

PRIVACY IN ONDERZOEK – 10 BELANGRIJKE REGELS

In veel wetenschappelijk onderzoek worden persoonsgegevens gebruikt. Voor onderzoekers is het van belang te weten welke regels gelden bij het gebruik van persoonsgegevens. Het volgende overzicht geeft de 10 belangrijkste regels.

Het is van belang op te merken dat dit overzicht bedoeld is om eerste indruk te krijgen van de geldende privacywetgeving (de Algemene Verordening Gegevensbescherming (**AVG**) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (**UAVG**)) en niet bedoeld is als uitputtend overzicht.

1. Persoonsgegevens

- Alle informatie over een geïdentificeerde of *identificeerbare* natuurlijke persoon wordt gezien als een persoonsgegeven. Identificatie kan direct plaatsvinden. Bijvoorbeeld aan de hand van naam, geboortedatum en/of adres. Identificatie kan ook indirect plaatsvinden. Dat wil zeggen dat ook gegevens die niet tot directe identificatie van een persoon leiden, maar met redelijkerwijs in te zetten middelen wel kunnen leiden tot identificatie, als persoonsgegevens moeten worden gezien. Bijvoorbeeld: een deelnemersnummer of de combinatie van postcode en huisnummer.
- Een naam is niet altijd nodig om een persoon te identificeren. Bepaalde identiteitskenmerken, eventueel in combinatie met andere kenmerken, kunnen voldoende zijn om tot identificatie te komen. Bijvoorbeeld: de mevrouw van 1.90 meter met grijs kort haar die rijdt in een rode cabrio of de meneer die helemaal rechts achterin de zaal die zit op de linkerstoel.
- Persoonsgegevens kunnen objectief of subjectief zijn. Bijvoorbeeld: Caspar vindt Lily sociaal en betrokken. Dit is een gegeven dat iets zegt over Caspar (zijn mening) én Lily (dat zij sociaal en betrokken is, volgens Caspar). Indien er persoonsgegevens gebruikt (verwerkt) worden dan zijn de AVG en UAVG van toepassing. Dat betekent dat o.a. deze 10 belangrijke regels gelden.

2. Pseudoniem ≠ anoniem

Pseudonimiseren betekent het verhullen van identiteit. Pseudonimisering maakt het mogelijk om (aanvullende) gegevens over een persoon te verwerken zonder dat diens identiteit direct kenbaar is. De direct identificerende gegevens worden dan vaak opgeslagen in een apart, versleuteld bestand (communicatiebestand). Het is van belang te weten dat gepseudonimiseerde/gecodeerde datasets geen anonieme datasets zijn. Pseudonimisering draagt bij aan een goede beveiliging van persoonsgegevens, maar betekent niet dat de betreffende gegevens anoniem zijn. Bij de verwerking van gepseudonimiseerde/gecodeerde persoonsgegevens zal nog steeds rekening moet worden gehouden met privacywetgeving.

3. Openbaar ≠ vrij te gebruiken

Persoonsgegevens uit 'openbare' bronnen zoals Instagram, Facebook en Twitter mogen niet vrij worden gebruikt. Elke verwerking van persoonsgegevens zal moeten voldoen aan de eisen van de privacywetgeving. 'Data scraping' met persoonsgegevens is dus niet zomaar toegestaan.

4. Altijd wettelijke grondslag vereist

Wanneer persoonsgegevens worden verwerkt, is *altijd* een wettelijke grondslag vereist. Zonder wettelijke grondslag mogen persoonsgegevens *niet* worden verwerkt en is de verwerking onrechtmatig. Binnen de context van wetenschappelijk onderzoek komen vaak twee mogelijkheden in beeld:

- Toestemming betrokkene > Om te kunnen spreken van rechtsgeldige toestemming moet sprake zijn van een *vrije, specifieke, geïnformeerde* en *ondubbelzinnige* wilsuiting van de betrokkene. Een betrokkene moet op voorhand weten waar hij toestemming voor geeft en wat er met zijn gegevens gebeurt. Dit betekent dat betrokkene vooraf ook moet worden geïnformeerd over de verdere verwerkingen die plaatsvinden met zijn persoonsgegevens, zoals koppelingen die worden gemaakt tussen bij hem verkregen gegevens en de gegevens uit andere (openbare) bronnen. Een aandachtspunt in dit verband is dat de wet bepaalt dat toestemming te allen tijde moet kunnen worden ingetrokken. Een intrekking heeft geen terugwerkende kracht, maar de persoonsgegevens van de betrokkene mogen vanaf dat moment niet verder worden verwerkt.
- Gerechtigd belang > Wanneer het vragen van toestemming onwenselijk (bijvoorbeeld vanwege de mogelijkheid van intrekking) of onmogelijk is (bijvoorbeeld omdat het gaat om een bestaande dataset), zou de wettelijke grondslag 'gerechtigd belang' bruikbaar kunnen zijn. Om hier een beroep op te kunnen doen, moeten worden voldaan aan drie voorwaarden:
 1. er moet sprake zijn van een gerechtigd belang van de verantwoordelijke of een derde;
 2. de verwerking moet noodzakelijk zijn om het gerechtigd belang te behartigen. Daarbij zijn proportionaliteit (het middel staat in verhouding tot doel) en subsidiariteit (er is geen minder ingrijpend middel beschikbaar) van belang; **en**
 3. het gerechtigd belang prevaleert boven het privacybelang van de betrokkenen.

5. Verbod verwerking bijzondere persoonsgegevens

De AVG kent naast 'gewone' persoonsgegevens ook bijzondere persoonsgegevens. De verwerking van bijzondere persoonsgegevens is verboden, tenzij sprake is van een uitzondering zoals vermeld in de AVG of de UAVG. Bijzondere persoonsgegevens zijn gegevens over: ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gezondheidsgegevens, iemands seksueel gedrag of seksuele gerichtheid en gegevens over strafrechtelijke veroordelingen en strafbare feiten. Wanneer deze gegevens worden verwerkt, betekent dit dat niet alleen moet worden nagegaan of sprake is van een wettelijke grondslag en kan worden voldaan aan de algemene gegevensbeschermingsbeginselen (zie hierna onder 6), er zal ook moet worden getoetst of het verbod op verwerking van bijzondere persoonsgegevens kan worden doorbroken. Binnen de context van wetenschappelijk onderzoek komen vaak twee ontheffingsgronden in beeld:

- Uitdrukkelijke toestemming
Een uitzondering op het verbod van verwerking van bijzondere persoonsgegevens is *uitdrukkelijke* toestemming van de betrokkene. De term *uitdrukkelijk* verwijst naar de manier waarop toestemming moet worden gegeven, de bovenstaande voorwaarden voor 'normale' toestemming zijn ook van toepassing.
- Uitzondering wetenschappelijk onderzoek
Als het onmogelijk is of onevenredige inspanning kost om uitdrukkelijke toestemming te vragen aan de betrokkenen, kan mogelijk een beroep worden

gedaan op de wettelijke uitzondering voor wetenschappelijk onderzoek. Er moet dan worden voldaan aan de volgende vier voorwaarden:

1. het onderzoek dient een algemeen belang;
2. de verwerking is noodzakelijk voor het betreffende onderzoek ;
3. het vragen van uitdrukkelijke toestemming blijkt onmogelijk of kost onevenredige inspanning; en
4. bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Let op, het Burgerservicenummer (BSN) mag alleen worden gebruikt als een specifieke wet dit voorschrijft. Op dit moment is er geen wet die voorziet in het gebruik van BSN binnen wetenschappelijk onderzoek. BSN mag daarom *niet* worden gebruikt voor wetenschappelijk onderzoek, ook niet met toestemming.

6. Algemene beginselen

Naast het bovenstaande, zal bij elke verwerking van persoonsgegevens ook moeten worden voldaan aan de algemene beginselen:

- a. Rechtmatigheid, behoorlijkheid en transparantie > Persoonsgegevens mogen alleen worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.
- b. Doelbinding > Persoonsgegevens mogen alleen worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. Verdere verwerking met het oog op wetenschappelijk onderzoek wordt niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd.
- c. Dataminimalisatie > Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt worden tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.
- d. Juistheid > Persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd. Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijd te wissen of te rectificeren.
- e. Opslagbeperking > Persoonsgegevens mogen niet langer worden opgeslagen dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is. In het kader van wetenschappelijk onderzoek mogen persoonsgegevens langer worden bewaard, mits passende en technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen.
- f. Integriteit en vertrouwelijkheid > Bij de verwerking van persoonsgegevens moet worden gezorgd voor passende beveiliging. Er dienen *technische en organisatorische* maatregelen te worden genomen om de gegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

7. Te verstrekken informatie

De betrokkenen zullen *altijd* - ook als op basis van gerechtvaardigd belang persoonsgegevens worden verwerkt en dus geen toestemming wordt gevraagd - duidelijk moeten worden geïnformeerd. Dit kan via een zogenaamde privacyverklaring. De Privacy Champions van de VU beschikken over een model privacyverklaring (NL & ENG). In een privacyverklaring wordt in ieder geval het volgende vermeld:

- de identiteit en contactgegevens van de verwerkingsverantwoordelijke;
- de doeleinden van de verwerking en de wettelijke grondslag;

- de ontvangers of categorieën van ontvangers van de persoonsgegevens;
- de bewaartermijn;
- de rechten van de betrokkenen;
- de doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte (= EU + Noorwegen, IJsland en Liechtenstein).

Dit geldt ook wanneer de persoonsgegevens niet worden verkregen bij de betrokkene zelf, maar via een andere bron. Wanneer het verstrekken van informatie aan de betrokkenen onmogelijk is of onevenredig veel inspanning zou vergen, dan wel het bereiken van de verwerkingsdoeleinden daardoor onmogelijk (dreigen te) worden gemaakt, biedt de AVG ruimte om te kunnen afzien van informatieverstrekking. Wel zal dan moeten kunnen worden onderbouwd dat toereikende waarborgen bestaan.

8. Gezamenlijk onderzoek / uitwisseling van onderzoeksdata

Indien de VU in het kader van onderzoek samenwerkt met andere instellingen en daarbij persoonsgegevens worden uitgewisseld dan moet worden nagedacht over de verdeling van verantwoordelijkheden ten aanzien van de privacywetgeving. Indien de VU het wetenschappelijk onderzoek in samenwerking met één of meer andere instellingen uitvoert, moet mogelijk een overeenkomst voor gezamenlijke verantwoordelijken worden gesloten. Indien onderzoek niet gezamenlijk wordt uitgevoerd, maar wel onderzoeksdata worden verstrekt aan of ontvangen van een andere instelling, dan moet er mogelijk een overeenkomst tussen zelfstandige verantwoordelijken worden gesloten. De Privacy Champions van de VU beschikken over modellen voor deze overeenkomsten (NL & ENG).

9. Verwerkersovereenkomst(en)

Wanneer bij het onderzoek gebruik wordt gemaakt van diensten van derden waarbij persoonsgegevens *ten behoeve van* de VU worden verwerkt (bijvoorbeeld: enquêtetools, cloudopslag of online deelnemerstools), zal met deze dienstverleners (verwerkers) een zogenaamde verwerkersovereenkomst moeten worden afgesloten. Dit is een wettelijke verplichting, die bedoeld is om te waarborgen dat de persoonsgegevens waar de VU verantwoordelijk voor is volgens de wet worden verwerkt. Een belangrijke afspraak in de verwerkersovereenkomst is dat de dienstverlener de persoonsgegevens uitsluitend verwerkt volgens de instructies van de VU (en eventueel de samenwerkingspartners) en niet voor eigen doeleinden. Daarnaast is van belang duidelijke afspraken te maken over de beveiliging, zeker wanneer het om gevoelige of bijzondere persoonsgegevens gaat. De Privacy Champions van de VU beschikken over een model verwerkersovereenkomst (NL & ENG).

10. Internationale doorgifte

Persoonsgegevens mogen niet naar landen buiten de Europese Economische Ruimte (EER) of internationale organisaties worden doorgegeven, tenzij wordt voldaan aan specifieke wettelijke vereisten. Er is sprake van internationale doorgifte als persoonsgegevens worden opgeslagen op een server in een land buiten de EER of wanneer een organisatie buiten de EER de persoonsgegevens ontvangt of kan inzien. Doorgifte naar landen buiten de EER is toegestaan:

- naar landen ten aanzien waarvan de Europese Commissie (EC) een '[adequaateitsbesluit](#)' heeft genomen. Op dit moment zijn dit 13 landen: Andorra, Argentinië, Canada ([let op](#), alleen voor commerciële activiteiten), Faeröer Eilanden, Guernsey, Israël, Isle of Man, Japan, Jersey, Nieuw-Zeeland, Uruguay, de Verenigde Staten ([let op](#), alleen voor organisaties die zijn gecertificeerd onder het [Privacy Shield](#)) en Zwitserland;

Naar landen waarvoor de EC géén adequaateitsbesluit heeft genomen mogen persoonsgegevens alleen worden doorgegeven:

- wanneer [passende waarborgen](#) worden getroffen, zoals Standard Contractual Clauses (SCC);

- op basis van uitzonderingen voor specifieke situaties (zie artikel 49 AVG).

OM REKENING MEE TE HOUDEN

Om ervoor te zorgen dat de privacy binnen het onderzoek goed kan worden geborgd, is het in ieder geval van belang om *voorafgaande* aan het onderzoek de volgende vragen te beantwoorden:

- Welke persoonsgegevens worden op welk moment in het onderzoek verwerkt?
- Bij wie of wat worden de persoonsgegevens verzameld?
- Met welke doelen worden de persoonsgegevens verwerkt? Zijn deze doelen specifiek, uitdrukkelijk en gerechtvaardigd?
- Hoe worden de persoonsgegevens verwerkt?
- Op basis van welke wettelijke grondslag(en) worden de persoonsgegevens verwerkt?
- Worden bijzondere persoonsgegevens verwerkt? Zo ja, is er een ontheffingsgrond voor de verwerking van deze gegevens?
- Welke organisatie(s) en/of welke personen zijn op welk moment betrokken bij de verwerking van de verschillende persoonsgegevens? Zijn zij (mede)verwerkingsverantwoordelijke of verwerkers?
- Worden persoonsgegevens doorgegeven naar landen buiten de Europese Economische Ruimte?
- Hoe worden de betrokkenen geïnformeerd over de gegevensverwerkingen?
- Welke technische systemen/middelen worden gebruikt bij de verwerking van de persoonsgegevens en welke afspraken met de leveranciers hiervan zijn eventueel al gemaakt?
- Hoe wordt gezorgd voor adequate beveiliging?