

Ben je student en ga je  
zelfstandig onderzoek doen?

Dit moet je weten van de AVG

# Inhoudsopgave

<b>Inleiding</b> .....	<b>4</b>
<b>Hoe ga je te werk?</b> .....	<b>5</b>
Ethische toetsing? Ondersteuning van privacy officer? .....	5
<b>1. Basisbegrippen</b> .....	<b>6</b>
Persoonsgegevens.....	6
Anoniem en pseudoniem.....	6
Betrokkene .....	8
Gevoelige en bijzondere persoonsgegevens .....	8
Verwerken.....	10
Algemene verordening gegevensbescherming (AVG) .....	10
Wettelijke grondslag .....	11
<b>2. Dataminimalisatie</b> .....	<b>13</b>
Noodzakelijkheid.....	13
Doelbinding .....	13
Bewaartermijnen .....	14
<b>3. Informatiebeveiliging</b> .....	<b>16</b>
Enkele belangrijke richtlijnen.....	16
Datalekken herkennen en melden.....	18
<b>4. Rechten van deelnemers</b> .....	<b>19</b>
<b>5. Deelnemers informeren</b> .....	<b>21</b>
Hoe kun je je deelnemers het beste informeren? .....	21
Welke informatie moet je aan je deelnemers verstrekken? .....	22
Voorbeeld van een informatiebrief .....	24

<b>6. Deelnemers om toestemming vragen .....</b>	<b>26</b>
Voorwaarden voor rechtsgeldige toestemming .....	26
Kinderen .....	27
Toestemming aantoonbaar maken.....	28
Voorbeeld van een toestemmingsverklaring .....	29
<b>7. Je uiteindelijke werkstuk of scriptie .....</b>	<b>30</b>
Schrijven.....	30
Openbaar maken.....	30

## Inleiding

Je bent student en je gaat zelfstandig (wetenschappelijk) onderzoek doen. Dan is de kans reëel dat je te maken krijgt met [persoonsgegevens](#). Voor de ene faculteit of studierichting geldt dat meer dan voor de andere. Maar wát je ook studeert, het is hoe dan ook belangrijk om op de hoogte te zijn van de 'privacyregels' uit de [Algemene verordening gegevensbescherming](#) (AVG) en het bijbehorende universitaire beleid. In deze brochure lees je er meer over.

Zoals uit de titel al blijkt, is deze brochure in de eerste plaats relevant als je – in het kader van je studie! – *zelfstandig* onderzoek gaat doen, hetzij in je eentje, hetzij in een groepje. Werk je mee aan het onderzoek van een docent of begeleider? Dan zijn de *principes* uit deze brochure zeker van belang, maar werken sommige dingen toch nét iets anders. Het is dan de verantwoordelijkheid van je docent of begeleider om uit te leggen hoe dat precies zit. Hij of zij zal jou instructies geven, gebaseerd op de AVG en het universitaire beleid. Wat de *achtergronden* van die instructies zijn, kun je dan weer lezen in deze brochure.

Veel succes met je onderzoek!

**Goed om te weten!** Ga je na je studie verder als onderzoeker onder contract bij een universiteit (bijvoorbeeld als PhD'er), dan gelden er enigszins afwijkende regels. In deze brochure is dat aangegeven in oranje kaders.

## Hoe ga je te werk?

1. Lees in ieder geval [hoofdstuk 1](#), zodat je op de hoogte bent van de basisbegrippen die te maken hebben met privacy en andere vormen van bescherming van persoonsgegevens.
2. Houd bij het opzetten van je onderzoek rekening met de informatie in de hoofdstukken [2](#), [3](#) en [4](#).
3. Zodra je precies weet hoe jouw onderzoek eruit gaat zien, kun je een informatiebrief voor je deelnemers opstellen ([hoofdstuk 5](#)) en kun je bepalen wat er in je toestemmingsverklaring moet komen te staan ([hoofdstuk 6](#)).
4. Waar je op moet letten bij het schrijven en eventueel publiceren van je paper of scriptie lees je in [hoofdstuk 7](#).

### Ethische toetsing? Ondersteuning van privacy officer?

Op de meeste faculteiten wordt gangbaar student-onderzoek niet ethisch getoetst door een Facultaire Ethische ToetsingsCommissie (FETC). Het is aan de docent of begeleider om de ethische aspecten van het onderzoek in de gaten te houden. **Let op!** Bij **FSW** vindt er wél een verplichte toetsing plaats voor bachelor- en masterthesisprojecten.

Zo ook kun je op de meeste faculteiten voor gangbaar studentonderzoek niet rechtstreeks een beroep doen op ondersteuning door een privacy officer (PO). Dit betekent dat je dus ook voor AVG-kwesties moet aankloppen bij je docent of begeleider. Wanneer deze er niet uitkomt, kan hij of zij wél advies inwinnen bij de privacy officer van dienst.

**Let op!** Heb je *concrete plannen* om je onderzoeksresultaten te publiceren in een wetenschappelijk tijdschrift en is je docent of begeleider het daarmee eens? Dan is bij bepaalde faculteiten ethische toetsing juist wél verplicht en kun je bovendien terecht bij de facultaire privacy officer. Informeer hiernaar bij je docent/begeleider.

# 1. Basisbegrippen

Om de informatie in deze brochure te kunnen begrijpen en om je onderzoek goed te kunnen inrichten, moet je op de hoogte zijn van de betekenis van een aantal basisbegrippen.

## Persoonsgegevens

Persoonsgegevens (ook wel: persoonlijke gegevens, *personal data* of *personally identifiable information*) wordt gedefinieerd als: alle informatie over een levende persoon van wie je weet wie het is of van wie je dat te weten zou kunnen komen. Gegevens over overleden personen en over organisaties of voorwerpen zijn dus geen persoonsgegevens.

### Voorbeelden:

- Namen en foto's zijn uiteraard persoonsgegevens, maar bij bepaalde veel voorkomende namen weet je zonder verdere context niet precies om wie het gaat.
- "Willemsparkweg 826 in Amsterdam"<sup>1</sup> is géén persoonsgegeven, maar "De hoofdbewoner van Willemsparkweg 826 in Amsterdam heeft een frietkraam" is dat wél, en "De dader van dit misdrijf woont op Willemsparkweg 826 in Amsterdam" ook.
- Stemgeluid is een persoonsgegeven (mensen zijn herkenbaar aan hun stem) en de antwoorden die mensen in een interview geven, zijn ook persoonsgegevens.

## Anoniem en pseudoniem

Gegevens die wel over mensen gaan, maar waarvan je met geen mogelijkheid (meer) kunt achterhalen bij welke persoon ze horen, noemen we **anoniem**. Anonieme gegevens zijn geen persoonsgegevens, en daarom is de AVG er niet op van toepassing. Het is dus slim om te

---

<sup>1</sup> Dit is een niet-bestaand adres.

proberen je gegevens zo snel mogelijk te **anonymiseren**, want dan ben je niet meer gebonden aan de regels van de AVG. **Let op:** anonymiseren is echt een lastige klus. Het behelst veel méér dan het weghalen van namen.

Soms hoor je ook de term **pseudoniem**. Bij pseudonieme gegevens is het nog wél mogelijk om – aan de hand van aanvullende informatie – vast te stellen op wie die gegevens betrekking hebben. Hier is de AVG dus wél van toepassing. We kennen de term pseudoniem vooral van bijvoorbeeld schrijvers die niet onder hun eigen naam publiceren, maar onder een pseudoniem. Er is dan informatie beschikbaar (bij de uitgever bijvoorbeeld) over de ware identiteit van de schrijver.

Het ‘pseudoniem maken’ of **pseudonimiseren** van persoonsgegevens is een veelgebruikte beveiligingsmaatregel.

**Voorbeeld:** Neem de eerdergenoemde zin: “De hoofdbewoner van Willemsparkweg 826 in Amsterdam heeft een frietkraam”.

Als je daarin “Willemsparkweg 826 in Amsterdam” vervangt door [adres1] krijg je:

“De hoofdbewoner van [adres1] heeft een frietkraam” .

Dit is in principe een *anonieme* zin; er is kennelijk iemand die ergens hoofdbewoner is en die een frietkraam heeft, maar je hebt geen idee wie dat zou kunnen zijn.

Soms is het echter nodig om de oorspronkelijke tekst nog te kunnen reconstrueren, bijvoorbeeld in verband met de wetenschappelijke integriteit en de repliceerbaarheid van je onderzoek. Als je een zg. *sleutelbestand* bijhoudt en daarin vermeldt:

[adres1] = “Willemsparkweg 826 in Amsterdam”

dan kun je aan de hand van dat sleutelbestand de oorspronkelijke tekst herstellen.

Om veiligheidsredenen is het wel zaak om het gepseudonimiseerde bestand en het sleutelbestand op verschillende plekken te bewaren

(liefst op verschillende systemen). Een hacker moet dan immers beide systemen hacken om iets aan je data te hebben.

## Betrokkene

De betrokkene is degene op wie de persoonsgegevens betrekking hebben (Engels: data subject).

**Voorbeeld:** In de zin “De hoofdbewoner van Willemsparkweg 826 in Amsterdam heeft een frietkraam” is de ‘hoofdbewoner van Willemsparkweg 826 in Amsterdam’ de betrokkene. We weten nu immers dat die een frietkraam heeft.

## Gevoelige en bijzondere persoonsgegevens

**Let op! Wil je bijzondere persoonsgegevens gaan verwerken?  
Overleg dan vooraf met je docent of begeleider.**

Sommige persoonsgegevens zijn extra gevoelig. **Gegevens over kinderen** (tot 16 jaar) zijn uiteraard gevoelig, net als bijvoorbeeld financiële gegevens, studieresultaten en kopieën van identiteitsbewijzen. Daarnaast zijn er in de wet acht categorieën van zg. “bijzondere persoonsgegevens” vastgelegd die je **niet mag verwerken, tenzij er een uitzondering van toepassing is**. Voor studenten zijn dit de relevante uitzonderingen:

- De betrokkene heeft de gevoelige of bijzondere persoonsgegevens **overduidelijk zelf openbaar gemaakt**, bijvoorbeeld op een sociaal medium of in een autobiografie; **OF**
- Je hebt de **uitdrukkelijke toestemming** van de betrokkene om de bijzondere persoonsgegevens te gebruiken.

De AVG onderscheidt een achttal van zulke van bijzondere persoonsgegevens.<sup>2</sup> Wil je ze gaan gebruiken? Neem dan altijd eerst contact op met je docent of begeleider:

- **Ras of etnische afkomst**

Ras of etnische afkomst kunnen bijvoorbeeld blijken uit iemands naam in combinatie met diens geboorteplaats, althans als die combinatie specifiek genoeg is.

- **Politieke opvattingen**

Dit gaat niet alleen over iemands partijlidmaatschap, maar over politieke opvattingen in het algemeen. Van politieke ambtsdragers mag je deze gegevens uiteraard wél gebruiken.

- **Religieuze of levensbeschouwelijke overtuigingen**

Ook dit moet je ruim zien: het gaat niet alleen om lidmaatschap van een kerkgenootschap, maar om spirituele of humanistische overtuigingen in het algemeen.

- **Lidmaatschap van een vakbond**

In Nederland ligt dit lidmaatschap niet zo gevoelig (en hopelijk blijft dat zo), maar in andere landen kunnen mensen ervoor in de gevangenis komen.

- **Gezondheidsgegevens**

Deze gegevens zijn uiteraard heel gevoelig. Het gaat beslist niet alleen om complete medische dossiers, maar eigenlijk om alles wat met ziekte en aandoeningen te maken heeft, tot dyslexie aan toe.

**Let op!** De meeste mensen beschouwen gegevens over hun geestelijke gezondheid (GGZ, bijvoorbeeld angststoornis, depressie, burn-out, psychose) als gevoeliger dan gegevens over lichamelijke aandoeningen.

---

<sup>2</sup> Bijzondere persoonsgegevens worden beschreven in art. 9 van de AVG. Daarom spreekt men ook wel van “artikel 9-gegevens”.

- **Biometrische gegevens**

Deze gegevens over de vorm of afmetingen van het lichaam worden alleen als bijzondere persoonsgegevens beschouwd wanneer ze worden gebruikt om mensen eenduidig te identificeren (bijv. vingerafdrukken, irisscans, gezichtsverhoudingen).

- **Genetische gegevens**

Het gaat hier echt om gegevens over het genoom van mensen, bijvoorbeeld bij afstammingsonderzoek.

- **Seksueel gedrag of seksuele gerichtheid**

Dit zijn gegevens over iemands seksuele activiteiten, voorkeuren en gerichtheid (LHBTI+) en over de vraag met welk geslacht iemand zich identificeert.

**Let op!** *Foto's* zijn alleen bijzondere persoonsgegevens als ze worden gebruikt om *onderscheid* te maken tussen mensen, bijvoorbeeld als je specifiek foto's verzamelt van mensen in een rolstoel, mensen met een bepaalde huidskleur of mensen die een abortuskliniek bezoeken.

Voor gegevens over iemands **strafrechtelijk verleden of gepleegde strafbare feiten** gelden ongeveer dezelfde voorwaarden als voor bijzondere persoonsgegevens. Mensen kunnen er veel last van hebben als deze gegevens voortdurend worden opgerakeld.

## Verwerken

Alles wat je met persoonsgegevens kunt doen, valt onder de noemer 'verwerken'.

**Bijvoorbeeld:** gegevens verzamelen, opslaan, analyseren, bewerken, inzien, doorgeven, publiceren, en zelfs anonimiseren en wissen.

## Algemene verordening gegevensbescherming (AVG)

De Algemene verordening gegevensbescherming (AVG; Engels: *General Data Protection Regulation, GDPR*) wordt vaak de 'privacywet' genoemd,

maar feitelijk is dat niet juist, of in ieder geval te beperkt. De AVG richt zich op **de bescherming van alle grondrechten** van mensen binnen de EU in verband met de – meestal elektronische – verwerking van hun persoonsgegevens. Natuurlijk, het gaat om de bescherming van hun persoonlijke levenssfeer, maar het gaat bijvoorbeeld óók om het tegengaan van discriminatie en het waarborgen van de vrijheid van meningsuiting en de vrije pers.

Voordat de AVG in 2018 van kracht werd, bestond er al een Europese *richtlijn* voor gegevensbescherming. De daarin opgenomen regels moesten door de individuele lidstaten nog worden vertaald naar eigen nationale wetgeving. Omdat elk land de regels weer nét iets anders interpreteerde, leverde dit een lappendeken van verschillende regels en regeltjes per land op, zó onoverzichtelijk dat bedrijven en andere organisaties erin vastliepen. Met de invoering van de AVG gingen overal dezelfde regels gelden, want de AVG is rechtstreeks van toepassing op alle lidstaten, zonder dat daar aanvullende nationale wetgeving voor nodig is. Deze harmonisatie is ook meteen de belangrijkste vernieuwing van de AVG.

## Wettelijke grondslag

Het verwerken van persoonsgegevens is alleen toegestaan als je daar een goede, wettelijk omschreven reden voor hebt. In juridisch jargon spreken we dan van een wettelijke grondslag of rechtsgrond. De AVG noemt er zes.<sup>3</sup> Voor onderzoek door studenten komen niet alle grondslagen in aanmerking.

---

<sup>3</sup> De zes wettelijke grondslagen worden genoemd in art. 6 AVG. Ze kunnen als volgt worden omschreven: (1) **toestemming**; (2) noodzakelijk voor de uitvoering van een **overeenkomst**; (3) een **wettelijke verplichting** om de gegevens te verwerken; (4) **vitaal belang** (als het niet verwerken van de gegevens ernstig ten koste gaat van iemands gezondheid); de uitvoering van een taak van

**In verreweg de meeste gevallen moet je als student de grondslag 'toestemming' gebruiken.**

Hoe je dat doet, lees je [verderop in deze brochure](#).

Alleen bij hoge uitzondering (bijv. bij *web scraping* of wanneer je over je onderzoek wilt publiceren in een wetenschappelijk tijdschrift) kun je ***in zéér uitzonderlijke gevallen en na goedkeuring van je docent of begeleider*** gebruikmaken van de grondslag 'de uitvoering van een taak van algemeen belang'. Dit vraagt echter in bepaalde opzichten om een andere opzet van je onderzoek. Wees je daarvan bewust.

**Goed om te weten:** Mocht je na je studie onderzoek gaan doen in het kader van een aanstelling bij een universiteit (bijv. een PhD), dan gelden er andere regels. Je kunt dan in principe bijna altijd een beroep doen op de grondslag 'de uitvoering van een taak van algemeen belang'.

---

**algemeen belang** (bijv. universitair onderzoek); (6) **gerechtvaardigd belang** (het voordeel voor degene die de data verwerkt is aantoonbaar groter dan het nadeel voor de betrokkene).

## 2. Dataminimalisatie

Dataminimalisatie is een van de belangrijkste uitgangspunten van de AVG: **verwerk niet méér gegevens dan je nodig hebt, en doe dat zo kort mogelijk.**

### Noodzakelijkheid

Stel jezelf altijd de volgende vragen:

- Is het wellicht mogelijk om de onderzoeksvraag te beantwoorden **zonder überhaupt persoonsgegevens** te hoeven verwerken? Is er bijvoorbeeld een andere, net zo effectieve methode voorhanden om de voor jouw onderzoek benodigde informatie op te halen zonder dat daar persoonsgegevens aan te pas komen?
- **Kun je niet toe met minder persoonsgegevens?** Met andere woorden: heb je alle persoonsgegevens die je van plan bent te verzamelen echt nodig? Het is niet toegestaan om persoonsgegevens te verzamelen omdat ze later misschien nog eens van pas kunnen komen.
- Als het noodzakelijk is om persoonsgegevens te verzamelen, is het dan mogelijk om die gegevens – of een deel daarvan - te **anonimiseren**? Nadat persoonsgegevens zijn geanonimiseerd, zijn het geen persoonsgegevens meer.

### Doelbinding

Persoonsgegevens mogen alleen worden gebruikt voor het doel waarvoor ze oorspronkelijk zijn verzameld. Als je persoonsgegevens in bezit hebt (of ontvangt), en je wilt ze gebruiken voor een ander doel dan het oorspronkelijke doel, dan mag dat alleen als dat nieuwe doel “verenigbaar” is met het oorspronkelijke doel. Dat zal bij onderzoek door studenten niet gauw het geval zijn.

Voor wetenschappelijk onderzoek *door professionele onderzoekers* staat er weliswaar een uitzondering in de AVG, maar die geldt niet voor jou als student. Dus: als je voor je onderzoek persoonsgegevens wilt gebruiken die zijn verzameld voor een ander doel dan (jouw) onderzoek, zul je daarvoor aan alle [betrokkenen](#) om [toestemming](#) moeten vragen.

**Voorbeeld:**

Je zit in het bestuur van een studentenvereniging en je hebt in die hoedanigheid toegang tot een grote hoeveelheid informatie over de leden. In het kader van een scriptie wil je onderzoeken of leden die op een dure locatie wonen ook vaker meedoen aan dure verenigingsactiviteiten, bijvoorbeeld wintersportvakanties.

De gegevens van de leden zijn *verzameld* voor specifieke doelen: voor de ledenadministratie en voor het organiseren van uitjes. Deze doelen zijn *niet verenigbaar* met jouw doel: onderzoek doen in het kader van je studie. Om de gegevens van de leden te mogen gebruiken voor jouw onderzoek, zul je hen dus om [toestemming moeten vragen](#).

**Goed om te weten:** Mocht je na je studie onderzoek gaan doen in het kader van een aanstelling bij een universiteit (bijv. een PhD), dan gelden er andere regels. De doelbindingseis geldt dan niet meer, omdat de AVG in dat verband een uitzondering kent voor wetenschappelijk onderzoek.

## Bewaartermijnen

Uit oogpunt van dataminimalisatie is het niet toegestaan om gegevens langer te bewaren dan nodig is voor het doel waarvoor je ze verwerkt. Dat is nogal vaag, en veel duidelijker wordt ook het niet want de AVG noemt geen enkele specifieke bewaartermijn. Het is allemaal afhankelijk van de omstandigheden.

Enkele tips en richtlijnen:

- Contactgegevens van deelnemers hoeft je vaak niet langer te bewaren dan totdat de met hen gemaakte afspraak heeft plaatsgevonden.
- Als je opnames van interviews maakt en je maakt daar een transcript van, is het in veel gevallen beter (i.v.m. mogelijke stemherkenning) om de oorspronkelijke opnames **niet** te bewaren. Uitzonderingen zijn bijvoorbeeld interviews met bekende personen of politieke ambtsdragers en interviews waarin zulke opmerkelijke uitspraken worden gedaan dat jou kan worden gevraagd om het bestaan van die uitspraken aan te tonen.
- Alle brondata worden in principe maximaal twee jaar bewaard, zodat eventuele onenigheid over een cijfer kan worden afgehandeld.
- De bewaartermijn van je werkstuk of scriptie is afhankelijk van het facultaire of universitaire beleid.

**Goed om te weten:** Mocht je na je studie onderzoek gaan doen in het kader van een aanstelling bij een universiteit (bijv. een PhD), dan gelden er andere bewaartermijnen.

### 3. Informatiebeveiliging

Deelnemers vertrouwen jou hun persoonsgegevens toe, soms met heel vertrouwelijke of privacygevoelige informatie. Je bent het tegenover hen verplicht om daar zorgvuldig mee om te gaan. Precies datzelfde verlangt ook de AVG van je. Hieronder vind je een belangrijke aantal richtlijnen. De onderstaande lijst is absoluut niet uitputtend, dus gebruik niet alleen deze lijst, maar ook je gezond verstand.

#### Enkele belangrijke richtlijnen

- **Deel persoonsgegevens niet met anderen**, behalve als dat echt noodzakelijk is voor je onderzoek en als je de deelnemers daarover vooraf hebt [geïnformeerd](#).
- Probeer persoonsgegevens altijd zo snel mogelijk [te anonimiseren of te pseudonimiseren](#).
  - Door persoonsgegevens te *anonimiseren* zorg je ervoor dat het geen persoonsgegevens meer zijn en dat de AVG er niet meer op van toepassing is.
  - *Pseudonimisering* is in de eerste plaats een beveiligingsmaatregel. Pak je het goed aan, dan is die maatregel heel effectief.
- Stel een **sterk wachtwoord** in op de laptop of andere computer waarop je de persoonsgegevens opslaat of verwerkt. Hoe meer tekens er in het wachtwoord zitten, hoe veiliger het is. Het gebruik van een wachtwoordmanager is aan te bevelen.
- Plaats bestanden met persoonsgegevens zo snel mogelijk op een van de **universitaire systemen**. Daar zijn ze meestal veiliger dan op je eigen laptop. Zet ze in ieder geval **niet** in een (gratis) clouddienst zoals die van Google of Amazon.
- Gebruik voor het werken met persoonsgegevens **geen onveilige software** en zeker geen software of tools waarvan je op voorhand

al weet dat ze onveilig zijn, zoals Dropbox (gebruik in plaats daarvan bijv. [Proton Drive](#) of [Nextcloud](#)).

- Verzend gevoelige persoonsgegevens **nooit zomaar naar een extern (niet-UU) mailadres**. Gebruik voor het verzenden (en ontvangen!) van dergelijke gegevens bijvoorbeeld encryptie, of verzend/ontvang ze via een veilig medium (bijv. [SURFfilesender](#)).
- Wees uitermate **voorzichtig met het gebruik van USB-opslagmedia**. USB-devices zijn extreem gevoelig voor verlies en diefstal. Als er gevoelige gegevens op staan, liggen die met enige pech letterlijk op straat. Probeer liever je bestanden zo snel mogelijk op te slaan op een universitair systeem. Wil je desondanks USB-opslagmedia gebruiken, zorg er dan voor dat ze encrypted zijn en dat ze beveiligd zijn met een sterk wachtwoord.
- Gebruik **geen persoonsgegevens in AI-prompts**.<sup>4</sup> Alles wat je in je prompts opgeeft, kan worden gebruikt om het AI-systeem te trainen. Anderen kunnen dan, door slim te prompten, die gegevens er wellicht weer uit krijgen.
- **Overweeg het gebruik van DuckDuckGo**. Dit is een privacy-vriendelijke browser waarmee je [tracking cookies](#) kunt tegenhouden. Bovendien kun je via de browser en de website van [DuckDuckGo](#) veiliger chatten met een aantal veelgebruikte AI-toepassingen, zoals ChatGPT, Llama, Claude en Mistral.
- **Wees op je hoede voor phishing**. Hackers proberen op allerlei manieren toegang te krijgen tot jouw systeem én tot de daarop aanwezige data. Ze proberen je bijvoorbeeld te verleiden om op een bepaalde knop in een mail te klikken, waarna er kwaadaardige software op je systeem wordt geïnstalleerd. Zelfs de bekende [captcha](#)'s zijn niet meer zomaar te vertrouwen.

---

<sup>4</sup> Gebruik ook geen vertrouwelijke gegevens en ook geen auteursrechtelijk beschermd materiaal in je prompts.

## Datalekken herkennen en melden

Het woord 'datalek' suggereert dat er alleen sprake is van een dergelijk incident als onbevoegden persoonsgegevens kunnen inzien of stelen. De wettelijke term is 'inbreuk in verband met persoonsgegevens' en de betekenis daarvan is veel breder dan een lek: ook als persoonsgegevens onbedoeld of onbevoegd zijn gewijzigd, zijn gewist of ontoegankelijk zijn geworden, kun je spreken van een 'inbreuk' of 'datalek'.

Het herkennen van een datalek is dus ingewikkelder dan alleen nagaan of onbevoegde mensen persoonsgegevens hebben kunnen inzien.

**Voorbeeld:** Als je audio-opnamen van een interview hebt gemaakt – rechtstreeks op je laptop – en die laptop wordt gestolen zonder dat je een backup van de opnamen hebt gemaakt (bijvoorbeeld op een UU-systeem), dan is dat een datalek, zelfs als jouw laptop was beveiligd met een sterk wachtwoord. De persoonsgegevens van je deelnemers zijn immers definitief verloren gegaan.

Merk je dat er een datalek is opgetreden (een "inbreuk in verband met persoonsgegevens" dus), meld dat dan altijd **onmiddellijk**<sup>5</sup> door een mail te sturen naar [datalek@uu.nl](mailto:datalek@uu.nl). Vermeld het volgende in die mail:

- Wat er precies is gebeurd, waar en wanneer (datum en tijdstip)
- Welke gegevens er zijn ingezien, gestolen, zoekgeraakt, beschadigd, gewijzigd of gewist
- Hoeveel mensen het slachtoffer zijn van het lek (hoeveel [betrokkenen](#)) en om wat voor categorieën betrokkenen het gaat (bijv. studenten, onderzoeksdeelnemers)
- Of je al iets hebt gedaan om de gevolgen van het lek te verkleinen
- Of je de slachtoffers al hebt ingelicht.

---

<sup>5</sup> Dit moet **onmiddellijk** omdat de universiteit slechts 72 uur de tijd heeft om het lek te onderzoeken en om vast te stellen of het moet worden gemeld bij de Autoriteit Persoonsgegevens.

## 4. Rechten van deelnemers

Mensen van wie er persoonsgegevens worden verwerkt, hebben allerlei rechten. Feitelijk zijn die rechten niets anders dan een wettelijke verankering van het uitgangspunt dat zij *controle* moeten kunnen houden op datgene wat er met hun persoonsgegevens gebeurt. De in de AVG beschreven rechten zijn niet in alle situaties van toepassing. Hieronder worden alleen de rechten beschreven die voor jouw onderzoek waarschijnlijk relevant zijn.<sup>6</sup>

Het bestaan van deze rechten moet je opnemen in je [informatiebrief](#).

- Iedereen heeft het recht om aan jou te vragen **of** je persoonsgegevens van hem of haar verwerkt. Als dat niet het geval is, moet je dat laten weten. Is dat **wél** het geval, dan gelden de onderstaande rechten.
- Deelnemers<sup>7</sup> hebben het recht om te worden **geïnformeerd** over de verwerking. Hierover lees je meer in [hoofdstuk 5](#).
- Als je, zoals vrijwel altijd het geval is, [toestemming](#) aan je deelnemers hebt gevraagd om hun persoonsgegevens te mogen verwerken, dan moeten ze die toestemming ook weer kunnen **intrekken**. Voor het intrekken van hun toestemming hoeven ze geen reden op te geven; je moet altijd voldoen aan het verzoek.

---

<sup>6</sup> Naast de genoemde rechten hebben deelnemers het recht om de verwerking van hun persoonsgegevens onder bepaalde omstandigheden te beperken (je mag er dan niets anders mee doen dan ze bewaren), om een digitale kopie van hun gegevens te ontvangen (met het doel om over te stappen op een andere dienstverlener) en om niet te worden onderworpen aan profilering of aan geautomatiseerde besluitvorming waar ze negatieve gevolgen van kunnen ondervinden.

<sup>7</sup> Waar in dit hoofdstuk 'deelnemers' worden vermeld, gaat het uiteindelijk om alle [betrokkenen](#), dus om alle mensen van wie je persoonsgegevens verwerkt.

- Deelnemers mogen jou ook om **inzage** in hun persoonsgegevens vragen om te controleren of die gegevens kloppen. Ze mogen ook om allerlei achtergrondgegevens vragen, zoals het doel waarvoor je de gegevens verwerkt en de bewaartermijn. Al die informatie staat in principe in je [informatiebrief](#).
- Merken deelnemers dat jouw gegevens aantoonbaar niet kloppen, dan moet je die gegevens **corrigeren**. Het zou ook zo kunnen zijn dat deelnemers zich achteraf niet herkennen in een uitspraak die ze eerder hebben gedaan. Je kunt dan met hen overleggen hoe je dat gaat oplossen.
- Deelnemers kunnen jou vragen hun gegevens te **wissen**. In de praktijk komt dat op hetzelfde neer als het intrekken van toestemming.

**Let op!** Deelnemers en anderen kunnen de bovenstaande rechten uiteraard alleen uitoefenen zo lang je (nog) kunt nagaan welke persoonsgegevens van hen zijn. Als je je gegevens hebt geanonimiseerd, is het voor je deelnemers niet meer mogelijk om de bovenstaande rechten uit te oefenen.

- Deelnemers hebben het recht om een klacht in te dienen. In eerste instantie doen ze dat bij jouzelf of bij je begeleider. Ze kunnen ook terecht bij de functionaris gegevensbescherming<sup>8</sup> van de universiteit. Komen ze er met ons niet uit, dan kunnen ze een klacht indienen bij de Autoriteit Persoonsgegevens (AP).

---

<sup>8</sup> De functionaris gegevensbescherming of FG is de interne AVG-adviseur en -controleur van de universiteit. De functie van de FG is wettelijk beschermd en de FG is gebonden aan geheimhouding. Mailadres: [fg@uu.nl](mailto:fg@uu.nl)

## 5. Deelnemers informeren

**Let op!** Het informeren van je deelnemers is een van de belangrijkste aspecten van het AVG-compliant maken van je onderzoek. De informatiebrief moet in heldere en begrijpelijke taal zijn geschreven.

Op ethische gronden moet je je potentiële deelnemers informeren over je onderzoek in het algemeen, zodat ze weten waar ze voor kiezen als ze wel of niet meedoen. Verwerk je bovendien persoonsgegevens van je deelnemers (en dat zal vaak het geval zijn, anders zou je deze brochure niet lezen), dan moet je hen nog veel meer informatie geven, bijvoorbeeld welke persoonsgegevens je verzamelt, wat je daarmee doet en [welke rechten de deelnemers hebben](#).

### Hoe kun je je deelnemers het beste informeren?

De AVG zegt niet op welke manier je je deelnemers moet informeren, zo lang je maar kunt aantonen dat je het hebt gedaan. Er zijn diverse methoden:

- Je kunt een **informatiebrief** schrijven, of zelfs een korte brochure. Deze kun je in geprinte vorm aan je deelnemers overhandigen, of je kunt hem als bijlage meesturen met een uitnodigingsmail. De informatiebrief is verreweg de meest gangbare methode om deelnemers te informeren.
- Doe je online onderzoek, bijvoorbeeld een online vragenlijst, dan kun je de informatie opnemen in de **inleiding van je vragenlijst**.
- In sommige gevallen (bijvoorbeeld bij onderzoek onder laaggeletterden) kan het de voorkeur verdienen om de informatie **mondeling** te verstrekken. Schrijf in dat geval een script met de informatie die je wilt geven, lees dit script voor en maak bij voorkeur een opname van het voorlezen.

- Als er geen contactmoment is tussen je deelnemers en jou, zoals bij *web scraping* (het binnenhalen van data vanaf internet, meestal uit social media), dan kun je een privacyverklaring schrijven en deze op een openbare website plaatsen. De inhoud van die verklaring is ongeveer gelijk aan hetgeen in de volgende paragraaf wordt opgesomd. Om aandacht op je onderzoek te vestigen, kun je een bericht op hetzelfde sociaal medium plaatsen waarin je een link naar de privacyverklaring opneemt.

## Welke informatie moet je aan je deelnemers verstrekken?

Of je nu persoonsgegevens gebruikt of niet, je moet je potentiële deelnemers altijd informeren over je onderzoek, zodat ze een afgewogen beslissing kunnen nemen of ze willen meedoen.

- **Wie ben je?**
- **Voor welk onderzoek nodig je de persoon uit?**
- **Hoe heb je de persoon gevonden of geselecteerd?**
- **Waar gaat het onderzoek over?** (achtergrond, doel)
- **Hoe wordt het onderzoek uitgevoerd?** (bijv. methoden en technieken, duur (per sessie), locatie, wat moeten deelnemers doen, wat zijn de eventuele nadelen, is er een beloning of vergoeding)
- **Door wie wordt het onderzoek uitgevoerd?** (samenstelling onderzoeksteam, indien relevant)
- **Doet u mee?** (vrijwillige deelname, stoppen is altijd mogelijk)
- **Worden er persoonsgegevens van de deelnemer gebruikt?** (wat zijn persoonsgegevens, worden ze gebruikt ja of nee)

Als je in je onderzoek persoonsgegevens van deelnemers gebruikt, neem je ook het volgende op in je brief:

- **Welke persoonsgegevens?** (beknopt overzicht van de soorten persoonsgegevens die je gebruikt – plus eventuele bijzondere persoonsgegevens – en waarom ze nodig zijn)
- **Wat gebeurt er met de persoonsgegevens?** (welke bewerkingen worden erop uitgevoerd, hoe worden ze overgebracht naar UU-systemen (indien van toepassing), anonimisering, pseudonimisering, opslag, bewaartermijn)
- **Wie kunnen de persoonsgegevens bekijken?** (wie heeft er toegang tot de persoonsgegevens, geldt er geheimhouding)
- **Worden de persoonsgegevens goed beveiligd?**
- **Mogen we de persoonsgegevens gebruiken?** (wettelijke grondslag – meestal toestemming)
- **Wat zijn de rechten van deelnemers onder de AVG?** (inzage, correctie, verwijdering (i.e. meestal intrekken toestemming), klachtrecht UU en AP, functionaris gegevensbescherming)
- **Contactgegevens voor meer informatie** (jouw gegevens, contactgegevens van docent of begeleider)

Dit lijkt erg veel, en dat is het ook. Aan jou de taak om dit beknopt in een brief te vatten. Hieronder vind je een voorbeeld.

## Voorbeeld van een informatiebrief

Utrecht, [datum]

Beste lezer,

Mijn naam is [naam student] en ik ben student aan de Universiteit Utrecht. In het kader van het vak *Geschiedenis in Levend Perspectief* ben ik van plan interviews te doen met mensen die herinneringen hebben aan de jaren '60 van de vorige eeuw. Voor zo'n interview wil ik u van harte uitnodigen. Ik ben specifiek bij u uitgekomen omdat wij elkaar kennen en ik u beschouw als iemand die mij belangrijke informatie zou kunnen geven over dit onderwerp. Vanzelfsprekend is deelname geheel vrijwillig en u kunt tussendoor altijd stoppen.

### **Hoe wordt het onderzoek uitgevoerd?**

In het interview zal ik u vragen hoe u het hebt ervaren om op te groeien in de jaren '60, vooral op het gebied van seksuele vrijheid. Ging het er echt zo wild aan toe als wel eens wordt beweerd? Of merkten veel mensen juist weinig van de veranderingen? In het interview stel ik misschien ook vragen over onderwerpen die u als gevoelig ervaart. Uiteraard bent u niet verplicht om daar antwoord op te geven.

Het interview vindt plaats op een plek die we nader zullen afspreken. Het duurt ongeveer 45 minuten en ik zal er, als u dat goed vindt, een geluidsopname van maken op mijn mobiele telefoon. Die opname zet ik vervolgens over naar een goed beveiligd computersysteem van de universiteit. De tekst van de opname typ ik helemaal uit en daarna wis ik de opname, zodat u niet meer herkenbaar bent aan uw stem.

### **Hoe ga ik om met uw gegevens?**

De uitgeschreven teksten van alle interviews ga ik analyseren, en die analyse wordt een belangrijk onderdeel van een *paper* voor het eerder genoemde vak. Het kan zijn dat ik in mijn paper dingen wil

opschrijven precies zoals u ze hebt gezegd. We kunnen onderling afspreken of ik daarbij uw naam zal noemen of niet. Na twee jaar verwijder ik alle uitgeschreven interviews. Het paper zelf wordt wellicht langer bewaard door de universiteit, omdat mijn cijfer erop gebaseerd is.

Ik ga heel zorgvuldig en vertrouwelijk om met uw persoonsgegevens. Uw contactgegevens deel ik met niemand en de uitgeschreven teksten alleen met mijn docent. Aan het begin van het interview vraag ik u om toestemming om een opname te mogen maken en om uw persoonsgegevens te mogen gebruiken. Die laatste toestemming kunt u na het interview nog intrekken, zonder dat u hoeft te zeggen waarom. Bovendien mag u controleren of de gegevens die ik van u heb, wel kloppen. En als er iets niet klopt, kunnen we overleggen hoe ik dat dan kan verbeteren.

### **Vragen of klachten?**

Hebt u vragen of klachten over mijn onderzoek? Dan kunt u contact opnemen met mijn docent [naam en e-mailadres docent]. Mocht u een klacht hebben die na contact met mijn docent niet is opgelost, dan kunt u terecht bij de functionaris gegevensbescherming van de universiteit ([fg@uu.nl](mailto:fg@uu.nl)). Komt u er met ons echt niet uit, dan kunt u naar de Autoriteit Persoonsgegevens stappen. Maar ik zal er alles aan doen om het niet zo ver te laten komen.

Alvast heel veel dank voor uw medewerking!

Met vriendelijke groet,

[naam, e-mailadres en evt. telefoonnummer student]

## 6. Deelnemers om toestemming vragen

Nadat je je potentiële deelnemers hebt geïnformeerd, kunnen ze een afgewogen beslissing nemen of ze willen meedoen aan je onderzoek en of ze er in het kader daarvan mee instemmen dat je hun persoonsgegevens verwerkt. Strikt genomen vraag je je potentiële deelnemers dus om twee verschillende dingen:

1. Of ze – vrijwillig – medewerking willen verlenen aan je onderzoek. Dit is de traditionele *'informed consent'* in ethische zin.
2. Of ze toestemming geven voor de verwerking van hun persoonsgegevens. Dit is toestemming in de zin van de AVG.

Stemmen ze hiermee in, dan is 'toestemming' de [wettelijke grondslag](#) waarop je de verwerking van persoonsgegevens baseert.

### Voorwaarden voor rechtsgeldige toestemming

De AVG eist dat toestemming voor de verwerking van persoonsgegevens vrij, specifiek, geïnformeerd en aantoonbaar is. Hieronder gaan we kort op die vier begrippen in:

- **Vrij:** Potentiële deelnemers moeten vrij zijn in hun keuze of ze hun persoonsgegevens willen laten verwerken of niet. Er mag dus geen druk op hen worden uitgeoefend, de toestemming mag niet gekoppeld zijn aan allerlei voordelen (en de weigering niet aan allerlei nadelen) en er mag geen sprake zijn van een machtsrelatie tussen degene die om toestemming vraagt en degene die om toestemming wordt gevraagd.

Voor werkgevers is het bijvoorbeeld bijna onmogelijk om rechtsgeldige toestemming van hun werknemers te verkrijgen omdat werknemers zich tegenover hun werkgever niet 'vrij' voelen om toestemming te weigeren.

- **Specifiek:** Je moet je potentiële deelnemers precies laten weten waar ze toestemming voor geven. Zoiets als “onderzoek in het kader van mijn studie” is veel te vaag. Je moet een duidelijk en beperkt doel omschrijven, bijvoorbeeld de titel van je scriptie of de korte omschrijving van een opdracht.
- **Geïnformeerd:** Je moet je potentiële deelnemers in de gelegenheid stellen een afgewogen, “geïnformeerde” beslissing te nemen over hun toestemming. Aan dit onderwerp hebben we in deze brochure een apart [hoofdstuk](#) geweid.
- **Aantoonbaar:** Voor toestemming is het nodig dat potentiële deelnemers een *ondubbelzinnige, actieve handeling* verrichten om hun wil kenbaar te maken. Denk aan het ondertekenen van een toestemmingsverklaring (heeft niet de voorkeur) of het in een opname verklaren dat ze akkoord gaan (heeft wél de voorkeur).

**Voorbeeld:** Je ziet wel eens websites waarop te lezen is: “Door deze website te blijven gebruiken, geeft u toestemming om uw persoonsgegevens te gebruiken voor direct marketing.” Het blijven gebruiken van een website is echter geen ondubbelzinnige, actieve wilsuiting. Daarom is deze “afgedwongen” toestemming niet rechtsgeldig.

## Kinderen

Kinderen zijn nog niet in staat om zelf een gefundeerde beslissing te nemen over de verwerking van hun persoonsgegevens, maar die verwerking kan wél grote gevolgen voor hun latere leven. Daarom is de AVG extra streng op het verkrijgen van toestemming als het om de persoonsgegevens van kinderen gaat. De regels zijn duidelijk:

- Als het kind jonger is dan 12 jaar, moet minimaal één van de ouders toestemming geven.

- Is het kind al 12 jaar geworden, maar nog geen 16, dan moet het kind zelf toestemming geven, plus minimaal één van de ouders.
- Jongeren die hun 16<sup>e</sup> verjaardag hebben gevierd, worden beschouwd als volwassenen. Zij hebben geen toestemming van hun ouders nodig.

Of je de toestemming van één of beide ouders nodig hebt, hangt af van de gevoeligheid van je onderzoek. Studenten zullen meestal geen onderzoek doen dat zó gevoelig is dat beide ouders toestemming moeten geven.

### Toestemming aantoonbaar maken

Voor het aantonen van toestemming heb je lang niet altijd een **schriftelijke verklaring** nodig. Bij opgenomen interviews kun je er bijvoorbeeld ook voor kiezen om een **opname** te maken van jouw vraag of iemand toestemming geeft, plus het antwoord daar op. Je kunt dan het beste een script gebruiken waarin je alle onderdelen van de toestemming (zie voorbeeld) in spreektaal vastlegt. Dat script lees je dan voor aan het begin van het interview.

Doe je online vragenlijstonderzoek dan kun je aan het begin van die lijst een **selectievakje** opnemen waarin je de toestemmingsvraag stelt.

#### **Afwijkende situatie: medewerking vragen**

Stel dat je onderzoek wilt doen onder kinderen op een school of onder werknemers in een bepaald kantoor. Om dat te mogen doen, zul je de medewerking moeten krijgen van het management van die school of organisatie. We spreken dan van *gatekeepers*. Je kunt hen in een brief of mail vragen of het onderzoek op hun school of kantoor mag plaatsvinden. Maar houd er vooral rekening mee dat die gatekeepers geen zeggenschap hebben over de persoonsgegevens die je verzamelt. Het zijn de deelnemers zelf (en/of hun ouders) die die zeggenschap hebben!

## Voorbeeld van een toestemmingsverklaring

### TOESTEMMINGSVERKLARING voor deelname aan:

[Titel van je onderzoek of project]

#### Deelname:

- Ik heb de informatiebrief over het onderzoek gelezen. Ik heb begrepen wat daar in staat.
- Ik heb vragen kunnen stellen en die zijn beantwoord.
- Ik heb genoeg tijd gehad om na te denken of ik mee wil doen.
- Ik doe vrijwillig mee.

#### Gegevens over mij:

- Ik weet dat er gegevens over mij worden verzameld.
- Ik ga ermee akkoord dat die gegevens worden gebruikt voor dit onderzoek of project, zoals dat is uitgelegd in de informatiebrief.
- Ik ga ermee akkoord dat er [beeld- en/of geluidsopnamen] worden gemaakt.
- Ik ga er **WEL/NIET** (*doorhalen zoals gewenst*) mee akkoord dat de [beeld- en/of geluidsopnamen] worden gebruikt in lessen en colleges waar de student aan deelneemt.
- Ik ga er **WEL/NIET** (*doorhalen zoals gewenst*) mee akkoord dat ik herkenbaar in beeld kom in de getoonde opnamen en/of dat mijn naam wordt genoemd in de scriptie van de student.

#### Toestemming:

Ik weet dat ik het recht heb om mijn toestemming voor het gebruik van mijn persoonsgegevens in te trekken, zoals dat beschreven staat in de informatiebrief.

Naam deelnemer: \_\_\_\_\_

Handtekening: \_\_\_\_\_ Datum: \_\_\_ / \_\_\_ / \_\_\_\_\_

## 7. Je uiteindelijke werkstuk of scriptie

### Schrijven

Tijdens het verzamelen en analyseren van je data heb je je beperkt tot datgene wat je echt nodig had (zie [Dataminimalisatie](#)). Bovendien heb je persoonsgegevens die je niet nodig had maar die je wél in bezit had, zo veel mogelijk [geanonimiseerd](#).

Uiteindelijk ga je je onderzoek en de resultaten daarvan beschrijven in een werkstuk of scriptie. Ondanks uitgangspunten als dataminimalisatie en anonimisering kan het in bepaalde gevallen nodig zijn om een naam te noemen of om gegevens te vermelden die op een andere manier herleidbaar zijn tot een persoon. Laat je die naam of die gegevens weg, dan kan je betoog abstract, ongrijpbaar of onbetrouwbaar overkomen.

#### De belangrijkste stelregels:

- Beperk het noemen van namen en het opnemen van herleidbare persoonsgegevens in je scriptie of werkstuk tot datgene wat **noodzakelijk** is voor je verhaal.
- Zorg dat je kunt **beargumenteren** waarom je dergelijke namen of persoonsgegevens wél vermeldt.
- Heb je **afspraken** gemaakt met deelnemers? Houd je daar aan.

### Openbaar maken

In de [bespreking van de AVG](#) (zie hoofdstuk 1) is al vermeld dat de AVG de vrijheid van meningsuiting beschermt. Dat wil zeggen: iedereen moet zijn of haar mening kunnen geven zonder bang te hoeven zijn voor vervolging. *Academische uitdrukkingsvormen* zijn manieren om wetenschappelijke of academische meningen of ideeën wereldkundig te maken. Ze vormen het sluitstuk van de academische vrijheid. In een

democratische maatschappij zijn publicaties van wetenschappers van levensbelang.

Je kunt je voorstellen dat dergelijke publicaties op gespannen voet kunnen staan met de bescherming van de persoonsgegevens van mensen die in die publicaties worden genoemd. Hier botsen twee grondrechten: gegevensbescherming en vrijheid van meningsuiting.

Bij academische uitdrukkingsvormen prevaleert de vrijheid van meningsuiting boven de privacy van de betrokkenen.<sup>9</sup> Een **officiële scriptie** wordt beschouwd als een academische uitdrukkingsvorm. In de praktijk betekent dit voor jou het volgende:

- Deelnemers die jou toestemming hebben gegeven voor de verwerking van hun persoonsgegevens, kunnen het intrekken van die toestemming niet gebruiken om jou te dwingen je scriptie aan te passen.
- Deelnemers en anderen vinden in de AVG ook geen andere aanknopingspunten om jou te dwingen hun persoonsgegevens te corrigeren of te verwijderen *uit jouw scriptie*. Heb je het heel bont gemaakt (bijvoorbeeld als je aperte onwaarheden hebt verkondigd), dan kunnen ze nog wel een gerechtelijke procedure starten,<sup>10</sup> maar niet op grond van de AVG.

---

<sup>9</sup> Ditzelfde geldt wanneer er persoonsgegevens worden verwerkt ten behoeve van journalistiek, kunst of literatuur.

<sup>10</sup> Dit zou dan moeten gebeuren op basis van smaad, laster of een andere onrechtmatige daad. Hopelijk werk je zorgvuldig genoeg om het zo ver niet te laten komen.