de samenwerking en de aard van de geografische samenwerking. Het zal vervolgens blijken dat er voor de te identificeren categorieën van onderzoek bekende geïdentificeerde risico's zullen zijn en bekende mitigerende maatregelen (technisch en organisatorisch) en bijbehorende passende juridische overeenkomsten.

#### *Verwerkersovereenkomsten*

Heeft u uw gegevensverwerking uitbesteed aan een verwerker? Beoordeel dan of de overeengekomen maatregelen in de bestaande hoofdovereenkomst met uw verwerker nog steeds toereikend zijn. En of deze voldoen aan de eisen die de AVG stelt aan verwerkersovereenkomsten. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan. Niet voor elke vorm waarbij persoonsgegevens door verschillende partijen worden gebruikt is een verwerkersovereenkomst vereist. Voor doorgifte van persoonsgegevens en voor verwerkingen van persoonsgegevens in een samenwerking geldt dat weliswaar afspraken gemaakt dienen te worden, maar deze zijn niet identiek aan een verwerkersovereenkomst.

#### *Data protection impact assessment*

Onder de AVG kunt u verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacy-risico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. De universiteiten bieden ondersteuning aan onderzoekers om te bepalen of een DPIA nodig is bij bepaald onderzoek.

#### *Functionaris voor de Gegevensbescherming*

Alle universiteiten moeten een Data Protection Officer (of: Functionaris voor Gegevensbescherming) aanstellen, een persoon die intern in de organisatie zorgdraagt dat alle regels uit de AVG worden nageleefd. Bij grotere onderzoeksprojecten met verschillende consortiumpartners is het soms raadzaam om een eigen Data Protection Officer toe te wijzen.

#### *Meldplicht datalekken*

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan.



#### 4.4 Monitoren van ontwikkelingen binnen de universiteit

Met de AVG is privacy veel meer dan voorheen een gedeelde verantwoordelijkheid geworden. Daarmee vraagt de invoering van passende technische en organisatorische maatregelen binnen een zeer complexe organisatie als een universiteit een goed overzicht van de fase waarin de organisatie zich bevindt. Een benadering die daarbij goed past is het "Maturity model privacy<sup>21</sup>". Daarmee wordt duidelijk dat op verschillende niveaus van volwassenheid van de organisatie verschillende diensten en producten nodig zijn.

**Capability Maturity Model for Safeguarding Privacy in Academic Research or: *The GDPR\* Readiness Levels***  
Marlon Domingus, April 2017 version 0.3

	Level 1. Initial	Level 2. Repeatable	Level 3. Defined	Level 4. Managed	Level 5. Optimised
<b>Across the university</b>	<p>'What is this acronym: "GDPR" everyone is talking about?'</p> <p>'I'm afraid we have to do something related to this, but don't know what, why and how.'</p> <p>University appoints a <i>Data Protection Officer (DPO)</i>.</p>	<p>People across the university are meeting on a regular basis to share their practices, based on application of the <i>Privacy Impact Assessment (PIA)</i>. A common language and understanding emerges on how to safeguard the privacy of data subjects in the collection, processing and sharing of personal data.</p>	<p>A <i>standard data protection process</i> is defined and communicated, in which people in various roles have a responsibility for their part and/or the whole. Generic instruments are evaluated, selected and implemented. A shared vocabulary exists to understand each other whilst working on tailored solutions.</p>	<p>Typical research scenarios are fully supported, <i>GDPR</i> compliant, as a standard service. Ongoing evaluation is in place for improving the quality of the <i>GDPR</i> compliance support. Tailored support is in place for specific (new / complex) aspects in research scenarios.</p>	<p><i>GDPR</i> is considered a starting point for the University to develop its own distinctive position. This position is <i>above par</i> and reflected in the University's policy, guidelines, principles of ethics committees, and as such recognisable both in research and research support.</p>
<b>Faculty</b>	<p>Faculty dealing with sensitive data have a heterogeneous understanding of <i>privacy</i> and <i>data protection</i>.</p> <p>What appropriate behaviour is, is a matter of opinions. In general 'privacy' is considered relevant, but a black box.</p>	<p>Faculty are discussing data protection practices from within their discipline.</p> <p>Faculty develop a strategy (with or without central support) to comply to various (external) data protection requirements by, e.g. research funders.</p>	<p>Faculty are familiar with what is expected of them in terms of safe-guarding the privacy of their data subjects, and have access to tooling and support to do so, in their administrative tasks and teaching capacities.</p> <p>Solutions for generic research scenarios are available for faculty.</p>	<p>Faculty routinely design their research in terms of <i>PBD</i> and have access to a library of relevant and tailored documents to support them. Privacy is no longer considered an <i>external threat</i>, or burden, but the obvious way to be transparent on how to treat the rights of data subjects / citizens.</p>	<p><i>GDPR</i> is considered the baseline from a research professionalism perspective. Privacy is seen as an <i>important strength</i>. By ensuring trust in transparent and responsible research, privacy is an enabler of societal relevance and impact of research.</p> <p>Regular checks are built in, to check what to improve and how.</p>
<b>Legal</b>	<p>Legal staff is getting acquainted with the <i>GDPR</i>. Examining the rights, responsibilities, roles and responsibilities.</p> <p>Discussing available relevant (best and worst) practices.</p>	<p>Relevant examples, practices, instruments and relevant legal expertise are combined. Templates and model provisions are drafted to cover the relevant area.</p> <p>The first <i>Register</i> draft is created. <i>PIA</i> strategies are explored.</p>	<p>All <i>GDPR</i> concepts, rights and roles are clear, defined and documented in the context of academic research.</p> <p>Legal staff pro actively contribute to research support with <i>Privacy By Design and by Default (PBD)</i> implementations.</p>	<p>All roles, instruments, contracts and template wordings are in place for <i>GDPR</i> compliant support in various research scenarios. Legal staff act as embedded research supporters, in cooperation with the <i>DPO</i> and the ethical committee(s).</p>	<p>Legal staff is actively involved in privacy impact assessments of (1) new innovative tooling and instruments and (2) innovative forms of cooperation in research, to assess the responsible application for research purposes.</p>
<b>CIO</b>	<p>Privacy is discussed in the context of governance and e-strategy. Privacy principles are discussed in the context of Higher Education Reference Architecture.</p>	<p>Privacy is included in the Business Function Model, Information Model, Business Process Model, Application Model &amp; Platform. A privacy policy is drafted.</p>	<p>A privacy policy enters into force. Guidelines are distributed. An updated information security policy is implemented. CIO designs <i>PBD</i> strategies.</p>	<p>All relevant <i>GDPR</i> aspects are addressed in the privacy-, information security policy and governance. CIO appoints privacy officers in collaboration with Legal.</p>	<p>CIO is at all times willing and able to demonstrate the <i>GDPR</i> compliance of information processing within the university. Checks and balances are in place to stimulate responsible behaviour.</p>
<b>IT</b>	<p>Privacy is typically approached from a information security point of view. Typically public cloud tooling is banned, usually with no alternative available. Many opinions on what is relevant and required.</p>	<p>Relevant <i>Privacy Enhancing Technologies (PETS)</i> are explored and tested in pilots with faculty. IT recognises the validity of research as a target group, distinct from support for education and business operations.</p>	<p>A chain of <i>PETS</i> is implemented as basic services for research.</p> <p>Selection and prioritisation in collaboration with Faculty, Legal and CIO.</p>	<p>The baseline <i>PETS</i> are embedded in the working environment of researchers and supported (both individually and in workshops for faculty).</p>	<p>Support for the whole research life cycle for both open science and closed science is available as self service from the IT service catalogue. A process is in place to design, implement and steward tailored <i>PET</i> solutions.</p>


 See: <https://creativecommons.org/licenses/by-nc/4.0/legalcode>
 \* See for EU General Data Protection Regulation (GDPR): <http://www.privacy-regulation.eu/en/index.htm>

<sup>21</sup> Bron: [https://www.edugroepen.nl/sites/RDM\\_platform/RDM\\_Blog/Lists/Posts/Post.aspx?ID=12](https://www.edugroepen.nl/sites/RDM_platform/RDM_Blog/Lists/Posts/Post.aspx?ID=12).



## 5 Bijlagen

De bijlagen van deze code worden als losse documenten toegevoegd.

**Bijlage 1 EUR voorbeeld: Overeenkomst Gezamenlijke Verwerkingsverantwoordelijken, Joint Controller Agreement**

**Bijlage 2 EUR voorbeeld: Informed Consent formulier**

**Bijlage 3 EUR voorbeeld: Dataclassificatie**

**Bijlage 4 EUR voorbeeld: registratie van onderzoek in het register van verwerkingen**