

Handreiking persoonsgegevens in onderzoek

Een praktisch stappenplan voor onderzoekers in het hoger onderwijs om aan de AVG te voldoen



Colofon

Dit document is bedoeld als praktische handreiking voor onderzoekers in het hoger onderwijs en gaat over het omgaan met persoonsgegevens in onderzoek. Het is bedoeld als hulpmiddel om aan de gegevensbeschermingswetgeving te voldoen.

Bestemd voor

Dit document is specifiek bestemd voor de onderzoeker in de sector onderwijs en onderzoek en voor datamanagers en privacyprofessionals die de onderzoekers ondersteunen en adviseren.

Samenstelling en beheer

Dit document is tot stand gekomen nadat de Autoriteit Persoonsgegevens ('AP') in haar sectorbeeld expliciet aandacht heeft gevraagd aan onderwijsinstellingen en FG's in de sector om samen te werken aan praktische guidance¹ hoe onderwijsinstellingen om moeten gaan met onderzoeksgegevens. Dit is gerealiseerd via het Privacy Expertise Centrum van SURF in samenwerking met de multidisciplinaire werkgroep 'Persoonsgegevens in onderzoek' ('werkgroep PGO') en een reviewgroep met privacy- en dataprofessionals uit de onderwijssector (hoger onderwijs/wo). De AP heeft in positieve zin kennisgenomen van dit initiatief.

Speciale dank gaat uit naar de werkgroepleden:

- Jan van den Berg, FG – Hogeschool van Amsterdam
- Iris Goes, Datamanager Onderzoek – Hogeschool Windesheim Almere/Zwolle
- Floor May-Smit, FG - NHL Stenden Leeuwarden
- Anita Polderdijk-Rijntjes, FG - Hogeschool Windesheim Zwolle
- Maartje Ridder, Research data management specialist – Hogeschool van Amsterdam

Vanuit SURF werkte mee Helma de Boer, lead Privacy Expertise Centrum.

en naar de reviewgroep:

- Sarah Coombs, Open Science adviseur – Hogeschool Saxion Deventer en DCC-PO
- Esther van der Ent, FG – HAN Arnhem/Nijmegen
- Esther Eisen-Tijssen, Datasteward – Hogeschool Windesheim Zwolle
- Marlon de Jong, - Datasteward, Privacy & Data Protection, Rijksuniversiteit Groningen
- Anke van Gorp, onderzoeker en privacy officer – Hogeschool Utrecht
- Jan-Willem Oordt, Chief Privacy Officer – Rijksuniversiteit Groningen
- Raoul Winkens, FG – Universiteit Maastricht

Licentie

Dit document is verstrekt onder de creative commons-licentie [CC BY 4.0](#) International (naamsvermelding). SURF aanvaardt geen aansprakelijkheid voor enig gebruik/toepassing van dit document.

Versiebeheer

Versie	Door	Datum	Toelichting/wijziging
1.0	Werkgroep PGO en PEC	28-11-2025	Initieel concept
1.1	SURF i.s.m. werkgroep PGO	11-12-2025	Diverse kleine correcties/verduidelijking/links
1.2	SURF o.b.v. feedback	05-03-2026	Diverse kleine correcties/bijlage checklist

¹ Zie ook [Sectorbeeld Onderwijs 2021-2023](#)² onder het kopje: 'Nog veel onduidelijkheid over onderzoeksgegevens' (pagina 4, laatste alinea).

Inhoudsopgave

Colofon	2
1 Inleiding	4
Reikwijdte	4
Doel	7
Status en disclaimer	7
Leeswijzer	8
2 Samenvatting voor de onderzoeker	9
3 Stappen onderzoekers	11
Data Lifecycle	11
Stap 1: Planning & Ontwerp	12
1.1 Is de AVG van toepassing op mijn onderzoek?	12
1.2 Welke AVG-rol is van toepassing?	13
1.3 Heb ik de juiste overeenkomst(en) gesloten met deze partijen?	14
1.4 Heb ik de juiste grondslag om persoonsgegevens te verwerken?	15
1.5 Voorwaarden en voorbeelden van grondslagen	18
1.6 Heb ik een doel voor het verwerken van de gegevens?	20
1.7 Vraag ik alleen die gegevens die nodig zijn voor mijn onderzoek?	21
1.8 Kan of wil ik (een deel van) de data hergebruiken/voor hergebruik beschikbaar maken?	22
1.9 Informeer ik de deelnemers op de juiste wijze?	23
1.10 Moet ik een DPIA uitvoeren?	23
1.11 Voldoet mijn datamanagementplan aan de AVG?	24
1.12 Onderzoek met/door studenten	25
Stap 2: Verzameling & Gebruik	25
2.1 Hoe informeer ik de onderzoeksdeelnemers over het gebruik van hun persoonsgegevens op een manier die voldoet aan de AVG?	25
2.2 Heb ik een procedure klaar als een onderzoeksdeelnemer de toestemming intrekt?	29
2.3 Sla ik de toestemmingsformulieren op een veilige plek op?	29
2.4 Gebruik ik veilige onderzoeksmiddelen?	29
2.5 Heb ik mijn onderzoek aangemeld in het register van verwerkingsactiviteiten?	30
Stap 3: Opslag & Beheer	31
3.1 Welke maatregelen kan ik treffen om de gegevens te beveiligen?	31
3.2 De documentstructuur aanpassen	32
3.3 Bewaartermijnen van jouw onderzoeksgegevens	33
3.4 Pseudonimiseren en anonimiseren	34
Stap 4: Analyse & Delen	37
4.1 Hoe kan ik veilig met persoonsgegevens blijven werken bij wijzigingen?	37
4.2 Kan ik al persoonsgegevens verwijderen?	38
4.3 Kan ik de gegevens anonimiseren of pseudonimiseren in mijn onderzoek?	39
4.4 Zijn de beveiligingsmaatregelen die ik heb getroffen nog voldoende passend?	39
Stap 5: Evalueren & Archiveren	39
Stap 6: Publiceren	40
Bijlage 1 - Datamanagementplan	41
Bijlage 2 – Toestemmingsformulier	42
Bijlage 3 - Begrippenlijst	43
Bijlage 4 – Beslisboom rolverdeling en af te sluiten overeenkomst	45
Bijlage 5 – Checklist voor de onderzoeker	46

1 Inleiding

Voor je ligt de handreiking Persoonsgegevens in Onderzoek 2025 (hierna 'handreiking'). Deze praktische handreiking is geschreven voor jou, onderzoeker in het hoger onderwijs. Hiermee helpen we jou aan de gegevensbeschermingswetgeving te voldoen, zoals de Algemene verordening gegevensbescherming (hierna 'AVG') en de Uitvoeringswet Algemene verordening gegevensbescherming (hierna 'UAVG').

Vanuit het onderzoeksveld is behoefte aan duidelijkheid over de (toepassing van de) AVG. De Autoriteit Persoonsgegevens (hierna 'AP') constateert dit ook in het Sectorbeeld Onderwijs 2021-2023.² De AP nodigt hierin de sector uit om in gesprek te gaan over persoonsgegevens in onderzoek. In het sectorbeeld noemt de AP *"de noodzaak tot duidelijkheid voor onderzoekers van (hogere) onderwijsinstellingen hoe om te gaan met persoonsgegevens bij (wetenschappelijk) onderzoek."*

Om deze duidelijkheid te scheppen, is vanuit het Privacy Expertise Centrum van SURF een werkgroep opgericht met als doel deze handreiking op te stellen. Deze werkgroep Persoonsgegevens in onderzoek (PGO) bestaat uit een multidisciplinair team waarin deskundigheid over de AVG, datamanagement en het doen van onderzoek bij elkaar is gebracht.

De werkgroep PGO heeft gekozen voor een handreiking om jou als onderzoeker *praktische* handvatten te bieden. De handreiking is gereviewd door de privacy- en security-gemeenschap van SURF, waarbij de hogere onderwijsinstellingen zijn aangesloten. De AP heeft in informele overleggen met de werkgroep PGO aangegeven het initiatief van de werkgroep PGO te steunen en dat de handreiking in positieve zin kan bijdragen aan de onduidelijkheid over de omgang met onderzoeksgegevens.

Reikwijdte

Deze handreiking is van toepassing op zowel:

- wetenschappelijk onderzoek verricht door universiteiten, als
- onderzoek gericht op de beroepspraktijk verricht door hogescholen.

Daarbij gaat het zowel om nieuwe datasets met persoonsgegevens (primair gebruik) of hergebruik van bestaande datasets (verder of secundair gebruik). In deze handreiking bedoelen we daarmee:

- Primair gebruik is wanneer je binnen het onderzoek persoonsgegevens rechtstreeks van de betrokkenen verzamelt met een specifieke doelstelling voor ogen.
- Secundair gebruik is wanneer je of de persoonsgegevens niet rechtstreeks bij de betrokkenen verzamelt of wanneer ze in eerste instantie voor een ander doel of onderzoek dan jouw huidige onderzoeksproject zijn verzameld en je wilt deze gegevens gebruiken voor verdere verwerking voor onderzoek. In deze handreiking spreken we van *hergebruik*.³

² <https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023>⁷

³ Het hergebruiken van onderzoeksgegevens, die je zelf hebt verzameld in een bepaald onderzoek, voor een ander onderzoek is ook een verder of secundair gebruik van persoonsgegevens. In deze gevallen maak je namelijk gebruik van persoonsgegevens die aanvankelijk voor een ander doeleinde of onderzoeksproject werden verwerkt. Zie onderzoektips.ugent.be⁷

Speciaal regime

In de handreiking gaan we uit van onderzoek aan een universiteit of hogeschool dat valt onder het speciale regime van de AVG dat op wetenschappelijk onderzoek van toepassing is.

Het speciale regime houdt in dat:

- (gevoelige) persoonsgegevens⁴ gebruikt mogen worden voor wetenschappelijk onderzoek (verenigbaar doel);
- er uitzonderingen zijn op het recht van gegevenswissing als dit het bereiken van het onderzoeksdoel in de weg staat
- en ook dat het recht op inzage, rectificatie en het recht op beperking van de verwerking niet meer van toepassing zijn mits gegarandeerd kan worden dat de gegevens uitsluitend voor wetenschappelijk doeleinden kunnen worden gebruikt.

In alle gevallen geldt dat er passende waarborgen getroffen moeten worden om persoonsgegevens te beveiligen.

Definitie wetenschappelijk onderzoek (inclusief praktijkgericht onderzoek)

De AVG geeft geen definitie van wetenschappelijk onderzoek. Het begrip 'wetenschappelijk onderzoek' onder de AVG moet ruim worden opgevat en omvat ook uit private middelen gefinancierd onderzoek.

In het kader van deze handreiking gaan we van de volgende definitie uit voor wetenschappelijk onderzoek⁵ (waaronder praktijkgericht onderzoek):

- Onderzoek waarin persoonsgegevens worden verwerkt.
- Relevante sectorale normen voor methodologie en ethiek zijn van toepassing, waaronder het begrip geïnformeerde toestemming, verantwoordingsplicht en toezicht.
- Het onderzoek wordt uitgevoerd met als doel de collectieve kennis en het welzijn van de samenleving te vergroten, in plaats van primair één of meerdere particuliere belangen te dienen.

⁴ Zie [commission.europa.eu what personal data considered sensitive](https://commission.europa.eu/what-personal-data-considered-sensitive)⁷.

⁵ Zie [20-01-06_opinion_research_en.pdf](#), p. 13⁷.

Definitie persoonsgegevens

Deze handreiking geldt als je voor jouw onderzoek *persoonsgegevens* verwerkt, namelijk:

1. **alle informatie:** gegevens waar betekenis aan zit gerelateerd aan een persoon zoals een naam, telefoonnummer, huisadres, informatie over gezondheid, politieke voorkeur of IP-adres;
2. **over:** de informatie zegt wat over iemand;
3. **een geïdentificeerde of identificeerbare:** het direct of indirect kunnen herleiden naar een individu, iemand specifiek kunnen aanwijzen;
4. **natuurlijk persoon:** gegevens van een levend persoon, bijvoorbeeld niet van bedrijven of iemand die is overleden.

Het begrip 'persoonsgegeven' verschilt per situatie: informatie kan voor de een wel een persoonsgegeven zijn en voor een ander niet. Denk bijvoorbeeld aan een kenteken. Pas als je toegang hebt tot de kentekendatabase van de RDW kun je zien op welke naam een voertuig is geregistreerd.

Informatie kan ook losstaand niet, maar in combinatie met andere informatie wél herleidbaar zijn naar een individu. Ook kan het zijn dat informatie dusdanig beveiligd is (bijvoorbeeld door maskering of encryptie), dat de gegevens niet meer (eenvoudig) herleidbaar zijn. Dit heet pseudonimiseren. De AVG is in ieder geval niet van toepassing op anonieme gegevens. Als het pseudonimiseren zo is gedaan dat het onredelijk veel vergt (qua budget of techniek) om toch te herleiden, dan kan het zijn dat de gegevens ook niet meer onder de scope van de AVG vallen⁶. Zie voor meer informatie hierover stap 2, paragraaf 2.4. [Pseudonimiseren en anonimiseren](#).

Er moet ook sprake zijn van een *verwerking* van persoonsgegevens. Alles wat met persoonsgegevens kan worden gedaan geldt als verwerking. Denk aan verzamelen, vastleggen, ordenen, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden, combineren, anonimiseren, wissen of vernietigen.

Gevoelige en bijzondere persoonsgegevens

De AVG stelt strengere eisen aan het verwerken van 'bijzondere categorieën van persoonsgegevens'⁷, zoals medische gegevens of geloofsovertuiging (zie de begrippenlijst in bijlage 3). De nadelige gevolgen zijn groter voor de onderzoeksdeelnemers als deze gegevens onvoldoende beschermd zijn. In de handreiking spreken we voor het gemak steeds van '*gevoelige gegevens*' omdat ook er ook gevoelige gegevens zijn (zoals bankrekeningnummer) die niet in de categorie bijzondere persoonsgegevens vallen, maar die ook extra bescherming nodig hebben.

⚠ Let op, het werken met bijzondere persoonsgegevens is verboden tenzij er een uitzondering geldt (zie artikel 9 AVG en artikel 24 UAVG).

⚠ Let op, het verwerken van het (gepseudonimiseerd) burgerservicenummer (BSN) is voor wetenschappelijk onderzoek binnen de setting van universiteiten en hogescholen niet toegestaan.

⁶ Guidelines on pseudonimisation: [edpb_guidelines_202501_pseudonymisation_en.pdf](#) ⁷ Overweging 26 AVG bepaalt welke factoren relevant zijn in het kader van anoniem te beschouwen data.

⁷ Zie [Bijzondere persoonsgegevens](#) ⁷ | Autoriteit Persoonsgegevens

Strafrechtelijke persoonsgegevens

Strafrechtelijke persoonsgegevens zijn heel gevoelige gegevens, maar die vallen niet onder het begrip 'Bijzondere persoonsgegevens'. Er gelden speciale regels voor. Overleg met je privacy-contactpersoon over het gebruik van dit soort gegevens.

Doel

De AVG legt een verantwoordingsplicht bij instellingen om aan te tonen dat zij rechtmatig persoonsgegevens verwerken. Zo moet de instelling kunnen aantonen dat een verwerking voldoet aan de kernprincipes van gegevensbescherming. Dit zijn: rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid.

Als je bij jouw onderzoek persoonsgegevens verwerkt, bijvoorbeeld van deelnemers, is het jouw taak aan deze principes te voldoen en dit aantoonbaar te maken. Hiermee bescherm je de rechten en vrijheden van de onderzoeksdeelnemers. Denk bijvoorbeeld aan de controle over je eigen gegevens houden, het voorkomen van discriminatie, stigmatisering, uitsluiting, financiële schade of lichamelijk schade.

Daarnaast zijn er andere redenen je aan de AVG te houden:

- zorgvuldige omgang met gegevens vergroot de kwaliteit en de betrouwbaarheid van je onderzoek(sresultaten);
- zorgvuldige omgang met gegevens behoudt het vertrouwen van deelnemers en het maatschappelijk veld in het onderzoek;
- schending van de AVG kan leiden tot reputatieschade en negatieve media-aandacht voor jouw instelling, faculteit/academie en voor jezelf als onderzoeker;
- schending van de AVG kan leiden tot boetes dan wel schadevergoedingen; en
- consortiumpartners, opdrachtgevers, subsidieverstrekkers en/of uitgevers vereisen naleving van de AVG.

De vertaalslag van de AVG naar de onderzoekspraktijk kan als complex worden ervaren. De handvatten van deze handreiking helpen deze complexiteit weg te nemen en het toepassen ervan leidt in algemene zin tot meer AVG-compliant onderzoek en eenduidigheid daarin.

Status en disclaimer

De handreiking heeft geen formeel juridische status. Het biedt uitsluitend handvatten en er worden geen verplichtingen opgelegd. Instellingen zijn, mits zij zich daaraan hebben gecommitteerd, gebonden aan de meest actuele versies van:

- de [Gedragscode gebruik persoonsgegevens in wetenschappelijk onderzoek](#)⁷; en
- de [Nederlandse gedragscode wetenschappelijke Integriteit](#)⁷.

Deze handreiking is uitsluitend bedoeld als hulpmiddel en informatief document. Het is de verantwoordelijkheid van de hogere onderwijsinstellingen om persoonsgegevens in onderzoek rechtmatig en zorgvuldig te verwerken volgens de AVG, al dan niet na het inwinnen van juridisch advies.

Leeswijzer

Na dit inleidende hoofdstuk volgt in hoofdstuk 2 een samenvatting die je helpt zorgvuldig met persoonsgegevens om te gaan. In de samenvatting zie je snel op welke plek in deze handreiking je toelichtende informatie kunt raadplegen. In hoofdstuk 3 vind je de stappen die je moet doorlopen om tijdens het hele onderzoek zorgvuldig met persoonsgegevens om te gaan. In de bijlagen vind je toelichtende informatie/hulpmiddelen.

Deze handreiking wordt periodiek herzien, ten minste eens per drie jaar of eerder als de (rechts)ontwikkelingen hiertoe aanleiding geven.

2 Samenvatting voor de onderzoeker

Een goede voorbereiding levert een soepele start en doorloop van het onderzoek op. Je weet dan bovendien waar je op moet letten als je tijdens het onderzoek zaken bijstelt. Stappen 1 t/m 3 vallen allemaal in de voorbereidende fase. Aan het eind van stap 3 kun je daadwerkelijk met het onderzoek starten. De samenvatting hieronder past bij de benadering volgens de Data Lifecycle van Harvard (zie paragraaf 3).

Stap 1 - Planning & Ontwerp

Dit is de voorbereidingsfase waarin je de basis legt voor een veilige en verantwoorde verwerking van de persoonsgegevens in je onderzoek. Belangrijk in deze fase is dat je de juiste wettelijke grondslag kiest voor het werken met de persoonsgegevens. Verder beschrijf je hier hoe je verschillende aspecten rondom het werken met persoonsgegevens aanpakt (bijvoorbeeld het doel van het onderzoek, welke AVG-rol van toepassing is, of je een DPIA uitvoert en hoe je de deelnemers informeert).

Stap 3 – Opslag & Beheer

In deze fase ga je het kader uit van stappen 1 en 2 concreet invullen, met de nadruk op toegangsmanagement en de juiste bescherming. Ook kijk je naar de mogelijkheid om te werken met anonieme of pseudonieme gegevens. Verder regel je de bewaar- en vernietigingstermijnen.

Stap 5 – Evalueren en Archiveren

Stap 5 is de afrondende fase en dat draait om archivering. Je onderzoek is klaar en je gaat nu daadwerkelijk aan de slag met je bewaar- en vernietigingstermijnen. Je slaat nog te bewaren persoonsgegevens op de juiste manier op en je verwijdert ze waar dat kan.

Stap 2 – Verzameling en Gebruik

Tijdens deze stap in de voorbereiding controleer je de transparantie richting de onderzoeksdeelnemers. Werk je met toestemming volgens de AVG (niet de ethische toestemming), dan regel je hier hoe je die toestemming op de juiste manier vraagt en wat je doet als iemand de toestemming intrekt. Je kijkt of je veilige middelen gebruikt en je meldt het onderzoek aan voor het verwerkingsregister.

Stap 4 – Analyse & Delen

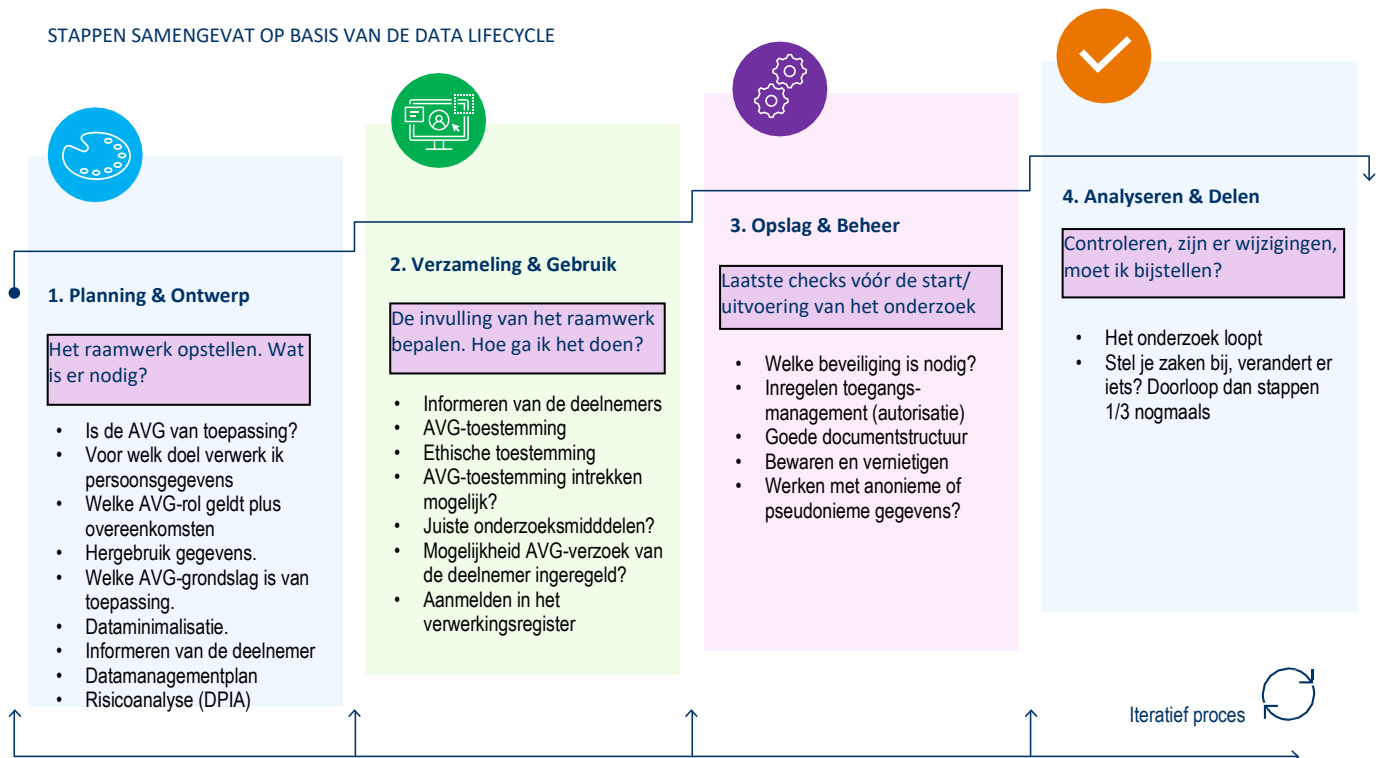
Tijdens deze fase ben je actief bezig met je onderzoek. Je controleert steeds of je nog veilig werkt als er zaken veranderen en of je eventueel al persoonsgegevens kunt verwijderen.

Stap 6 – Publiceren

In de laatste stap ga je over naar de publicatie van je onderzoek. Je zorgt ervoor dat er geen herleidbare persoonsgegevens worden gepubliceerd. Wil je de onderzoeksdataset delen, dan zorg je voor adequate anonimisering.

Op de volgende pagina een overzicht van de punten voor stappen 1 t/m 4.

STAPPEN SAMENGEVAT OP BASIS VAN DE DATA LIFECYCLE



Stappen 1 – 4 gaan concreet in op het werken met persoonsgegevens in onderzoek

Stappen 5 en 6 gaan over de afronding, zie daarvoor de stappen verderop in het document (evalueren, archiveren en publiceren).

Zie ook de checklist in bijlage 5.

3 Stappen onderzoekers

Data Lifecycle

De handreiking gebruikt de Data lifecycle voor onderzoek van Harvard, afgebeeld in schema 1.⁸



Schema 1: Data lifecycle van Harvard.

⁸ <https://datamanagement.hms.harvard.edu/plan-design/biomedical-data-lifecycle>⁷ Zie ook [Data Lifecycle Harvard – Information Security & Data Privacy](#)⁷ (Plan, Create/collect, Store, Use, Share, Archive/Destory).

In dit hoofdstuk vind je per stap van de lifecycle de vragen voor zorgvuldig gegevensgebruik waarmee je aan de slag kunt, al dan niet met behulp of advies van je interne of externe adviseurs. Het kan zijn dat de *lifecycle* binnen jouw instelling afwijkt, maar het stappenplan in deze handreiking is algemeen opgesteld, zodat je deze - al dan niet in gewijzigde vorm/volgorde - ook kunt toepassen als je een andere *lifecycle* volgt. Enkele stappen zijn samengevoegd. In het midden van de cirkel in schema 1 staat 'Store & Manage' ('Opslag & Beheer'). Dit onderdeel moet je binnen iedere stap opnieuw bekijken.

Stap 1: Planning & Ontwerp

1.1 Is de AVG van toepassing op mijn onderzoek?

Verwerking van persoonsgegevens

Eerst bepaal je of de AVG van toepassing is op jouw onderzoek. In de inleiding vind je informatie die helpt om vast te stellen of er sprake is van *persoonsgegevens* en van een *verwerking*.

De AVG is alleen van toepassing op (tot een natuurlijk persoon herleidbare) persoonsgegevens, en dus niet op gegevens die niet te herleiden zijn naar individuele personen. We spreken dan van anonieme gegevens. Als je concludeert dat je met anonieme gegevens werkt, hoeft je deze handreiking niet te volgen. Dat geldt ook als je gegevens zodanig pseudonimiseert dat het onevenredig veel moeite kost om ze naar individuele personen te herleiden. Kanttekening hierbij: de AVG is ook van toepassing op het pseudonimiseren en anonimiseren van persoonsgegevens. Ook dat zijn een verwerkingen van persoonsgegevens.

 Let op, écht anonimiseren of voldoende pseudonimiseren is erg moeilijk en gaat veel verder dan alleen het weghalen van namen. Check altijd bij de privacy-contactpersoon van je organisatie of je dit goed doet. Zie voor meer informatie hierover stap 2, paragraaf 2.4. Pseudonimiseren en anonimiseren.

Wees je ervan bewust dat het kan voorkomen dat je tijdens je onderzoek persoonsgegevens verzamelt die je niet voor je onderzoek zelf nodig hebt, doordat je wel mensen betreft (zelfs als je geen onderzoek doet naar personen). Denk daarbij bijvoorbeeld aan opnames van interviews waarin je weliswaar geen persoonlijke informatie verzamelt, maar op de opname kan de geïnterviewde herkenbaar zijn (door de stem of context) en dat geldt als een persoonsgegeven. Ook dan is de AVG van toepassing en moet je maatregelen nemen om hier zorgvuldig mee om te gaan. In de handreiking wordt voor het leesgemak gesproken van "onderzoeksdeelnemers" maar deze moet ruimer worden gelezen: het gaat over alle personen van wie je persoonsgegevens verwerkt

Binnen of buiten de EER?

De AVG is van toepassing⁹ als je onderzoek doet als onderdeel van een instituut dat in de Europese Economische ruimte (EER) is gevestigd, dus in een EU-land of Noorwegen, Liechtenstein en IJsland. Dat geldt ook als je onderzoek doet waarbij persoonsgegevens van mensen buiten dit gebied zijn

⁹ Zie Universiteit Gent, AVG: [wanneer is deze wetgeving van toepassing op mijn onderzoek?](#) ⁷

betrokken of als je van buiten de EER onderzoek doet naar personen in de EER. Onder omstandigheden is de AVG ook van toepassing als je samenwerkt met partijen die buiten de EER zijn gevestigd, zoals een consortium met niet-Europese onderwijsinstellingen. Bespreek en onderzoek met deze partijen of de AVG van toepassing is. Wissel je gegevens uit buiten de EER, bekijk samen met de privacy-contactpersoon van je organisatie of wellicht ook een DTIA (Data Transfer Impact Assessment) nodig is. Dat kan tot extra vereiste maatregelen leiden bij stap 2.

Is de AVG van toepassing op jouw onderzoek? Beantwoord dan de vragen van paragrafen 1.2 t/m 1.12.

1.2 Welke AVG-rol is van toepassing?

Bij een onderzoek zijn vaak meerdere partijen betrokken. Om te weten welke rechten en verplichtingen je hebt, moet je nagaan welke AVG-rol van toepassing is. De volgende twee rollen zijn mogelijk:

- **Verwerkingsverantwoordelijke.** Een verwerkingsverantwoordelijke bepaalt zelfstandig of samen met een andere partij de doelen en de middelen van de gegevensverwerkingen (de “hoe” en het “waarom”). Deze partij(en) is/zijn volledig verantwoordelijk en aansprakelijk voor naleving van de AVG.
- **Verwerker.** Een verwerker is de partij die ten behoeve (ook wel: in opdracht) van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Deze partij mag slechts op schriftelijke instructie van de verwerkingsverantwoordelijke verwerken en mag géén essentiële aspecten van de verwerking bepalen. Ook mag de verwerker de persoonsgegevens niet voor eigen doeleinden verwerken. Deze partij lift mee op de grondslag van de verwerkingsverantwoordelijke en heeft een beperkte aansprakelijkheid. Bijvoorbeeld de hostingpartij waar je je onderzoeksgegevens opslaat is een verwerker. Zie ook de voorbeelden hieronder.

In schema 2 zijn enkele veelvoorkomende situaties uitgewerkt.

Situatie	AVG-rol Verwerkingsverantwoordelijke	AVG-rol Zelfstandig of gezamenlijk verwerkingsverantwoordelijke	AVG-rol Verwerker
Onderzoek verricht door hogere onderwijsinstelling	Hogere onderwijsinstelling, bijvoorbeeld wanneer deze het onderzoeksplan schrijft en contact heeft met de deelnemers.	Zelfstandig verwerkingsverantwoordelijke als je je eigen doel nastreeft en daarvoor de middelen bepaalt. Als je in een samenwerkingsverband samen het middel bepaalt, maar elk van de samenwerkende partijen streeft een eigen doel na, dan is er ook sprake van zelfstandig verwerkingsverantwoordelijken	Een partij die ondersteunt bij de uitwerking van jouw onderzoek, is waarschijnlijk een verwerker. Denk aan transcribeerpartijen, partijen die audio- of video-opnames maken en (server) hostingpartijen (Google Drive, Research Drive, M365).

Situatie	AVG-rol Verwerkingsverantwoordelijke	AVG-rol Zelfstandig of gezamenlijk verwerkingsverantwoordelijke	AVG-rol Verwerker
Samenwerkingsverband tussen meerdere hogere onderwijsinstellingen	Hogere onderwijsinstelling (en)	Situatieafhankelijk. Bij een gezamenlijk onderzoeksproject, waarbij partijen samen al dan niet in meer of mindere mate het doel en de middelen bepalen kan sprake zijn van gezamenlijk verwerkingsverantwoordelijken.	Als jouw instelling enkel de instructies van de andere instelling uitvoert, en jouw instelling dus geen of nauwelijks (onderzoeks) vrijheid heeft om zelf te bepalen wat je met de persoonsgegevens wilt bereiken, is de kans groot dat jouw instelling verwerker is.

Schema 2 Rolverdelingen onderzoek

NB Als de andere partij penvoerder is of subsidie heeft gekregen voor het onderzoek, betekent niet automatisch dat jouw instelling verwerker is. Dit is een mogelijkheid, maar dit moet nader bepaald worden aan de hand van de feitelijke omstandigheden rondom de gegevensverwerkingen (wie bepaalt of bepalen het 'hoe' en 'waarom').

1.3 Heb ik de juiste overeenkomst(en) gesloten met deze partijen?

Als je duidelijk hebt welke rol jij en andere partijen hebben, is het belangrijk afspraken te maken met deze partijen. Denk aan hoe beide partijen zorgvuldig omgaan met persoonsgegevens en welke verantwoordelijkheid iedere partij daarin heeft, wat er moet gebeuren bij een datalek, een verzoek om inzage of verwijdering en ook wie en hoe je met de onderzoeksdeelnemers of de Autoriteit Persoonsgegevens communiceert.

Als je *gezamenlijk verwerkingsverantwoordelijke* bent, sluit je een overeenkomst voor gezamenlijke verwerkingsverantwoordelijkheid (GVO) af. Daarin leg je rechten en verplichtingen over en weer vast. Ook moet je de inhoud van deze regeling aan de onderzoeksdeelnemers kenbaar maken. Een aanwijzing dat de GVO de juiste overeenkomstvorm is, is dat er een consortiumovereenkomst ligt.

Deel je gegevens met een andere partij die *zelf verwerkingsverantwoordelijk* is, dan sluit je een gegevensuitwisselingsovereenkomst (een 'GUO')¹⁰ af. Hierin staat vaak opgenomen waar de verplichtingen van de een eindigt en van de ander begint. Ook gaat het om op welke (veilige)

¹⁰ Andere termen die hiervoor worden gehanteerd zijn 'Data Sharing Agreement' en 'Data Transfer Agreement'.

manier persoonsgegevens worden gedeeld. Partijen blijven ieder voor zich verantwoordelijk voor naleving van de AVG.

Werk je *samen met een verwerker* (de partij die je nodig hebt om bepaalde persoonsgegevens in jouw opdracht te verwerken) of ben je zelf een verwerker, dan leg je de afspraken vast in een verwerkersovereenkomst.

In bijlage 4 vind je een beslisboom als hulpmiddel voor het bepalen van de rolverdeling en de af te sluiten overeenkomsten.

Jouw privacy-contactpersoon kan je helpen met het bepalen van de juiste rol en het afsluiten van de juiste overeenkomsten.

1.4 Heb ik de juiste grondslag om persoonsgegevens te verwerken?

Om persoonsgegevens in jouw onderzoek te verwerken, heb je een grondslag nodig. De grondslagen staan genoemd in de AVG. Het is belangrijk om voor de start van je onderzoek te weten welke grondslag geldt voor jouw onderzoek. In principe is er geen hiërarchie tussen de grondslagen.

Het verwerken van bijzondere persoonsgegevens is in beginsel niet toegestaan, wel maakt de AVG ruimte voor uitzonderingen. Indien je bijzondere persoonsgegevens verwerkt kan het zijn dat daarvoor naast een van onderstaande grondslagen tevens een beroep moet doen op een van uitzonderingsgronden uit de AVG en/ of de UAVG.¹¹

Bekijk goed welke mogelijkheden er zijn en wat het beste past bij je onderzoek. Hieronder lichten we de relevante grondslagen toe (algemeen belang, toestemming en gerechtvaardigd belang).

Grondslag Taak van algemeen belang

In de inleiding is een definitie gegeven van wetenschappelijk onderzoek zoals we dat binnen deze handreiking hanteren. Als je wetenschappelijk onderzoek (waaronder praktijkgericht onderzoek) verricht, dan valt dat onder de taak van algemeen belang die universiteiten en hogescholen via de wet (Wet Hoger onderwijs en onderzoek, hierna “WHW”) hebben toegewezen gekregen. Kijken we naar de taakstelling uit de WHW dan moet het onderzoek aan bepaalde voorwaarden voldoen om een geslaagd beroep op deze verwerkingsgrondslag te doen.

Kort samengevat:

- Als universiteit verricht je fundamenteel onderzoek of toegepast onderzoek onder leiding van een hoogleraar. Als hogeschool verricht je doorgaans onderzoek gericht op de beroepspraktijk onder leiding van een lector.
- Jouw onderzoek dient een maatschappelijk belang/heeft geen primair privaat doel.
- Jouw onderzoek voldoet aan de relevante methodologische en ethische normen van de sector en wordt volgens goede praktijken (ethisch onderzoek) verricht.

Je hoeft in deze gevallen geen toestemming te vragen voor het verwerken van persoonsgegevens in jouw onderzoek in relatie tot de AVG, tenzij je bijzondere persoonsgegevens voor je onderzoek gebruikt. Check in dat geval bij je privacy-contactpersoon of er toch moet worden gekeken of (en

¹¹ Voor praktische voorbeelden van de uitzonderingsgronden, zie onderzoektips.ugent.be/nl/tips/00001839/ ↗

zo ja hoe) er toestemming kan worden gevraagd en regel dat zo nodig tegelijk met de ethische toestemming. Voor het gebruik van bijzondere persoonsgegevens gelden in ieder geval striktere beschermingseisen. Ook gelden er extra eisen voor het vragen van toestemming.

De grondslag 'algemeen belang' kan dus ook gelden wanneer je gevoelige gegevens gebruikt. Wel moet je hier waarschijnlijk extra veiligheidsmaatregelen nemen om de rechten van jouw onderzoeksdeelnemers te beschermen, maar je hoeft niet altijd toestemming te vragen. Neem over het nemen van extra maatregelen en het vragen van toestemming contact op met de privacy-contactpersoon van je organisatie.

Als je onderzoek voldoet aan de voorwaarden voor de AVG-grondslag 'taak van algemeen belang' kan je afwijken van bepaalde verplichtingen ten aanzien van de rechten van jouw onderzoeksdeelnemers, voor zover deze beperkingen nodig zijn om het beoogde onderzoeksdoeleinde te bereiken. Overleg dit met de privacy-contactpersoon van je organisatie.

Grondslag Toestemming vragen volgens de AVG-vereisten

Het kan voorkomen dat de mogelijke grondslag 'toestemming' is. Je vraagt dan de betrokken persoon om toestemming (naast eventuele ethische toestemming die gaat over (vrijwillige) deelname aan het onderzoek). Dat moet je wel op de juiste manier doen.

Voor een geslaagd beroep op toestemming volgens de AVG, moet je aan vier voorwaarden voldoen, de toestemming moet:

- vrijelijk,
- ondubbelzinnig,
- geïnformeerd, en
- specifiek zijn geven.¹²

Vrijelijk gegeven wil zeggen dat je een onderzoeksdeelnemer niet onder druk mag zetten of benadeelt bij het onthouden van toestemming. Ook moet je de deelnemer tijdig informeren over de verwerking(en) en de mogelijkheid van het intrekken van de toestemming. Het kan lastig zijn vrije toestemming te krijgen van kwetsbare groepen mensen of van mensen in een afhankelijke positie (zoals studenten, cliënten of patiënten) die vanwege een machtsverhouding druk kunnen voelen om toe te stemmen. Het intrekken van toestemming betekent dat je moet stoppen met de verwerking van de persoonsgegevens. Je moet ze dan verwijderen. Vraag je toestemming als je gevoelige persoonsgegevens verwerkt, dan geldt er een extra strenge toets en is er uitdrukkelijke toestemming nodig. Overleg met de privacy-contactpersoon van je organisatie hoe je op de juiste manier toestemming kunt vragen.

Grondslag Gerechtvaardigd belang

In andere gevallen kan je een beroep doen op de verwerkingsgrondslag van gerechtvaardigd belang. Gerechtvaardigd belang als grondslag voor de verwerking van persoonsgegevens voor onderzoek komt waarschijnlijk niet vaak voor. In die gevallen moet je een driestapstoets¹³ doorlopen:

¹² Zie Autoriteit Persoonsgegevens, [Grondslag toestemming](#)⁷

¹³ Zie Autoriteit Persoonsgegevens, [Grondslag gerechtvaardigd belang](#)⁷

1. er is sprake van een *gerechtvaardigd* belang van de voor de verwerkingsverantwoordelijke of van een derde (een belang dat niet in strijd is met de wet). Dit belang moet je kunnen benoemen; en
2. er is een noodzaak van de verwerking van de persoonsgegevens voor de behartiging van het gerechtvaardigde belang. De noodzaak moet je onderbouwen; en
3. de fundamentele rechten en vrijheden van de deelnemers prevaleren niet. Je moet hierbij een belangenafweging maken waarbij je kijkt naar de belangen van de organisatie voor het onderzoek en die van de betrokkenen. Des te gevoeliger de gegevens of des te kwetsbaarder de deelnemers zijn, des te zwaarder hun belangen wegen. Zorg dat je de Functionaris voor Gegevensbescherming (FG) betreft bij de belangenafweging en dat je de afweging documenteert.

De betrokkenen hebben overigens de mogelijkheid om bezwaar te maken tegen de verwerking.

De grondslag gerechtvaardigd belang kun je niet gebruiken als je gevoelige gegevens verwerkt in jouw onderzoek of voor die taken die jouw instelling uitvoert in het algemeen belang (onderzoek).

Toelichting ethische toestemming

Naast de toestemming als grondslag om persoonsgegevens te verwerken, is ook de ethische toestemming van belang: de toestemming voor deelname aan het onderzoek. Om verwarring te voorkomen tussen 'geïnformeerde toestemming' zoals bedoeld in de AVG, en de term 'informed consent' die ook wel voor ethische toestemming wordt gebruikt, hanteren we hier steeds 'ethische toestemming' om het verschil te duiden.

Ethische toestemming is een maatregel om de bescherming van het recht op menselijke waardigheid en het recht op menselijke integriteit te waarborgen.

Hoewel beide vormen van toestemming kunnen worden gecombineerd, is de ethische toestemming niet onderworpen aan dezelfde voorwaarden als de toestemming als rechtsgrond in de AVG. Vraag eventueel bij de ethische commissie van je organisatie na waar je rekening mee moet houden.

Voor onderzoek dat valt onder de Wet medisch-wetenschappelijk onderzoek (WMO) met mensen, kunnen er aanvullende eisen voor ethische toestemming zijn. Zie ook website van de Centrale Commissie Mensgebonden Onderzoek (ccmo.nl ⁷⁾).

Mocht je toestemming gebruiken als verwerkingsgrondslag van persoonsgegevens volgens de AVG, dan is het aan te raden dit in hetzelfde formulier te doen, maar zorg ervoor dat het verschil duidelijk is.

Anders dan 'toestemming als grondslag om persoonsgegevens te verwerken' is deze ethische toestemming niet bedoeld voor de naleving van de AVG. Je kunt beide vormen van toestemming

documenteren met behulp van hetzelfde formulier, maar het verschil moet wel duidelijk zijn (en het een leidt ook niet automatisch tot het ander).

1.5 Voorwaarden en voorbeelden van grondslagen

Als je persoonsgegevens verwerkt, moet je ook controleren of deze de noodzakelijkheidstoets doorstaat (tenzij de grondslag ‘toestemming’ van toepassing is, dan deze toets niet nodig).

Je kijkt daarbij naar de proportionaliteit en doeltreffendheid:

- Behaal je met de verwerking van gegevens het gestelde doel of is dat niet zeker?
- Staat het legitieme doel in verhouding tot het feit dat hiervoor persoonsgegevens moeten worden verwerkt?

En je kijkt naar de subsidiariteit:

- Is dit de beste manier om het te bereiken: kan het doel niet op een andere, minder ingrijpende wijze (met minder privacyinbreuk) worden bereikt?

In schema 3 vind je voorwaarden en voorbeelden van grondslagen:

Taak van algemeen belang	Voorwaarden	Voorbeelden
De verwerking van persoonsgegevens met het oog op wetenschappelijk onderzoek of onderzoek gericht op de beroepspraktijk kan worden gebaseerd op de ‘taak van het algemeen belang’. Deze taak is vastgelegd in de WHW. Niet ieder onderzoek valt hier automatisch onder.	• Jouw onderzoek wordt verricht door of onder leiding van een hoogleraar of lector. • Je kunt motiveren dat het onderzoek bijdraagt aan kennisvermeerdering en ziet op een maatschappelijk vraagstuk. • Jouw onderzoek voldoet aan de relevante methodologische en ethische normen van de sector, en conform goede praktijken (is ethisch, bijvoorbeeld door advisering door een ethische commissie). • Je hebt jouw onderzoek met passende waarborgen omkleed zodat de rechten van de deelnemers voldoende zijn beschermd. Het laatste geldt te meer als er gevoelige gegevens worden verwerkt. Zie voor de laatste voorwaarde de overige stappen in deze handreiking.	✓ Onderzoek naar armoedebestrijding of kansengelijkheid, gezondheid of welzijn, duurzame energie, veiligheid of ondernemerschap. Het kan zijn dat je hiervoor gevoelige gegevens verwerkt. ✗ Wanneer het onderzoek bepaald en betaald wordt door een commerciële organisatie voor eigen doeleinden, kan deze partij zich hier niet kan baseren, kies dan zo mogelijk voor ‘Toestemming’ als grondslag. Zie ook de AVG-rolverdeling. ✗ Institutioneel onderzoek (onderzoek met eigen data in het kader van de bedrijfsvoering van de eigen organisatie).

Toestemming	Voorwaarden	Voorbeelden
De grondslag toestemming is ook een grondslag die gebruikt kan worden bij onderzoek.	- Jouw onderzoek valt niet onder de taak van het algemeen belang. - Toestemming geven gebeurt door een duidelijke, actieve handeling, bijvoorbeeld via een schriftelijke verklaring. - De toestemming moet vrij gegeven zijn. - De betrokkene moet geïnformeerd zijn over de verwerking(en) en het intrekken van de toestemming. - De toestemming moet per verwerking van persoonsgegevens gevraagd worden. - Toestemming moet een actieve handeling zijn. - Jij moet kunnen aantonen dat je toestemming hebt verkregen. - Toestemming kan ieder moment worden ingetrokken, dus dit moet worden medegedeeld en hiervoor moet je een proces inrichten.	✓ Commercieel onderzoek, d.w.z. onderzoek waarbij de kennisvermeerdering in het belang is van een commerciële organisatie en niet voor de maatschappij. ✓ Onderzoek waarbij gevoelige gegevens worden verwerkt en dat niet onder de taak van algemeen belang valt.¹⁴ ✓ Het delen van jouw onderzoeksgegevens met andere (onderzoeks)partijen voor hergebruik wanneer de verenigbaarheidstoets negatief uitvalt. ✗ Onderzoek met (zeer) kwetsbare groepen deelnemers of mensen in een afhankelijke positie als ze hierdoor geen vrije toestemming kunnen geven.
Gerechtvaardigd belang	Voorwaarden	Voorbeelden
Soms is het mogelijk om als verwerkingsgrondslag het gerechtvaardigd belang van jouw instelling of van een derde te nemen voor onderzoek.	- Je beoordeelt of dit de beste manier is om het onderzoek uit te voeren - Jouw onderzoek valt niet onder de taak van het algemeen belang.	✓ Commercieel onderzoek, d.w.z. onderzoek waarbij de kennisvermeerdering in het belang is van een commerciële organisatie en niet primair voor de maatschappij. ✓ Onderzoek met beperkte impact op de rechten en vrijheden van onderzoeksdeelnemers, bijvoorbeeld

¹⁴ Soms mogen – onder voorwaarden – bijzondere persoonsgegevens zonder het vragen van toestemming worden verwerkt (o.a. zie artikel 24 UAVG). Overleg hiervoor met de privacy-contactpersoon van je organisatie.

	• je kunt een gerechtvaardigd belang benoemen (mag niet in strijd zijn met de wet). • Je kunt de noodzaak onderbouwen van de verwerking van de gegevens in relatie tot het gerechtvaardigde belang; • Je verricht een belangenafweging en de belangen van de deelnemers prevaleren niet (afhankelijk van de kwetsbaarheid van deze groep); • Je verwerkt geen gevoelige persoonsgegevens	door weinig/zeer algemene persoonsgegevens te gebruiken. ✓ Secundair gebruik/hergebruik, mits met juiste waarborgen. ✗ Onderzoek met gevoelige gegevens. ✗ Onderzoek met (zeer) kwetsbare groepen deelnemers. Of een groep kwetsbaar is hangt af van jouw onderzoek. Denk aan kinderen, ouderen, migranten, patiënten, andersvaliden, mensen die handelingsonbekwaam zijn etc.
--	--	--

Schema 3. Voorwaarden en voorbeelden grondslagen

Raadpleeg jouw privacy-contactpersoon als je twijfelt over jouw grondslag, over hoe je deze goed kunt motiveren en of je gevoelige gegevens verwerkt.

1.6 Heb ik een doel voor het verwerken van de gegevens?

Doeleinden

Je mag persoonsgegevens alleen verzamelen en gebruiken voor een welbepaald en duidelijk vooraf omschreven doel, in dit geval voor jouw onderzoek. Verdere verwerking van persoonsgegevens is in beginsel verboden zodra je het omschreven verwerkingsdoel hebt bereikt en verdere verwerking van de persoonsgegevens een ander doel heeft dat niet verenigbaar is met het doel dat je vooraf hebt omschreven.

Tips doelbinding

- ☐ Omschrijf jouw onderzoeksdoel zo concreet mogelijk zodat je kunt bepalen welke persoonsgegevens je voor welk doel voor of binnen het onderzoek nodig hebt (bijvoorbeeld voor communicatie met de deelnemers).
- ☐ Toets of de door jou gevraagde persoonsgegevens echt noodzakelijk zijn om dit doel te realiseren.
- ☐ Als je persoonsgegevens wilt *hergebruiken voor het doen van wetenschappelijk onderzoek*, dan wordt dat geacht verenigbaar te zijn met het oorspronkelijke doel en mag je deze gegevens gebruiken en zelfs delen met derden (tenzij je je op de grondslag 'toestemming' hebt gebaseerd, daarvoor geldt dat je alleen mag hergebruiken als je daar bij de toestemming al specifiek om hebt gevraagd). Let er wel op dat je dit mogelijk hergebruik vooraf meldt aan de deelnemers. De verenigbaarheidstoets (zie volgende bullet) kan dan achterwege blijven. Je moet dan wel:
 - afspraken maken met de ontvangers van de gegevens (zie 1.3);
 - de persoonsgegevens passend beveiligen. Denk bijvoorbeeld aan het toepassen van pseudonimisering, de toegang tot de gegevens te beperken, encryptie toe te passen,

beveiligde opslag te gebruiken. Je privacy-contactpersoon kan je meer vertellen over wat als passend wordt beschouwd in jouw situatie.

- ❑ Als je persoonsgegevens *voor iets anders dan wetenschappelijk onderzoek wilt hergebruiken*, dan moet je controleren of dat mag in relatie tot het oorspronkelijke doel van de verwerking. Dit heet de verenigbaarheidstoets (artikel 6, lid 4 AVG). Je mag persoonsgegevens alleen voor een ander doel hergebruiken als dit:
 - is gebaseerd op de toestemming van de onderzoeksdeelnemer;
 - de rechten en vrijheden van andere dan deze deelnemer niet in het geding zijn; en
 - de doeleinden van de verdere verwerking verenigbaar zijn met de doeleinden waarvoor je de persoonsgegevens aanvankelijk hebt verzameld.

Je moet beoordelen of het hergebruik binnen het verwachtingspatroon van de onderzoeksdeelnemers valt. De volgende factoren kunnen daarbij een rol spelen:

- het verband tussen het oorspronkelijk doel en het nieuwe doel;
- de context waarin de gegevens zijn verzameld;
- de soort en aard van de gegevens (betreffen het gevoelige gegevens?);
- de mogelijke gevolgen van het hergebruik (wat zijn de gevolgen voor de deelnemer?);
- het bestaan van voldoende technische en organisatorische maatregelen (denk aan pseudonimisering).

Valt dit gebruik niet binnen het verwachtingspersoon van de deelnemers? Dan kun je de gegevens niet hergebruiken. Bedenk dat het anonimiseren van die gegevens voor hergebruik ook geldt als een verwerking van persoonsgegevens. Hierover moet je van tevoren transparant zijn.

1.7 Vraag ik alleen die gegevens die nodig zijn voor mijn onderzoek?

Voorafgaand aan je onderzoek moet je erover nadenken of je persoonsgegevens nodig hebt voor het beantwoorden van jouw onderzoeksvraag of dat je kunt volstaan met anonieme data. En als je persoonsgegevens nodig hebt, denk dan goed na over *welke* persoonsgegevens noodzakelijk zijn. Beperk de gegevens tot een minimum. Je gebruikt alleen die persoonsgegevens die je nodig hebt om je doel te bereiken. Dit heet *dataminimalisatie*. Dit maakt het beheer eenvoudiger en vermindert de impact van een beveiligingsprobleem.

Door dataminimalisatie toe te passen is een onderzoeksdeelnemer ervan verzekerd dat er niet méér (gevoelige) gegevens over die deelnemers verwerkt. Daarnaast zijn de risico's bij een verkeerde verwerking, bijvoorbeeld bij een hack of bij het versturen van gegevens aan een verkeerde ontvanger, beperkter. En dat is gunstig voor zowel de onderzoeksdeelnemers als voor jouw instelling.

Stel je dus altijd de vraag: heb ik deze gegevens van deze persoon daadwerkelijk nodig voor het beantwoorden van mijn onderzoeksvraag? En zo ja, hoe gedetailleerd moeten deze gegevens zijn (of kun je bijvoorbeeld werken met minder gegevens, zoals geboortjaar in plaats van datum)?

Een voorbeeld hiervan is dat je uitsluitend per telefoon en per e-mail wilt communiceren met jouw onderzoeksdeelnemer. In dat geval is het niet nodig een huisadres op te vragen. Of wanneer je onderzoek doet naar digitale weerbaarheid van medewerkers, dan het niet nodig te vragen naar lidmaatschap van een vakbond.

Toereikend, relevant, noodzakelijk

Om aan dataminimalisatie te voldoen moet je ervoor zorgen dat de persoonsgegevens toereikend en relevant zijn en beperkt tot wat noodzakelijk is. Dit betekent het volgende:

- **Toereikend** - Voldoende om jouw onderzoek naar behoren te kunnen uitvoeren.
 *Let op: dit betekent dat je niet te veel maar ook niet te weinig gegevens moet verzamelen. Ook wanneer je te weinig gegevens hebt verzameld, kan het zijn dat je jouw onderzoeksvraag niet goed kunt beantwoorden of dat je hier later achteraan moet gaan.*
- **Relevant** - De persoonsgegevens hebben een rationeel verband met jouw onderzoek; en,
- **Beperkt tot wat noodzakelijk is** - Je verzamelt niet meer en je bewaart niet meer dan je voor jouw onderzoek nodig hebt. Dit betekent dat je ook moet nadenken over een bewaartermijn. Zie voor meer hierover bij stap 2.3.

Tips dataminimalisatie

- ☐ Ga zo snel mogelijk na of, en zo ja: waar je in je onderzoek kunt pseudonimiseren of anonimiseren.
- ☐ Vraag niet meer gegevens uit dan je nodig hebt. Vraag bijvoorbeeld om geboortjaar alleen en niet om de volledige geboortedatum, vraag om woonplaats in plaats van adres, verwerk alleen de vier cijfers van een postcode, werk met audio in plaats van video, etc.
- ☐ Werk waar mogelijk met meerkeuzevragen en zo min mogelijk met open vragen. De kans op herleidbaarheid en bijvoorbeeld stigmatisering is groter bij open vragen (want meer uniek).
- ☐ Doe de dataminimalisatie check in iedere stap binnen jouw onderzoek. Misschien had je in eerste instantie bepaalde persoonsgegevens wel nodig, maar zijn deze nu niet meer relevant.
- ☐ Bekijk daarnaast of het nodig is dat je weet wie welke vragenlijst heeft ingevuld. Is dat namelijk niet het geval, ontkoppel dan direct de antwoorden van de inzender. Dit kan bijvoorbeeld ook door respondenten geen persoonlijke link naar een vragenlijst te sturen maar een algemene link (ieder respondent dezelfde link).

Al deze informatie kun je opnemen in je datamanagementplan of onderzoeksprotocol.

1.8 Kan of wil ik (een deel van) de data hergebruiken/voor hergebruik beschikbaar maken?

Het is verstandig in de planningsfase van je onderzoek alvast na te denken over of je de gegevens die je nu voor je onderzoek gebruikt, kunt of wilt delen met andere (onderzoeks)partijen of eventueel later zelf nog wilt gebruiken voor wetenschappelijk onderzoek.

Tips hergebruik

- ☐ Ga na welke gegevens je wilt of kunt delen voor ander onderzoek (zie stap 1.8 en stap 4).
- ☐ Ga na of de gegevens kunnen worden geanonimiseerd (zie stap 2.4).
Is anonimiseren niet mogelijk, deel dan niet meer dan de gegevens die nodig zijn voor het doel waarvoor je de gegevens deelt (zie stap 1.7).

- ☐ **Evalueer de grondslag voor deze verdere verwerking:**
 - Als voor jouw onderzoek toestemming is gegeven, dan moet er ook toestemming zijn gegeven voor hergebruik ervan voor verenigbare doelen (zie 'Tips doelbinding', 1.6).
 - Zijn de gegevens verzameld met een beroep op een taak van algemeen belang, dan moet ook dit nieuwe onderzoek onder de taakstelling vallen. Dit geldt ook als je de gegevens verstrekt aan andere partijen.
- ☐ **Ga na of het delen van deze gegevens binnen de verwachting van de onderzoeksdeelnemers valt.**
- ☐ **Zorg voor passende beveiliging van deze gegevens, bij voorkeur door pseudonimisering toe te passen, de toegang tot de gegevens te beperken, encryptie toe te passen, beveiligde opslag te bewerkstelligen en afspraken te maken met de ontvangers van de gegevens (stap 2.4).**
- ☐ **Geef in het datamanagementplan en het register van verwerkingsactiviteiten aan dat je voornemens bent de gegevens te hergebruiken dan wel te delen met derde partijen voor hergebruik. Zie stap 1.11 en bijlage 1).**

Als je geanonimiseerde gegevens ontvangt of deelt, dat wil zeggen dat jij of de andere partij de gegevens niet kunt herleiden naar natuurlijke personen, dan is de AVG niet van toepassing voor jou of die partij.

Zie voor meer informatie hierover Stap 2: Opslag & Beheer.

Heb je vragen over hergebruik van persoonsgegevens en de praktische implicaties hiervan voor jouw onderzoek? Neem contact op met de privacy-contactpersoon van jouw instelling.

1.9 Informeer ik de deelnemers op de juiste wijze?

De onderzoeksdeelnemer heeft recht op informatie. Als onderzoeker is het jouw taak de deelnemers te informeren op een behoorlijke, begrijpelijke en transparante wijze. Doorgaans gebeurt dit in de informatiebrief en/of het toestemmingsformulier. In Stap 3 gaat de handreiking uitgebreid in op de wijze van voorafgaand informeren en de overige voorwaarden.

 Het is belangrijk hier te noemen dat je niet mag beginnen met het verwerken van persoonsgegevens totdat je de onderzoeksdeelnemers hebt geïnformeerd (tenzij hier uitzonderingen op van toepassing zijn).

1.10 Moet ik een DPIA uitvoeren?

Een *data protection impact assessment* ('DPIA') is een instrument waarmee je de impact van jouw voorgenomen gegevensverwerking bepaalt en risicobeperkende maatregelen opneemt (en ook treft).

Misschien moet je een DPIA uitvoeren voordat je met jouw onderzoek begint. Je verricht een DPIA wanneer de verwerking van deze gegevens *waarschijnlijk* een hoog risico voor de rechten en vrijheden van de onderzoeksdeelnemers vormt.

Denk daarbij bijvoorbeeld aan:

- het verwerken van gevoelige persoonsgegevens, al dan niet op grote schaal;
- wanneer je gegevens van kwetsbare groepen verwerkt, zoals kinderen, werknemers, patiënten, mensen die onder de armoedegrens leven, of mensen in een afhankelijke positie (zoals patiënten, cliënten), etc.;
- of er sprake is van gecombineerde datasets waarbij het verwerken mogelijk niet aansluit bij de verwachting van een deel van de deelnemers;
- of je nieuwe technologieën gebruikt (automatische besluitvorming/AI).

Raadpleeg jouw privacy-contactpersoon om te bepalen of een DPIA nodig is. Mocht dit het geval zijn, dan mag je nog niet beginnen met het verwerken van de persoonsgegevens totdat het assessment is afgerond.

1.11 Voldoet mijn datamanagementplan aan de AVG?

Het opstellen van een datamanagementplan ('DMP') is een essentiële stap bij het plannen en ontwerpen van onderzoek waarin persoonsgegevens worden verwerkt. Een DMP stimuleert je om vooraf goed na te denken over de omgang met persoonsgegevens gedurende het gehele onderzoeksproces. Het is van belang om ook de AVG-aspecten hierin mee te nemen.

Omschrijf op welke manier je met persoonsgegevens omgaat en hoe je voldoet aan de beginselen van de AVG, zoals rechtmatigheid, transparantie en dataminimalisatie. Voor de AVG is het van belang dat je in het DMP ten minste stilstaat bij de volgende aspecten:

1. Onderzoeksdoel en risico's

Je gaat na welke persoonsgegevens je verzamelt, waarom deze nodig zijn, en hoe je de hoeveelheid gegevens minimaliseert. Geef ook aan op welke manier je toestemming verkrijgt of op welke andere grondslag je deze gegevens zal verkrijgen. Je hebt zo nodig een DPIA uitgevoerd.

2. Opslag

Je geeft aan hoe je de persoonsgegevens veilig opslaat. Vraag binnen je instelling na welke tools en infrastructuur hiervoor beschikbaar zijn en volg de interne afspraken voor opslag. Denk aan lokale systemen en beveiligde cloudomgevingen, zoals SURF Research Drive. Daarnaast beschrijf je zo nodig welke aanvullende technische en organisatorische maatregelen je treft om gegevens voldoende te beschermen. Vraag je privacy-contactpersoon om hulp.

3. Delen (autorisatie en toegangsbeveiliging)

Je omschrijft welke personen toegang hebben tot gegevens in welke fase van het onderzoek. Je geeft aan met wie je de gegevens deelt en waarom. Je licht toe hoe je veilige samenwerking en uitwisseling van gegevens faciliteert, bijvoorbeeld door versleuteling of geanonimiseerde datasets.

4. Bewaren en vernietigen

Je geeft aan wat er met gegevens gebeurt tijdens en na afloop van het onderzoek. Hoe en wanneer worden gegevens verwijderd en/of geanonimiseerd voor archivering.

Het DMP biedt niet alleen houvast voor jezelf, maar het helpt ook om aan te tonen dat je maatregelen neemt om te voldoen aan de AVG. Vaak wordt een DMP ook door subsidieverstrekkers of opdrachtgevers geëist. Maak het DMP tot een levend document en pas het aan wanneer dat nodig is tijdens je onderzoek.

Wil je meer weten over het opstellen van een DMP? Raadpleeg dan de informatiepagina's, richtlijnen en templates die beschikbaar zijn via je instelling of onderzoeksorganisatie, of neem contact op met de datasteward van jouw instelling. In bijlage 1 vind je een template van een DMP.

1.12 Onderzoek met/door studenten

Als onderzoek wordt uitgevoerd door of met studenten, moet je extra goed kijken naar de grondslag. Als onderzoek alleen voor educatieve doeleinden wordt uitgevoerd, kun je je bijvoorbeeld waarschijnlijk niet baseren op de grondslag 'algemeen belang'.

Aandachtspunten:

- Kies de juiste grondslag;
- Bepaal op welke manier je het toegangsmanagement wilt regelen (krijgen studenten toegang tot alle data, of beperk je dit?);
- Is er misschien een non-disclosure agreement nodig?

Zorg als onderzoeker altijd voor extra begeleiding van studenten tijdens het onderzoek en regel de eindverantwoordelijkheid van de begeleider/supervisor.

Stap 2: Verzameling & Gebruik

In deze fase ga je over tot het verzamelen van persoonsgegevens en verwerk je deze voor je onderzoek. Voor deze fase zijn vijf vragen van belang die je eerst moet nalopen om zorgvuldig om te gaan met de rechten en vrijheden van jouw onderzoeksdeelnemers.

2.1 Hoe informeer ik de onderzoeksdeelnemers over het gebruik van hun persoonsgegevens op een manier die voldoet aan de AVG?

Je moet onderzoeksdeelnemers altijd tijdig (voorafgaand) informeren over hoe je met hun persoonsgegevens omgaat tijdens en na jouw onderzoek (tenzij er een uitzondering geldt). Als je toestemming als grondslag gebruikt, moet je bovendien extra informatie verstrekken om rechtmatig een beroep te kunnen doen op de grondslag toestemming.

Tips informeren onderzoeksdeelnemers

☐ **Verstrek de juiste informatie, afhankelijk van waar je je gegevens vandaan hebt**

Voor het verstrekken van die informatie aan de onderzoeksdeelnemers maakt de AVG een onderscheid tussen of je de persoonsgegevens bij de deelnemer zelf of via een andere bron hebt verkregen. Denk bijvoorbeeld aan hergebruik doordat je gegevens van een andere partij hebt ontvangen. Afhankelijk hiervan moet je bepaalde informatie aanleveren.

In schema 5 staat welke informatie je moet verstrekken.

Informatie die je vooraf aan de deelnemer moet worden geven wanneer je de persoonsgegevens hebt gekregen van:	deelnemer	een andere bron
De identiteit en contactgegevens van de instelling of organisatie namens wie je het onderzoek uitvoert, en als die instelling niet in de EER is gevestigd de	✓	✓

Informatie die je vooraf aan de deelnemer moet worden geven wanneer je de persoonsgegevens hebt gekregen van:	deelnemer	een andere bron
identiteit en contactgegevens van de vertegenwoordiger van die instelling in de Europese Unie (EU).		
De contactgegevens van de functionaris voor gegevensbescherming (FG) van de instelling of organisatie namens wie je het onderzoek uitvoert	✓	✓
Doeleinden van de verwerking van persoonsgegevens zoals die in het register van verwerkingsactiviteiten zijn opgenomen en de AVG-grondslag. Is de AVG-grondslag gerechtvaardigd belang? Vermeld dan ook op welk belang een beroep wordt gedaan.	✓	✓
De (categorieën van) ontvangers van de persoonsgegevens. D.w.z. de gegevens van organisaties (ontvangers) en/ of een beschrijving van het type organisaties (categorieën van ontvangers) waarmee persoonsgegevens worden gedeeld of waaraan toegang tot de persoonsgegevens wordt verleend	✓	✓
Als je van plan bent de persoonsgegevens door te geven buiten de EER of aan een internationale organisatie op welke juridische grond je dat gedaan wordt.	✓	✓
De categorieën van verwerkte gegevens.		✓
Bewaartermijnen, of indien onmogelijk, de criteria om de termijnen te bepalen.	✓	✓
Het recht op inzage, wissing, rectificatie, beperking, bezwaar en overdraagbaarheid. Let op: als er sprake is van wetenschappelijk onderzoek, gelden een aantal van deze rechten niet. Het recht op gegevensoverdracht geldt overigens alleen bij de grondslagen 'uitvoering overeenkomst' en 'toestemming'.	✓	✓
Wanneer een verwerking is gebaseerd op de AVG-grondslag toestemming: het recht om de toestemming te allen tijde in te trekken.	✓	✓
Het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP).	✓	✓
Of betrokkenen wettelijk of contractueel verplicht zijn de persoonsgegevens te verstrekken en wat de (mogelijke) gevolgen zijn als betrokken de gegevens niet verstrekt. NB Dit is niet altijd relevant voor wetenschappelijk onderzoek.	✓	
Of er gebruikmaakt van geautomatiseerde besluitvorming, inclusief profilering, hoe besluiten tot stand komen en het recht op uitleg door een mens.	✓	✓
Als u de gegevens van een andere organisatie heeft gekregen: de bron waar de persoonsgegevens vandaan komen. En wanneer dat het geval is dat gegevens afkomstig zijn van openbare bronnen.		✓

Schema 5. Informatie deelnemers

☐ **Weet wanneer je de onderzoeksdeelnemers niet hoeft te informeren**

Je hoeft de deelnemers geen informatie te verstrekken als ze dezelfde informatie al in het verleden al hebben ontvangen. Dit moet je als onderzoeker dan wel kunnen aantonen.

☐ **Persoonsgegevens uit een andere bron, soms deelnemers informeren niet nodig**

Wanneer je persoonsgegevens uit een ander bron hebt gekregen, hoef je bovenstaande informatie ook niet te verstrekken als:

- dat onmogelijk is of onevenredig veel inspanning vergt; of
- het verkrijgen of verstrekken van de gegevens wettelijk is voorgeschreven; of
- de persoonsgegevens vertrouwelijk moeten blijven vanwege een wettelijk beroepsgeheim (zie artikel 14 lid AVG).

Het blijft van belang dat je moeite doet om de informatie ergens te verstrekken, bijvoorbeeld via een nieuwsbrief of een belangenvereniging en te publiceren op een website.

In het geval van hergebruik hoef je de deelnemer niet te informeren als:

- de betrokkene al over de informatie beschikt; of
- wanneer het verstrekken van de informatie onevenredig veel inspanning zou vergen, in het bijzonder bij verwerking met het oog wetenschappelijk of historisch onderzoek. Bij hergebruik van gepseudonimiseerde gegevens is het informeren van betrokkenen over de nieuwe verwerking van hun gegevens vaak niet haalbaar. Als dit niet haalbaar is leg je vast waarom niet, zodat je dit kunt verantwoorden als de toezichthouder hierom vraagt; of
- als informeren tot gevolg heeft dat je het doel van de verwerking van de persoonsgegevens niet meer kunt bereiken of als het daardoor ernstig in het gedrang komt.

☐ **Informeer op een duidelijke en begrijpelijke manier (schriftelijk en op verzoek ook mondeling)**

Deelnemers moeten de inhoud goed begrijpen, ook de informatie over de verwerking van hun persoonsgegevens. Ga na of:

- Nederlands of Engels wel de juiste taalkeuze voor jouw doelgroep is of dat een andere taal of talen verstandiger is/zijn (ook gebarentaal kan een optie zijn);
- het taalniveau is aangepast op jouw doelgroep qua leeftijd, zeker als sprake is van minderjarigen, gebruik bijvoorbeeld een tool die je helpt om op taalniveau B1¹⁵ te schrijven en gebruik plaatjes als dat kan;
- de woordkeuze past bij jouw doelgroep, bijvoorbeeld als sprake is van kwetsbare groepen, hogleraren of overheidsfunctionarissen waar jouw onderzoek op ziet.

Het is aan te raden om informatie gelaagd te verstrekken: je geeft de benodigde informatie op het juiste moment en niet meer dan dat. Op die manier voorkom je dat je juist minder transparant bent door een overload aan informatie en je voorkomt dat de betrokkene de essentie en het overzicht verliest. De gelaagde verstrekking van de informatie verenigt het vereiste van beknoptheid met het vereiste om alle noodzakelijke informatie te verstrekken.

¹⁵ Zie tips via communities.surf.nl⁷, paktaal.nl/taalniveaus⁷ en accessibility.nl/kennisbank/tools/leesniveau-tool⁷

☐ **Informeer kosteloos**

Je mag geen geld vragen voor de informatieverstrekking.

☐ **Stem de inhoud van de informatiebrief, het (eventuele) toestemmingsformulier en het datamanagementplan op elkaar af**

De informatie die je aan de deelnemer verstrekt, moet aansluiten bij het interne proces. Voorkom daarom dat de verschillende documenten van elkaar afwijken, anders zijn er namelijk aanpassingen nodig die gevolgen kunnen hebben voor de risico-inschatting en de benodigde maatregelen of wellicht moet het DMP worden aangepast.

☐ **Informeer voorafgaand aan de gegevensverwerking**

Je mag geen persoonsgegevens gebruiken vóórdat je hebt geïnformeerd. Als je de persoonsgegevens van de betrokkenen zelf krijgt moet je ze informeren op het moment van inzameling van de persoonsgegevens. Als je persoonsgegevens uit een andere bron krijgt, moet je de informatie uiterlijk één maand na het moment van verkrijging van de persoonsgegevens aan betrokkene geven. Die termijn mag korter maar nooit langer dan één maand zijn:

- Wanneer je de persoonsgegevens gebruikt om met betrokkene te communiceren moet betrokkene uiterlijk informeren op het moment van eerste contact;
- Wanneer je de gegevens aan een ander (ontvanger) wil doorgeven moet je betrokkene uiterlijk informeren op het tijdstip van de doorgifte van de persoonsgegevens;
- Bij latere wijziging van de verwerking (bijvoorbeeld nieuwe ontvangers, nieuwe verenigbare doeleinden, doorgifte buiten de EU, etc.) moet je betrokkene daarover vooraf informeren en dat moet je ruim op tijd doen, zodat de betrokkene de tijd heeft om eventueel rechten uit te oefenen.

☐ **Verstrek specifieke informatie als je toestemming gebruikt als grondslag en vraag op de juiste wijze toestemming**

Als je toestemming vraagt voor verwerking van de persoonsgegevens, geef dan ook aan dat de toestemming altijd kan worden ingetrokken en hoe. Je moet toestemming ontvangen van de ouder/wettelijk vertegenwoordiger als een onderzoeksdeelnemer jonger is dan 16 jaar.

Toestemming moet per verwerking van persoonsgegevens worden gevraagd. Dat wil zeggen dat je ook per onderzoek toestemming vraagt als je de gegevens voor verschillende onderzoeken gebruikt. In de praktijk kan dit lastig zijn op voorhand heel specifiek te zijn. Wees zo specifiek mogelijk en gebruik eventueel een getrapte toestemming, waarbij deelnemers gedurende een bepaalde tijdsduur op verschillende momenten toestemming kunnen geven voor een op dat moment nader bekend onderzoek.

Daarnaast moet sprake zijn van een actieve handeling zoals een handtekening of een vinkje zetten, een opt-in (dus geen opt-out: 'ik verwerk je gegevens tenzij je aangeeft dat je het niet wil').

Voorbeelden van methodes voor het verkrijgen van toestemming:

- Via een digitaal of op papier ondertekend toestemmingsformulier.
- Via een online vragenlijst (waarbij de betrokkene is geïnformeerd dat invullen van de vragenlijst als toestemming wordt gezien).

- Mondeling. Bijvoorbeeld door dit op audio/video opnames of in aanwezigheid van een getuige vast te leggen.

Een voorbeeld van wat er in een toestemmingsformulier moet worden opgenomen, tref je aan in bijlage 2.

2.2 Heb ik een procedure klaar als een onderzoeksdeelnemer de toestemming intrekt?

Toestemming volgens de AVG mag altijd worden ingetrokken en na intrekking mogen de persoonsgegevens (vanaf dat moment) niet meer verwerkt worden. Je moet deze gegevens dan verwijderen. Let op, het gaat hier dus niet om de ethische toestemming.

Het intrekken van toestemming is een absoluut recht. Je moet hier in principe altijd gehoor aan geven, zelfs als je vermoedt dat je onderzoek hiermee in gevaar komt. Je mag vanaf het moment van intrekken de gegevens niet verder verwerken. Een verzoek om intrekken van de toestemming kun je niet honoreren als de persoonsgegevens zijn geanonimiseerd. De gegevens zijn dan niet meer herleidbaar naar een individu.

Je hebt de onderzoeksdeelnemers hierover geïnformeerd. Dan is het belangrijk intern een proces in te richten, of aan te haken bij bestaande processen binnen jouw instelling. Op die manier kun je (snel) gehoor geven aan het intrekken van de toestemming.

2.3 Sla ik de toestemmingsformulieren op een veilige plek op?

Als onderzoeker moet je kunnen aantonen dat je toestemming hebt gekregen. Bewaar de gegeven toestemmingen daarom goed. In veel gevallen kun je werken met een informatiebrief en apart toestemmingsformulier waarbij je op het toestemmingsformulier naar de informatiebrief verwijst. Je bewaart alle toestemmingsformulieren, maar de informatiebrief hoeft je maar éénmaal te archiveren en niet voor iedere respondent afzonderlijk, immers deze informatiebrieven zijn allemaal identiek.

Je moet de toestemmingsformulieren op een veilige plek opslaan, bijvoorbeeld binnen Research Drive. De toegang tot deze formulieren moet je beperken tot het noodzakelijke (net zoals de toegang tot sleutelbestanden voor pseudonimisering). Niet iedere onderzoeker of andere medewerker hoeft toegang te hebben.

Hoe lang je zo'n formulier moet bewaren, hangt af van de wijze waarop de dataverzameling is ingericht. Als er tijdens het onderzoeksproject persoonsgegevens worden geanonimiseerd en er geen bronbestanden (meer) zijn met herleidbare gegevens en er is geen behoefte meer om extra gegevens van de respondenten te verzamelen, dan kan ook het nut van de verzamelde toestemmingsformulieren zijn verstreken (houd wel altijd rekening met het kunnen aantonen van de onderzoeksintegriteit).

2.4 Gebruik ik veilige onderzoeksmiddelen?

Wanneer je (digitale) onderzoeksmiddelen inzet, is het belangrijk na te gaan of deze middelen in lijn zijn met het beleid van jouw instelling. Is er geen beleid of bestaat hier onduidelijkheid over,

houdt er dan rekening mee dat in ieder geval deze middelen ook moeten voldoen aan de AVG (dan wel dat jij afspraken maakt over hoe een eventuele andere partij met de onderzoeksgegevens omgaat).

Tips veilige inzet onderzoeksmiddelen

- ☐ Ga na of jouw instelling beleid heeft over het gebruik van privételefoons, opnames of kunstmatige intelligentie. Zo ja, houd je hieraan of volg de procedure in jouw instelling voor afwijkingen van beleid.
- ☐ Ga na of jouw instelling (of afdeling) bepaalde (onderzoeks)tools heeft goedgekeurd. Houd er rekening mee dat je vaak een proces moet doorlopen voor het aanvragen van nieuwe (onderzoeks)tools in je organisatie als je die nodig hebt.
- ☐ Kies aanbieders van onderzoeksmiddelen die (voor zover je kunt nagaan) goed met persoonsgegevens omgaan. Dat wil zeggen dat ze aan de basisprincipes van de AVG moeten voldoen, mede afhankelijk van of zij verwerkingsverantwoordelijk of verwerker zijn. Raadpleeg de website en lees de privacyverklaring en de gebruikersovereenkomst (eventueel voorzien van verwerkersovereenkomst) om je een beeld te vormen.
- ☐ Ga na of de aanbieders persoonsgegevens voor eigen doeleinden gebruiken. Dit kan het geval zijn, bijvoorbeeld voor analytische doeleinden om hun dienstverlening te verbeteren. Dit kan ook voor direct marketingdoeleinden of doorverkoop aan derden. Vraag jezelf af of je dit wenselijk en/of passend vindt en of dat AVG-compliant is. Zo niet, onderhandel dat deze gegevens hiervoor niet worden gebruikt, of kies een andere partij om mee samen te werken.
- ☐ Maak afspraken over de omgang met persoonsgegevens in de juiste overeenkomst (zie stap 1.3).
- ☐ Check altijd op aanwezigheid van (survey)tools in de eigen instelling. Vaak moet je die verplicht gebruiken en is er nagedacht over punten als:
 - o op welke manier deze partij jouw onderzoeksdeelnemers informeert;
 - o of de ingevulde survey's adequaat beveiligd zijn;
 - o wat er gebeurt als er sprake is van een mogelijk beveiligingsincident of datalek;
 - o via welke systemen je de gegevens opslaat
 - o of de persoonsgegevens binnen de EER worden opgeslagen;
 - o of de gegevens met derde partijen worden gedeeld;
 - o of de gegevens kunnen worden gepseudonimiseerd of geanonimiseerd;
 - o of de gegevens kunnen worden ingezien (door de onderzoeksdeelnemer) of worden verwijderd (bijvoorbeeld na het aflopen van de termijn voor het invullen van de surveys).

Ga ook in deze stap van jouw onderzoek na of jouw beveiliging nog passend is (zie Stap 2: Opslag & Beheer).

2.5 Heb ik mijn onderzoek aangemeld in het register van verwerkingsactiviteiten?

Jouw instelling moet in het kader van de verantwoordingsplicht een register van de verwerkingsactiviteiten bijhouden. Als onderzoeker moet je de verwerking van persoonsgegevens voor jouw onderzoek daarin (laten) registreren. De registratie doe je in principe voor elke nieuwe verwerking. Het datamanagementplan kan hierbij helpen, zie stap 1.11.

Daarnaast is het belangrijk om de informatie met betrekking tot de geregistreerde verwerkingsactiviteiten up-to-date te houden gedurende de looptijd van je onderzoek.

Stap 3: Opslag & Beheer

3.1 Welke maatregelen kan ik treffen om de gegevens te beveiligen?

Als onderzoeker moet je de persoonsgegevens in jouw onderzoek iedere stap in jouw onderzoek *passend* beveiligen. Deze stap komt bij iedere vervolgstap in de lifecycle terug. Check altijd de eisen die jouw instelling aan informatiebeveiliging stelt. Wat passend is, hangt af van meerdere omstandigheden. Denk aan:

- de schaalgrootte van de gegevens;
- de context van jouw onderzoek;
- de gevoeligheid van de gegevens;
- wie toegang moet hebben tot de gegevens;
- of je deze gegevens met meerdere partijen deelt;
- wat de stand van de techniek is op het gebied van beveiligingsmaatregelen.

In deze handreiking geven we geen uitputtende set aan maatregelen. Stem dit af met de privacy-contactpersoon van je organisatie. Sla nooit zomaar gegevens op je privéapparatuur en privéclouds op. Denk in ieder geval aan de volgende maatregelen.

Maatregelen

☐ **Beperk de toegang**

Beperk de toegang tot de persoonsgegevens tot de personen die dit echt nodig hebben voor jouw onderzoek(sondersteuning). Dit geldt zowel voor personen van jouw eigen instelling als samenwerkingspartners en derden die de gegevens moeten ontvangen.

Stel hiervoor een autorisatiematrix op. Meestal heeft je organisatie hier een template voor. Ga uit van rollen en niet van personen.

☐ **Voorkom ongeautoriseerde toegang**

Zorg ervoor dat je toegang tot gegevens authenticceert. Beveilig de toegang tot de persoonsgegevens met multifactorauthenticatie (MFA). Dit is tegenwoordig een basismaatregel voor informatiebeveiliging. Gebruik waar mogelijk een Virtueel Particulier Netwerk (VPN)-verbinding als je van buiten je instelling toegang wil tot je gegevens. Vaak dwingt je organisatie dat ook af. Een VPN-verbinding helpt om je te beschermen tegen het onderscheppen van je data door een kwaadwillende.

☐ **Technische beveiliging systemen**

Voer altijd softwareupdates door, gebruik een firewall en houd je aan de overige maatregelen op jouw systemen die voldoen aan de stand van de techniek.

☐ **Maak een back-up**

Zorg periodiek voor een back-up, zodat jouw onderzoeksinformatie niet verloren gaat als er problemen zijn met de toegang tot jouw systemen dan wel het systeem crasht. Gebruik daarvoor de back-upfaciliteit die jouw organisatie aanbiedt en niet bijvoorbeeld Dropbox en beveilig deze back-up met een extra wachtwoord als dat nodig is. Check dus wat je organisatie geregeld heeft voor back-ups, qua locatie, frequentie, etc. en lift hierop mee.

☐ **Deel persoonsgegevens veilig**

Gebruik [Research Drive](#)[↗] en/of [SURFfilesender](#)[↗] als je gevoelige bestanden of onderzoeksinformatie wil delen. Gebruik geen e-mail om gegevens te delen, omdat de kans op datalekken/ongeautoriseerde toegang hierdoor groot is.

☐ **Pas je documentenstructuur aan**

Bij het organiseren van je documenten is het belangrijk dat bestands- en mapnamen geen informatie bevatten die direct herleidbaar is tot individuele personen. In paragraaf 2.2 vind je een aantal concrete manieren om de bestands- en mapnamen te kiezen.

☐ **Beperk de opslag tot de EER**

Om controle te houden over jouw onderzoeksgegevens, is het verstandig de doorgifte/opslag buiten de EER zoveel mogelijk te beperken.

☐ **Hanteer een clean desk**

Laat geen onderzoeksinformatie in het zicht van derden liggen (binnen en buiten de instelling). Gebruik je fysieke papieren, zoals ingevulde vragenlijsten, berg die dan op in een kast die op slot kan (en doe deze ook op slot).

☐ **Beperk toegang tot instellingen/locatie**

Zorg ervoor dat de plekken waar je de onderzoeksinformatie bewaard afgesloten kunnen worden en alleen toegankelijk zijn voor mensen die toegang mogen hebben (b.v. met een sleutel of persoons- of functiegebonden pasje).

☐ **Sla de gegevens niet langer op dan noodzakelijk**

Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk voor het doel van jouw onderzoek. In het kader van reproduceerbaarheid en het bevorderen van hergebruik van data wil je data mogelijk langere tijd bewaren. Dit betekent dat je moet nadenken over bewaartermijnen die deze belangen in acht nemen. En deze ook zorgvuldig moet omschrijven. Stem deze plannen af met eventuele vereisten voor toestemming.

In paragraaf 2.3 tref je een aanbeveling aan (schema 4) voor de bewaartermijnen per documenttype. Controleer altijd het bewaar- en vernietigingsbeleid van je eigen instelling.

☐ **Houd je aan beleid en volg trainingen**

Vaak hebben instellingen beleid voor gegevensbescherming, al dan niet toegespitst op onderzoek. Raadpleeg deze en houd je hieraan. Volg ook (verplichte of facultatieve) trainingen op dit vlak.

☐ **Meld datalekken met persoonsgegevens**

Vermoed je dat sprake is van een datalek van de gegevens van je onderzoek, bijvoorbeeld doordat iemand ten onrechte toegang heeft (gehad) tot persoonsgegevens of omdat deze per ongeluk zijn verwijderd, meld het (vermoedelijke) datalek dan direct volgens de datalekprocedure die binnen jouw instelling geldt.

☐ **Kijk of je gegevens kunt anonimiseren of pseudonimiseren.** Aangezien dit een uitgebreid onderwerp is, komt dit hieronder separaat aan bod.

3.2 De documentstructuur aanpassen

Een aantal concrete manieren om de bestands- en mapnamen te kiezen.

1. Vermijd persoonlijke informatie:

Gebruik geen namen, burgerservicenummers (!), e-mailadressen of andere direct herleidbare gegevens in de bestands- of mapnamen. Voorbeeld:

- a. Niet: "JanJansen_Interview01.docx"
- b. Wel: "Respondent01_Interview.docx"

2. Gebruik neutrale codes:

Werk met unieke, niet-herleidbare codes voor je documenten. Voorbeeld:

"R01_Transcript.docx", waarbij "R01" verwijst naar een respondent in je database.

3. Documenteer je structuur: maak een apart document met daarin de betekenis van de gebruikte codes en structuren van je bestanden en mappen. Sla dit bestand veilig en apart van de data op.

4. Beperk toegang: zorg dat alleen noodzakelijke personen toegang hebben tot de documentatie die de codes verklaart, zoals een coderingsleutel.

5. Check bestandsnamen voorafgaand aan data publicatie: in het kader van Open Science en FAIR data wil je misschien je dataset publiceren na afloop van het onderzoek. Controleer de bestands- en mapnamen van de items voordat je publiceert, zodat deze geen herleidbare informatie bevatten.

Het nadenken over je documentenstructuur helpt je om overzichtelijker en eenvoudiger te werken tijdens je onderzoek. Tegelijkertijd helpt het om de gevolgen van een eventueel datalek te beperken.

Heb je vragen over het inrichten van je bestandsnamen en mappenstructuur? Neem contact op met de datasteward of andere onderzoekondersteuner van jouw instelling.

3.3 Bewaartermijnen van jouw onderzoeksgegevens

Aanbeveling aan voor de bewaartermijnen per documenttype. Controleer altijd het bewaar- en vernietigingsbeleid van je eigen instelling.

Document	Voorbeeld	Aanbevolen bewaartermijn	Toelichting
Toestemmings-formulieren	Ondertekend toestemmingsformulier (kan ook samen met een formulier voor ethische toestemming).	Minimaal zolang de persoonsgegevens worden gebruikt of gedeeld, of nog nodig zijn. Check hiervoor het beleid van je organisatie.	Verplicht om toestemming te kunnen aantonen zolang persoonsgegevens worden verwerkt. Alleen van toepassing als je op basis van de grondslag 'toestemming' werkt
Opnames (audio/video)	Interviews of focusgroepen	Zo kort mogelijk; vernietig bijvoorbeeld na transcriptie of analyse (als de gegevens niet meer nodig zijn)	Beperk de opslag van gevoelige persoonsgegevens door deze snel te verwerken en te pseudonimiseren waar mogelijk.
Transcripties/vragenlijsten	Schriftelijk uitgeschreven interviews of ingevulde enquêtes	Bewaartermijn afhankelijk van doel. bij voorkeur maximaal 10 jaar.	Houd rekening met het beleid van je instelling, de Nationale Gedragscode Wetenschappelijke Integriteit en de subsidiegever. Voor het medisch domein kunnen afwijkende

Document	Voorbeeld	Aanbevolen bewaartermijn	Toelichting
			bewaartermijnen gelden.
Metadata/analysebestanden	Gecodeerde gegevens voor analyses	Kan langer bewaard worden (bijvoorbeeld 10+ jaar), mits geanonimiseerd.	Voor hergebruik en replicatieonderzoek zijn geanonimiseerde datasets vaak langer nodig. Bij voorkeur verwijder je de dataset en bewaar je de syntax voor de reproduceerbaarheid.
Overige documenten	Projectdocumentatie	Bewaartermijn zoals voorgeschreven door beleid instelling.	Controleer institutionele eisen en andere relevante regelgeving.

Schema 4: richtlijn bewaartermijnen per document.

Heb je vragen over bewaartermijnen van jouw onderzoeksgegevens? Neem contact op met de datasteward of andere onderzoekondersteuner van jouw instelling.

3.4 Pseudonimiseren en anonimiseren

Het onderscheid tussen pseudonimiseren en anonimiseren vinden veel mensen lastig te maken. Om dit goed te kunnen maken, moet je vaststellen of het proces onomkeerbaar is of niet. Eenvoudig gesteld:

Pseudonimiseren is meestal omkeerbaar¹⁶ - Bij de beveiligingsmaatregel pseudonimiseren kunnen persoonsgegevens niet direct aan een individu worden gekoppeld zonder te beschikken over aanvullende informatie (sleutel). De sleutel wordt apart en beveiligd opgeslagen. De AVG blijft wel van toepassing. Als je geen direct herleidbare persoonsgegevens nodig hebt, zorg dan standaard voor pseudonimering. Kies bewust of je terug moet kunnen naar het persoonsgegeven (bijvoorbeeld als een hoog risico op borstkanker wordt geconstateerd bij een deelnemer)

Anonimiseren is onomkeerbaar - Het volledig anonimiseren van persoonsgegevens houdt in dat individuen niet meer identificeerbaar zijn, ook niet met aanvullende informatie. Dit is onomkeerbaar. De AVG is dan niet meer van toepassing. Je spreekt dan van gegevens en niet meer van persoonsgegevens. Houd er rekening mee dat voor het tijdelijk in bezit hebben van persoonsgegevens die voor anonimisering bestemd zijn, nog steeds een verwerkingsgrondslag en adequate bescherming nodig is.

¹⁶ De guidelines van de EDBP: [edpb_guidelines_202501_pseudonymisation_en.pdf](#).

⚠ Echt anonimiseren is erg moeilijk. Een anonieme dataset kan, o.a. gelet op voorschrijdende techniek, die anonimiteit verliezen. De AVG is dan (opnieuw) van toepassing. Vraag altijd hulp bij je privacy-contactpersoon.

Samengevat:

Pseudonimiseren is iets anders dan anonimiseren. De gepseudonimiseerde persoonsgegevens kunnen immers worden gecombineerd met de sleutel of met andere datasets, waarbij personen alsnog kunnen worden geïdentificeerd. Dat maakt dat de AVG nog altijd toepasbaar is op gepseudonimiseerde gegevens. Pseudonimiseren is onder bepaalde voorwaarden soms beter dan anonimiseren.

Een effectieve methode van anonimisering zorgt ervoor dat voor alle partijen de mogelijkheid is uitgesloten om:

1. Een persoon te individualiseren ('single out');
2. Verschillende records in verband te brengen met een individu ('linkability');
3. Informatie over een individu af te leiden ('inference').

Gegevens zijn pas anoniem als het 'redelijkerwijs' onmogelijk is personen te identificeren, rekening houdend met beperkingen in kosten en tijd, en met de huidige technologie en toekomstige technologische ontwikkelingen.¹⁷ Anders gezegd: als identificatie in praktijk ondoenlijk is doordat herleidbaarheid een excessieve inspanning qua tijd, mankracht of middelen kost.

Bovenstaande laat enige ruimte over voor discussie over wat onder 'redelijkerwijs' wordt verstaan. In de handreiking wordt daarom niet aangegeven wanneer er concreet wel of niet sprake is van anonieme gegevens. Wel vind je hieronder praktische tips over wat je kunt doen om gegevens te anonimiseren of pseudonimiseren.

Het heeft de voorkeur persoonsgegevens waar mogelijk te anonimiseren.

Als anonimiseren niet mogelijk is of de bruikbaarheid van de persoonsgegevens te veel beïnvloedt, kun je overwegen om gegevens te pseudonimiseren. Bedenk ook dat een andere, derde partij de pseudonimisatie niet zomaar ongedaan kan maken (zonder sleutel).

¹⁷ Punt 26 van de considerans van de AVG.

Wanneer je pseudonimisering overweegt, moet je telkens rekening houden met de volgende factoren:

- de stand van de techniek (schaalbaar, bestand tegen aanvallen) en de kosten van de implementatie van eventuele maatregelen. ;
- de aard, omvang, context en het/de doel(en) van jouw verwerking. Dit beïnvloedt het type pseudonimisering; en
- de risico's die jouw verwerking met zich meebrengt voor de rechten en vrijheden van de onderzoeksdeelnemers.

Niet alle pseudonimiseringstechnieken zijn even effectief en ze hebben mogelijk niet dezelfde implementatiekosten of -vereisten. Je moet in dat geval een pseudonimiseringstechniek kiezen door de optimale aanpak te vinden voor gegevensbescherming door ontwerp (privacy by design) en beveiliging.

Heb je vragen over het pseudonimiseren of anonimiseren van je onderzoeksgegevens? Neem contact op met de privacy-contactpersoon van jouw instelling.

Stappen om te anonimiseren

- ☐ Verwijder direct herleidbare gegevens (naam, geboortedatum, postcode, etc.).
- ☐ Verwijder unieke kenmerken uit de dataset.
- ☐ Pas aggregatie toe:
 - Combineer gegevens in bredere categorieën, zoals leeftijdsgroepen ("20-29 jaar") in plaats van exacte leeftijden.
 - Voeg kleine wijzigingen toe aan datawaarden, zonder de onderzoeksresultaten te beïnvloeden.
 - Introduceer ruis.¹⁸
- ☐ Controleer herleidbaarheid.
- ☐ Test of de dataset echt niet meer te herleiden is tot individuen, ook niet in combinatie met andere datasets. Er bestaan hiervoor verschillende tools.

Belangrijke aandachtspunten:

- Vaak gaat op: hoe kleiner het aantal deelnemers, hoe moeilijker je de set kunt anonimiseren.
- In de praktijk is eerder sprake van pseudonimisering dan van anonimisering. Vraag jezelf af of individuen toch echt niet te achterhalen zijn na het doorlopen van de verschillende stappen. Onderzoek naar specifieke onderzoekspopulaties, bijvoorbeeld participanten met weinig

¹⁸ Voor meer informatie over dit soort technieken, zie:

- [Privacyontwerpstategieën \(Het Blauwe Boekje\)](#) ⁷ van Jaap-Henk Hoepman.
- Het [anonimisatieprotocol](#) ⁷ van Radboud University.
- De guidelines van de EDBP: [edpb_guidelines_202501_pseudonymisation_en.pdf](#) ⁷.
- Universiteit Gent geeft [concrete voorbeelden voor het pseudonimiseren](#) ⁷.

voorkomende kenmerken (dat kan ook een deelnemer met een weinig voorkomende functie zijn) of patiëntgroepen met zeldzame aandoeningen zijn moeilijk te anonimiseren.

- Het anonimiseren kan de bruikbaarheid van je onderzoeksinformatie beperken. Beoordeel per onderzoeksproject/onderzoeksvraag opnieuw welke maatregelen passend zijn.
- Documenteer je aanpak.
- Beschrijf hoe je de anonimiseren uitvoert in je DMP.
- Als anonimiseren niet mogelijk is of de bruikbaarheid van de persoonsgegevens te veel beïnvloedt, kun je overwegen om gegevens te pseudonimiseren.

Stappen om te pseudonimiseren:

- ☐ Vervang identiteitsgegevens: wissel direct herleidbare informatie (zoals namen, adressen of e-mailadressen) in voor een unieke code, zoals een nummer of pseudoniem. Veelvoorkomende andere manieren van pseudonimiseren zijn:
 - hashing;
 - encryptie;
 - tokenisatie.
- ☐ Opsplitsen gegevens en sleutel: sla de gepseudonimiseerde gegevens en de sleutel op twee verschillende omgevingen op. Zorg ervoor dat de sleutel wordt opgeslagen in een goed beveiligde omgeving, zoals een versleutelde database.
- ☐ Beperk toegang: zorg ervoor dat slechts een beperkt aantal personen toegang hebben tot zowel de gegevens als de sleutel.
- ☐ Documenteer je aanpak: beschrijf je aanpak van pseudonimiseren in het DMP.

Stap 4: Analyse & Delen

Bij de eerdere stappen van het onderzoek heb je nagedacht over een zorgvuldige inrichting en verzameling van persoonsgegevens. Misschien heb je al gegevens gedeeld met andere partijen en hierover afspraken gemaakt.

In deze fase van het onderzoek is het van belang dat je veilig met deze gegevens blijft werken. Bekijk hiervoor de vragen en tips in paragraaf 4.1 t/m 4.4.

4.1 Hoe kan ik veilig met persoonsgegevens blijven werken bij wijzigingen?

Gaandeweg het onderzoek kom je er misschien achter dat je meer gegevens nodig hebt of dat de context van je onderzoek wijzigt.

Check bij wijzigingen altijd of de maatregelen nog steeds voldoende zijn.

Tips

- ☐ Zodra er meer (interne) medewerkers bij jouw onderzoek betrokken worden, ga dan goed na of toegang tot persoonsgegevens noodzakelijk is, of dat je kan volstaan met toegang tot een deel van de persoonsgegevens of zelfs anonieme gegevens. En regel de toegang tot deze gegevens goed in en pas dit zo nodig aan in de autorisatiematrix.
- ☐ Heeft een medewerker geen toegang tot persoonsgegevens meer nodig, beperk dan de toegang tot deze gegevens.
- ☐ Betrek je nieuwe partijen bij jouw onderzoek, maak dan ook met hen de juiste afspraken via de bijpassende overeenkomsten (stap 1.3).

- ☐ Heb je meer data nodig voor jouw onderzoek en betreffen dit meer of andere persoonsgegevens:
 - wees kritisch op of de gegevens voldoen aan het vereiste van dataminimalisatie;
 - geef de wijziging aan in het verwerkingsregister en DMP;
 - pas waar nodig de informatiebrief/het toestemmingsformulier hierop aan;
 - ga na of de impact voor de onderzoeksdeelnemers wijzigt en je een uitgevoerde DPIA moet updaten of (alsnog) een DPIA moet uitvoeren;
 - onderzoek of aanpassing van de gesloten overeenkomsten nodig is (zodat deze kloppen én zodat je kunt onderzoeken of de gemaakte afspraken, waaronder beveiligingsmaatregelen, nog voldoende zijn).

4.2 Kan ik al persoonsgegevens verwijderen?

Volgens de AVG moet je persoonsgegevens verwijderen als je ze niet meer nodig hebt. Ga na of je in deze fase al persoonsgegevens kunt verwijderen zonder dat dit het doel en integriteit van jouw onderzoek schaadt.

Je kunt persoonsgegevens bijvoorbeeld verwijderen als:

- de gegevens zijn verwerkt;
- je opnames hebt gemaakt of andere persoonsgegevens hebt verzameld, kun je deze gegevens mogelijk wissen na verwerking. Je kunt bijvoorbeeld de oorspronkelijke opnames wissen zodra je transcripties hebt gemaakt van interviewopnames, als dat verder geen problemen oplevert voor het aantonen van de onderzoeksintegriteit.
- de persoonsgegevens niet noodzakelijk zijn voor jouw onderzoek. Dat geldt bijvoorbeeld voor persoonsgegevens die onderzoeksdeelnemers hebben verstrekt zonder dat daarom is gevraagd of waarvan je achteraf beoordeelt dat ze niet relevant zijn).

Tips veilig verwijderen

- ☐ Neem in jouw informatiebrief/toestemmingsformulier op hoe jij omgaat met het bewaren/verwijderen van persoonsgegevens.
- ☐ Zorg ervoor dat je gegevens zo verwijdert dat dit onherstelbaar is. Mogelijk kun je software gebruiken of kan de interne servicedesk je helpen dit veilig te doen. Check ook eventueel de digitale prullenbakken/verwijderde items.
- ☐ Vernietig papieren op een manier die past binnen jouw instelling (bijvoorbeeld met versnipperaars of speciale bakken die door een hiertoe gecertificeerd bedrijf worden opgehaald en vernietigt).
- ☐ Documenteer het proces: geef in de je DMP aan welke gegevens je gaat wissen, wanneer je dit doet en hoe je dit uitvoert. Dit helpt ook bij een correct antwoord op een eventueel inzageverzoek later.

Het kan noodzakelijk zijn om gegevens voor langere tijd te bewaren, bijvoorbeeld voor ethische goedkeuring of voor het repliceren van resultaten bij publicatie of vervolgonderzoek. Leg deze afweging vast (bijvoorbeeld bij het bepalen van bewaartermijnen) en kijk of je de gegevens gepseudonimiseerd of versleuteld kunt bewaren.

Vragen over het vroegtijdig verwijderen van persoonsgegevens? Neem contact op met de datasteward of privacy-contactpersoon van jouw instelling.

4.3 Kan ik de gegevens anonimiseren of pseudonimiseren in mijn onderzoek?

Als het nog niet mogelijk is de persoonsgegevens te verwijderen, bijvoorbeeld omdat je ze nodig hebt, ga dan na of je in deze fase de gegevens wél kunt anonimiseren. Mocht dat ook niet mogelijk zijn, kijk dan naar mogelijkheden tot pseudonimiseren. Zie stap 2.4.

In jouw onderzoek/paper zelf publiceer je anonieme gegevens, tenzij herleidbare gegevens onoverkomelijk zijn. In dat geval moet je daar al rekening mee houden bij stap 1, Planning & Ontwerp en je informatiebrief/toestemmingsformulier richting de onderzoeksdeelnemers.

4.4 Zijn de beveiligingsmaatregelen die ik heb getroffen nog voldoende passend?

Het kan zijn dat jouw onderzoek is gewijzigd of dat er meer medewerkers of partijen betrokken zijn bij jouw onderzoek. Ook de ontwikkeling op het gebied van de stand van de techniek staat niet stil. Onderzoek of de beveiligingsmaatregelen die je (bij eerdere stappen in jouw onderzoek) hebt getroffen nog voldoende passend zijn. Zie stap 2. Beheer & Opslag.

Twijfels? Raadpleeg dan jouw interne contactpersoon (datasteward, security officer, CISO etc).

Stap 5: Evalueren & Archiveren

In deze fase van het onderzoek is de verwerking van persoonsgegevens afgerond. Je regelt hier dat je:

- bewaart wat bewaard moet worden;
- verwijdert wat verwijderd of opgeruimd kan worden;
- de resultaten overdraagt aan archiefbeheer.

Tips

- Je instelling heeft waarschijnlijk beleid voor bewaar- en vernietigingstermijnen. Dit beleid moet je volgen. Is er geen beleid, kijk dan naar voorbeelden bij vergelijkbare instellingen of vraag na bij de jurist van je organisatie.
- Controleer of je (persoons)gegevens verder kunt minimaliseren, met twee archiveringsdoelen in gedachten:
 - 1) Selecteer en organiseer de gegevens die nodig zijn om je bevindingen te valideren. Gegevens die belangrijk zijn voor het verifiëren van het onderzoek, moeten worden bewaard.
 - 2) Selecteer en organiseer de gegevens die mogelijk waardevol zijn voor verder onderzoek door jou, je team of collega-onderzoekers.
- Bespreek het beëindigen van het project binnen het team en met samenwerkingspartners.
- Verwijder kopieën van gegevens uit secundaire locaties (bijvoorbeeld het platform waarmee gegevens verzameld zijn, laptop, SURFdrive, enz.).
- Bekijk hoe je de toegang tot projectmappen en dergelijke beheert. Denk bijvoorbeeld aan het verwijderen van toegang na afloop waar mogelijk, bijvoorbeeld voor externen of onderzoekers die zelf geen toegang meer nodig hebben tot de data na afronding.
- Als je niet van plan bent om de gegevens nog te gebruiken voor toekomstige projecten, overweeg dan om ze na archivering ook uit je werkomgeving te verwijderen.
- Als je nog steeds met de gegevens werkt, overweeg dan om je werkdirectory op te ruimen.
- Verwijder alle tijdelijke werkbestanden (bijvoorbeeld gegevens die gemakkelijk opnieuw kunnen worden gegenereerd door gearchiveerde scripts).
- Verwijder dubbele of verouderde versies (bijv. final_v1.csv, final_v2.csv, enz.).

Stap 6: Publiceren

Als je letterlijke quotes wilt gebruiken in een publicatie van je onderzoek, is het aan te raden om dit vooraf af te stemmen met degene van wie de quote is.

Opties voor de publicatie:

1. Geanonimiseerde publicatie in een publieke repository¹⁹.
2. Publicatie met toegangsrestricties waarin persoonsgegevens niet-herleidbaar zijn gemaakt of zijn gemaskeerd (controleer altijd welke procedure hiervoor geldt en of dit past bij de gegeven toestemming en de gemaakte afspraken - overleg met je privacyteam).
3. Alleen metadata en materialen die zijn gebruikt voor het uitvoeren van het onderzoek (zoals vragenlijsten, codeboeken, scripts, etc.).

 Let op: als je de gebruikte set onderzoeksdata open beschikbaar wilt stellen, zorg er dan voor dat die set écht volledig geanonimiseerd is.

¹⁹ Bekijk ook de informatie over [FAIR data](#)²⁰ (Wikipedia) en het publiceren volgens het principe 'As open as possible and as closed as necessary'.

Bijlage 1 - Datamanagementplan

- [Uniform DMP voor onderzoek⁷](#) - DCC-PO (NL en ENG)

Bijlage 2 – Toestemmingsformulier

Controleer bij je privacy-contactpersoon of je organisatie een template heeft voor het vragen van toestemming en het intrekken van toestemming.

Zie [Grondslag toestemming](#)⁷ (Autoriteit Persoonsgegevens) voor uitleg over deze grondslag en de manier waarop je toestemming kunt vragen.

 Let op dat je een toestemmingsformulier later niet zomaar hergebruikt. Controleer altijd of het formulier dat je wilt gebruiken daadwerkelijk passend is bij de situatie.

Bijlage 3 - Begrippenlijst

Zie het [privacywoordenboek van de AP](#)⁷ voor een heldere uitleg van allerlei privacybegrippen. Onderstaande begrippen ter aanvulling:

Begrip	Toelichting
EER	Bij de Europese Economische Ruimte (EER) horen alle EU-landen plus Liechtenstein, Noorwegen en IJsland.
Persoonsgegevens	Bij persoonsgegevens gaat het om informatie die ofwel direct over iemand gaat, ofwel indirect naar deze persoon te herleiden is, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens. Bijvoorbeeld door meerdere persoonsgegevens met elkaar te combineren.
Bijzondere (categorieën van) persoonsgegevens	Bijzondere persoonsgegevens⁷ zijn gegevens die zo privacygevoelig zijn dat het een grote(re) impact op iemand kan hebben als een organisatie deze gegevens verwerkt. Bijvoorbeeld gegevens over iemands gezondheid of politieke voorkeur. Daarom krijgen bijzondere persoonsgegevens extra bescherming in de AVG (zoals gegevens waaruit iemands ras of etnische afkomst, politieke opvattingen blijken, gegevens over iemands gezondheid, seksueel gedrag). In dit document vallen de bijzondere persoonsgegevens binnen de term 'gevoelige gegevens' omdat ook er ook gevoelige gegevens zijn die niet in de categorie bijzondere persoonsgegevens vallen, maar die ook extra bescherming nodig hebben. ⚠ Let op, het verwerken van bijzondere persoonsgegevens is verboden tenzij er een uitzondering van toepassing is. Vraag je privacy-contactpersoon wat je moet doen. ⚠ Strafrechtelijke gegevens vallen niet onder deze definitie.
Metadata	Informatie die iets zeggen over andere gegevens, zoals aanmaakdatum, auteur, onderwerp, grootte, etc.
Onderzoeksdeelnemers	Alle personen van wie je persoonsgegevens verwerkt voor jouw onderzoek (ook als het onderzoek niet over die deelnemers zelf gaat).

Begrip	Toelichting
Primair gebruik persoonsgegevens	Primair gebruik is wanneer je binnen het onderzoek persoonsgegevens rechtstreeks van de betrokkenen verzamelt met een specifieke doelstelling voor ogen.
Secundair gebruik persoonsgegevens	Secundair gebruik is wanneer je of de persoonsgegevens van een (bestaande) dataset niet rechtstreeks bij de betrokkenen verzamelt of wanneer ze in eerste instantie voor een ander doel of onderzoek zijn verzameld dan jouw huidige onderzoeksproject zijn verzameld. In deze handreiking spreken we van hergebruik.
Wetenschappelijk onderzoek (in het kader van deze handreiking)	• Onderzoek waarin persoonsgegevens worden verwerkt. • Relevante sectorale normen voor methodologie en ethiek zijn van toepassing, waaronder het begrip geïnformeerde toestemming, verantwoordingsplicht en toezicht. • Het onderzoek wordt uitgevoerd met als doel de collectieve kennis en het welzijn van de samenleving te vergroten, in plaats van primair één of meerdere particuliere belangen te dienen.

Bijlage 4 – Beslisboom roloverdeling en af te sluiten overeenkomst



Bijlage 5 – Checklist voor de onderzoeker

De checklist past bij de benadering volgens de Data Lifecycle van Harvard (zie hoofdstuk 2 en 3).

Check	Stappen	Lifecycle-stap	Handreiking
☐	Ik heb gecontroleerd of de AVG van toepassing is op mijn onderzoek.	Stap 1 Planning & Ontwerp	Pagina 12
☐	Ik heb afspraken over gegevensgebruik met andere partijen in de juiste overeenkomsten vastgelegd.	Stap 1 Planning & Ontwerp	Pagina 14
☐	Ik heb nagedacht over hergebruik van de gegevens uit mijn onderzoek en hiervoor maatregelen getroffen.	Stap 1 Planning & Ontwerp	Pagina 22
☐	Ik heb onderzocht of ik een DPIA moest verrichten en heb maatregelen getroffen om gegevens passend te beschermen.	Stap 1 Planning & Ontwerp	Pagina 23
☐	Ik heb een datamanagementplan (DMP) opgesteld waarin ik keuzes op het gebied van gegevensbescherming heb toegelicht.	Stap 1 Planning & Ontwerp	Pagina 24
☐	Ik informeer deelnemers tijdig en op de juiste wijze. De inhoud van mijn informatiebrief komt overeen met het DMP en het verwerkingsregister.	Stap 2 Verzameling & Gebruik	Pagina 26
☐	Ik heb mijn processen zo ingericht dan ik tegemoet kan komen aan de AVG-verzoeken van deelnemers.	Stap 2 Verzameling & Gebruik	Pagina 30
☐	Ik heb mijn onderzoek aangemeld in het verwerkingsregister.	Stap 2 Verzameling & Gebruik	Pagina 31
☐	Ik ga bij iedere stap in mijn onderzoek na of de getroffen maatregelen nog passend zijn.	Alle stappen	Pagina 32, 38 en 40
☐	Ik heb de passende beschermingsmaatregelen genomen, ik heb waar mogelijk geanonimiseerd of gepseudonimiseerd en de bewaartermijnen vastgesteld en gezorgd voor de juiste locatie voor langdurige opslag.	Stap 3 Collect & Create	Pagina's 34/35
☐	Ik heb gecontroleerd of ik nog veilig werk en heb gegevens waar mogelijk verwijderd, geanonimiseerd of gepseudonimiseerd dan wel de bewaartermijnen nageleefd en gezorgd voor de juiste locatie voor langdurige opslag.	Stap 4 Analyse & delen	Pagina 38/40
☐	Ik ga bij iedere stap in mijn onderzoek na of de getroffen maatregelen nog passend zijn.	Alle stappen	Pagina 32, 38 en 40