Themabeleid Privacy & Bescherming Persoonsgegevens

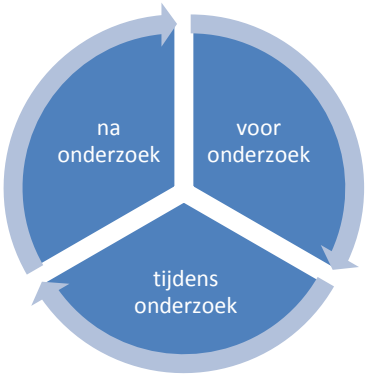
Wetenschappelijk Onderzoek – Gebruik Persoonsgegevens

Leeswijzer

Dit themabeleid wetenschappelijk onderzoek is onderdeel van het Beleid Privacy en Bescherming Persoonsgegevens en beschrijft voor wetenschappelijk onderzoek de wijze waarop Tilburg University de Algemene Verordening Gegevensbescherming (AVG) implementeert inzake de bescherming van de Persoonsgegevens.

De richtlijnen zoals opgenomen in dit beleid zijn alleen van toepassing indien er in een wetenschappelijk onderzoek gewerkt wordt met Persoonsgegevens (gegevens die nu of in de toekomst te herleiden zijn naar een natuurlijk persoon).
Indien er geen Persoonsgegevens worden verwerkt of indien deze bij het verkrijgen al volledig Geanonimiseerd zijn (en daarmee nooit te herleiden naar persoon) dan is deze richtlijn niet van toepassing. **Let op**! Het Anonimiseren van Persoonsgegevens is wél een Verwerking waarop de richtlijn van toepassiing is.

Voor de leesbaarheid hebben we dit beleid onderverdeeld in drie fases gebaseerd op de verschillende fases van onderzoek doen:



Alle informatie met betrekking tot de Europese wetgeving (AVG) en de Bescherming van Persoonsgegevens is opgenomen op een TiU website[1] waaronder ook Frequently Asked Questions. Op deze website zijn ook praktische uitwerkingen en voorbeelden te vinden.

In het beleid zijn verwijzigingen opgenomen naar andere beleidsstukken. Deze zijn gemarkeerd als '**verwijzing'.** De richtlijnen die van toepassing zijn, zijn weergegeven in blokken, om ze eenvoudig vindbaar te maken:

Onderwerp	Regels en richtlijnen waaraan Onderzoek dient te voldoen op het gebied van Bescherming Persoonsgegevens.

In dit beleid zijn veel definities opgenomen (zie **bijlage 2**). De termen die in de definitielijst staan zijn Onderlijnd.

In onderzoek worden normaliter meer data verzameld dan enkel Persoonsgegevens. Dit beleid gaat echter voornamelijk in op juridische aspecten die betrekking hebben op Persoonsgegevens.

Elke school/divisie binnen TiU heeft zogenaamde Data Representatives[2] aangesteld. Zij zijn eerste aanspreekpunt voor medewerkers in geval van vragen over de Bescherming van Persoonsgegevens. Voor vragen over datamanagement, data-opslag en data-archivering waarbij

[1] https://www.tilburguniversity.edu/nl/intranet/ondersteuning-werk/juridisch/privacy/avg/
[2] https://www.tilburguniversity.edu/nl/intranet/ondersteuning-werk/juridisch/privacy/avg/contact/

al dan niet Persoonsgegevens wordt verwerkt kan de onderzoeker terecht bij het Research Data Office (RDO). Voor meer detail verwijzen we naar de **Regeling Onderzoeksdatamanagement**.

Dit beleid bevat algemene handvatten aan onderzoekers. Het rechtmatig gebruik van Persoonsgegevens in wetenschappelijk onderzoek is echter **afhankelijk van de feiten en omstandigheden per geval**. De onderzoeker dient dan ook per geval een afweging te maken of de verwerking voldoet aan dit beleid, het algemene Beleid Privacy en Bescherming Persoonsgegevens van TiU en de toepasselijke wetgeving en blijft daarvoor verantwoordelijk.

Ten tijde van de totstandkoming van dit beleid was de nieuwe Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek van de VSNU nog in ontwikkeling, waardoor deze nieuwe versie niet is meegenomen bij de totstandkoming van dit beleid. Op het moment dat de Gedragscode definitief wordt vastgesteld zal dit beleid geëvalueerd worden en in lijn gebracht worden met de Gedragscode. Daarnaast worden door de Europese Unie naar verwachting ook nog aanvullende regelingen (bijvoorbeeld in de vorm van adviezen van WP29) uitgebracht die mogelijk invloed hebben op de inhoud van deze richtlijn.
Voorts zal de praktijk moeten uitwijzen op welke onderzoeksdisciplines nog verdere invulling gegeven zal moeten worden aan dit beleid.

Het beleid zal dan ook in ieder geval jaarlijks worden geëvalueerd en herzien, tenzij op basis van gewijzigde wet en regelgeving of gewijzigde beleidsstandpunten eerdere herziening noodzakelijk is.

Wanneer in dit beleid wordt gesproken over hij, wordt hieronder verstaan hij/zij of personen die zich niet identificeren met een mannelijk danwel vrouwelijk geslacht.

Inhoudsopgave

Stroomschema

In ontwikkeling, nog in te voeren

1. Inleiding

Deze richtlijn is **alleen van toepassing indien in Wetenschappelijk Onderzoek Persoonsgegevens worden verwerkt**. Indien er geen Persoonsgegevens worden verwerkt dan is deze richtlijn niet van toepassing.

Een Persoonsgegeven is

---

alle informatie die een natuurlijk persoon kan identificeren dan wel die informatie die nu of in de toekomst naar deze persoon te herleiden is.

Deze definitie van Persoonsgegevens is gebaseerd op de AVG en zeer ruim.

Er is een verschil met Pseudonimiseren. Bij Pseudonimisering worden identificerende gegevens gescheiden van niet-identificerende gegevens en vervangen door kunstmatige identificatoren. Een voorbeeld van Pseudonimisering is het vervangen van de gegevens van een respondent in een onderzoek door een uniek respondentennummer. De medische gegevens worden dan gekoppeld aan dit respondentennummer in plaats van aan NAW-gegevens. Hierdoor is voor buitenstaanders niet zichtbaar wie de persoon is waaraan de medische gegevens toebehoren. Alleen degene die de koppeling kan maken tussen respondentennummer (bijv. onderzoeker) is in staat om de medische gegevens te koppelen. Er dienen dan wel voldoende (organisatorische en technische) maatregelen genomen te worden zodat onbevoegden deze bestanden niet kunnen koppelen. In geval van Pseudonimisering is de AVG en daarmee deze richtlijn wel van toepassing.

Voor Anonieme gegevens is de AVG niet langer van toepassing. Houdt wel rekening met het feit dat bij Anonieme gegevens er geen enkele mogelijkheid meer is voor identificatie of herleiden tot personen. Het Anonimiseren is een verwerkingshandeling en valt wel nog onder de AVG. Indien gegevens toch nog te herleiden zijn tot een persoon is er geen sprake van Anonimisering.

Indien gegevens te herleiden zijn naar Personen dan spreken we over Persoonsgegevens. Dit kan derhalve zowel direct herleidbare Persoonsgegevens (zoals naam, email) of indirect herleidbare Persoonsgegevens zijn (zoals bijvoorbeeld kenteken of een combinatie van initialen en postcode en huisnummer)

In wetenschappelijk onderzoek wordt veel met Respondenten gewerkt. Tilburg University (TiU) hecht veel waarde aan het zorgvuldig verwerken van Persoonsgegevens in het kader van wetenschappelijk onderzoek omdat misbruik van gegevens grote schade kan berokkenen aan Respondenten, medewerkers, studenten en Tilburg University. Daarbij wordt een goede balans gezocht tussen privacy, veiligheid en functionaliteit.

Dit Beleid is van toepassing op alle Verwerkingen van Persoonsgegevens die plaatsvinden in het kader van Wetenschappelijk Onderzoek onder verantwoordelijkheid van Tilburg University en geldt voor iedereen die werkzaam is onder verantwoordelijkheid van Tilburg University.

Onder Verwerking wordt verstaan het verwerken van Persoonsgegevens, al dan niet geautomatiseerd, zoals verzamelen, vastleggen, structureren, opslaan, wijzigen, analyseren, opvragen, raadplegen, gebruiken, verstrekken (doorsturen), verspreiden, ter beschikking stellen, combineren, afschermen of vernietigen van gegevens. Met andere woorden alles wat je doet met Persoonsgegevens.

Het betreft Verwerkingen van Persoonsgegevens in een papieren dossier of archief, digitaal bestand of in een applicatie / systeem (waaronder in mailboxen en op computers of andere gegevensdragers zoals usb-sticks) en het Beleid is van toepassing **op alle Personeel (ook Personeel Niet in Loondienst) inclusief student-assistenten, uitzendkrachten of ingehuurd personeel en stagiaires, (buiten)promovendi en studenten die een bijdrage leveren aan het onderzoek**. Het betreft dus alle verwerkingen van Persoonsgegevens die onderzoekers uitvoeren in het kader van wetenschappelijk onderzoek.

In de AVG wordt gesproken over Betrokkene of datasubject, dit betreft in wetenschappelijk onderzoek voornamelijk Respondenten (ook wel proefpersonen of deelnemers genoemd). De term Respondenten zal derhalve in het vervolg gebruikt worden.

De aspecten van wetenschappelijk onderzoek die relevant zijn voor Persoonsgegevens kunnen weergegeven worden in drie fasen: voor, tijdens en na afronding van het onderzoek. Deze drie fasen hebben hun eigen aandachtspunten als het gaat om bescherming van Persoonsgegevens waarmee de onderzoeker rekening moet houden.

Een onderzoek wordt uitgevoerd onder leiding van een onderzoeker. Hij is verantwoordelijk voor de naleving van dit beleid en dient te waarborgen dat iedereen die onder zijn verantwoordelijkheid meewerkt aan het onderzoek (bijv. (buiten)promovendi, student-assistenten en studenten) zich houdt aan dit beleid inzake bescherming Persoonsgegevens.

Verantwoordelijk	Voor onderzoek zijn er verschillende vormen van verantwoordelijkheid. :
	• De **onderzoeker** is zelf verantwoordelijk voor, gebruik makend van de voorzieningen die Tilburg University aanbiedt:
	  ○ Voor het naleven van het **Beleid Privacy & Bescherming Persoonsgegevens** (inclusief dit Themabeleid) van de universiteit en daarmee de AVG alsmede de **Regeling Onderzoeksdatamanagement**.
	  ○ Voor een goed datamanagement en dataopslag in overeenstemming met de uitgangspunten in de **Regeling Onderzoeksdatamanagement.**
	  ○ Voor het maken van een Datamanagementplan voorafgaand aan een nieuwe onderzoek conform het facultair datamanagement beleid en

	○ Waarborgen dat promovendi en studenten (die onder verantwoordelijkheid van Onderzoeker werkzaamheden verrichten) de Regelingen en het Beleid zoals hierboven vermeld naleven. • De **decaan** van de betreffende faculteit is verantwoordelijk voor: ○ De implementatie van het **Beleid Privacy & Bescherming Persoonsgegevens** met betrekking tot wetenschappelijk onderzoek binnen de faculteit (eventueel aan de hand van facultair beleid) ○ Het voorlichten van het wetenschappelijk personeel over dit beleid ○ Het toezicht houden op de naleving dan dit beleid en hierover verantwoording afleggen aan het College van Bestuur. • Het **College van Bestuur** verantwoordelijk voor: ○ Het opstellen van een algemeen universiteit beleidskader zoals vastgelegd in het **Beleid Privacy & Bescherming Persoonsgegevens**. ○ Het bieden van flankerende kennis, advies en begeleiding bij Verwerking Persoonsgegevens ○ Het bieden van een adequate infrastructuur voor dataopslag en beheer. ○ Het uitvoeren van audits respectievelijk te begeleiden.

2. Algemene richtlijnen

De in dit hoofdstuk genoemde richtlijnen zijn algemene richtlijnen die niet specifiek van toepassing zijn op één van de fases van het wetenschappelijk onderzoek en betreffen:

- Gebruik van datasets (**paragraaf 2.1**)
- Rechtmatigheid – Verwerkingsgrondslag (**paragraaf 2.2**)
- Rechtmatigheid – Bijzondere Persoonsgegevens (**paragraaf 2.3**)
- Doelbinding (**paragraaf 2.4**)
- Regeling Onderzoeksdatamanagement (**paragraaf 2.5)**
- Ethische commissie (**paragraaf 2.6**)
- Informed consent (**paragraaf 2.7**)
- Internationale onderzoeken (**paragraaf 2.8**)
- Intrekken van Toestemming (**paragraaf 2.9**)
- Rechten van Betrokkenen (**paragraaf 2.10**).

2.1. Gebruik van datasets

Voorafgaand aan de start van een onderzoekproject besluit de betrokken onderzoeker of hij zelf data verzamelt dan wel gebruik maakt van bestaande datasets of een combinatie daarvan. Dit proces verloopt simultaan met de aanvraag voor de ethische toetsing (indien van toepassing).

Bij wetenschappelijk onderzoek wordt er vaak gebruikt gemaakt van papieren of digitale datasets waarin ook Herleidbare Persoonsgegevens voorkomen. Het kan hierbij gaan om:

- Opzetten van nieuwe dataset met Respondenten (**paragraaf 2.1.1**)

- Hergebruik van reeds verzamelde datasets (secundair gebruik) (**paragraaf 2.1.2**)

Daarnaast zijn er specifieke richtlijnen bij gebruik van openbare datasets en in geval van webscraping waarmee Persoonsgegevens verzameld worden.

- Gebruik van openbare datasets (**paragraaf 2.1.3**)
- Dataset op basis van webscraping (**paragraaf 2.1.4**).

2.1.1. Opzetten nieuwe dataset met Respondenten

Bij een wetenschappelijk onderzoek kun je een nieuwe dataset opstellen door gegevens te verzamelen bij Respondenten dan wel door dat twee bestaande (al dan niet openbare) datasets worden gecombineerd. Een dataset kan de vorm hebben van een bestand, maar ook andere vormen zoals video en audio opnames, interviews, scoreformulieren, eye-tracking etc vallen onder deze definitie. Deze Respondenten kunnen zelf geworven worden bijvoorbeeld door een oproep voor deelname of uit een proefpersonenpool.

Respondenten	Voor Respondenten geldt dat dat het belangrijk is dat zij vrijwillig deelnemen en dat zij **vooraf goed geïnformeerd** zijn over het onderzoek o.a. met betrekking tot Bescherming Persoonsgegevens. Dit moet plaatsvinden door een Informed consent formulier. (**paragraaf 2.7 en 3.1**). Indien Verwerkingsgrondslag toestemming is of er Bijzondere Persoonsgegevens worden verwerkt gelden er aanvullende vereisten. (**paragraaf 2.3**)
Dataminimalisatie	Indien herleidbare Persoonsgegevens noodzakelijk zijn voor wetenschappelijk onderzoek: • De onderzoeker mag **alleen Persoonsgegevens die noodzakelijk zijn voor het doel van het wetenschappelijk onderzoek verzamelen (zo weinig mogelijk),** maar waarborgt wel dat er voldoende gegevens verzameld worden om de vraagstelling van het onderzoek te kunnen beantwoorden. Zie **Beleid Privacy & Bescherming Persoonsgegevens hoofdstuk 6**.
Beveiliging	Indien Persoonsgegevens gebruikt worden in onderzoek dan dienen deze adequaat beveiligd Verwerkt te worden. **Beleid Privacy & Bescherming Persoonsgegevens hoofdstuk 9**.
Informatieverplichting	De Respondenten hebben het Recht op Informatie en dienen goed geïnformeerd te worden. Zie **paragraaf 2.10** voor Rechten van Betrokkene en **Beleid Privacy & Bescherming Persoonsgegevens paragraaf 10.3.**
Registratie	Onderzoek dient vastgelegd te worden in Verwerkingsregister (**paragraaf 3.2**)

2.1.2. Gebruik van reeds bestaande datasets (Secundair gebruik)

Bij wetenschappelijk onderzoek komt het regelmatig voor dat data die voor een ander onderzoek verzamelt wordt, wordt hergebruikt bij een nieuw onderzoek. Dit noemt men secundair gebruik, waarvoor de AVG specifieke regelgeving heeft opgenomen (artikel 5 lid 1 sub b). Het gebruik van een reeds bestaande dataset is toegestaan op basis van de AVG vanwege het

belang van wetenschappelijk onderzoek onder voorwaarden (art. 89) zoals passende waarborgen, technische en organisatorische maatregelen, Pseudonimisering etc).
Bij hergebruik van reeds bestaande dataset zullen waar mogelijk alleen Geanonimiseerde of Gepseudonimiseerde gegevens gedeeld worden, waarbij de onderzoeker het koppelbestand in geval van Gepseudonimiseerde gegevens niet ontvangt.

Indien er sprake is van Bijzondere Persoonsgegevens (art 9 lid 2 sub j AVG) dan geldt er nog een aanvullende toets bij Wetenschappelijk Onderzoek: alleen toegestaan indien noodzakelijk, evenredig en passende maatregelen.

Tenslotte geldt op basis van artikel 14 lid 5b van de AVG het recht van Betrokkene om direct geïnformeerd te worden over de Verwerking als Persoonsgegevens niet van Betrokkene zijn ontvangen tenzij dit onevenredig veel inspanning vergt. In dit laatste geval dienen de Betrokkene dan wel openbaar te worden geïnformeerd (door middel van Privacy Statement).

Anonimiseren of Pseudonimiseren	Bij gebruik van reeds bestaande datasets dienen Persoonsgegevens zoveel mogelijk Geanonimiseerd te worden. Indien de primaire dataset Geanonimiseerd is, is deze richtlijn niet meer van toepassing en hoeft ook het Verwerkingsregister niet bijgewerkt te worden. Indien Anonimiseren niet mogelijk is dan dienen Persoonsgegevens zoveel mogelijk Gepseudonimiseerd te worden. De AVG en deze richtlijn is hierop van toepassing. Zie verdere toelichting hieronder.
Dataminimalisatie	Indien herleidbare Persoonsgegevens noodzakelijk zijn voor wetenschappelijk onderzoek: • De onderzoeker mag **alleen Persoonsgegevens die noodzakelijk zijn voor het doel van het wetenschappelijk onderzoek verzamelen (zo weinig mogelijk),** maar waarborgt wel dat er voldoende gegevens verzameld worden om de vraagstelling van het onderzoek te kunnen beantwoorden
Beveiliging	Indien Persoonsgegevens gebruikt worden in onderzoek dan dienen deze adequaat beveiligd Verwerkt te worden. Zie **hoofdstuk 9 Beleid Privacy & Bescherming Persoonsgegevens**.
Informatieverplichting	De Respondenten hebben het Recht op Informatie en dienen goed geïnformeerd te worden. Zie **paragraaf 2.10** voor Rechten van Betrokkene
Registratie	Onderzoek dient vastgelegd te worden in Verwerkingsregister (**paragraaf 3.2**)

2.1.3. Gebruik van openbare datasets

Bij wetenschappelijk onderzoek wordt veelal gebruik gemaakt van openbare datasets waarin niet eenvoudig herleidbare Persoonsgegevens zijn opgenomen, te onderscheiden in:

- Openbare datasets die gedownload kunnen worden, zoals data van het CBS of de European Social Survey en World Value Survey (WVS). Deze datasets bevatten wel Persoonsgegevens, maar deze zijn Geanonimiseerd [3] of Gepseudonimiseerd (waarbij

[3] Geanonimiseerde datasets bevatten geen Persoonsgegevens en vallen daarmee niet onder deze richtlijn.

Tilburg University de sleutel voor het koppelen van de datasets niet heeft) en daarmee (voor Tilburg University) niet te herleiden naar personen. Deze datasets zonder herleidbare Persoonsgegevens vallen daarmee niet onder de AVG. Vaak dien je bij gebruik van deze datasets (bij afsluiten licentie) wel een aantal zaken te verklaren bijvoorbeeld dat je ze niet commercieel gebruikt.

- Openbare databases waar gebruik van gemaakt kan worden door middel van een licentie.

Attentiepunt hierbij dat indien 2 openbare datasets gecombineerd worden er mogelijk wel sprake kan zijn van (in de toekomst) herleidbare Persoonsgegevens.

Gebruik openbare datasets	Bij gebruik van openbare datasets wordt **in principe** gebruik gemaakt van Geanonimiseerde of Gepseudonimiseerde Persoonsgegevens (zonder koppelbestand) die daarmee niet herleidbaar zijn. De onderzoeker dient te waarborgen dat voldaan wordt aan de eisen gesteld in de licentie of bij het downloaden, en dat de Persoonsgegevens niet Herleidbaar zijn. **Let op**: Indien de openbare dataset of deze door combinatie van datasets Persoonsgegevens bevat die wel Herleidbaar zijn dan dient het onderzoek te voldoen aan alle vereisten zoals opgenomen in dit Beleid. De Data Representative kan ondersteunen bij het vaststellen of dit noodzakelijk is.

2.1.4. Dataset op basis van Webscraping

Naast openbare datasets wordt regelmatig gebruik gemaakt van Webscraping uit (semi) openbare bronnen. Als een onderzoeker fora, social media of andere (semi) openbare websites wil scrapen, kan er sprake zijn van auteursrecht en gebruiksvoorwaarden van de openbare bron.

Gebruik webscraping	Voor wetenschappelijk onderzoek mag onderzoeker door middel van **Webscraping** onder voorwaarden Persoonsgegevens verwerken indien deze **openbaar** zijn en zijn verzameld met een vergelijkbaar doel. Dit geldt ook voor Bijzondere Persoonsgegevens die door Betrokkene zelf duidelijk openbaar zijn gemaakt. **Let op**: er kan sprake zijn van auteursrecht en gebruiksvoorwaarden van de openbare bron. Zie voor meer detail: **Auteursrecht InfoPunt op Intranet**

Daarnaast dient de onderzoeker ook rekening te houden met de context waarin de openbare informatie geplaatst is. De openbare informatie mag gebruikt worden voor wetenschappelijk onderzoek als deze met het doel is geschreven. Dit geldt ook nadrukkelijk voor Bijzondere Persoonsgegevens die door betrokkene zelf duidelijk openbaar zijn gemaakt. Een aantal voorbeelden ter verduidelijking:

- *Indien een onderzoeker blogs van AirBnB gebruikt (waarin reizigers hun ervaringen weergeven) die openbaar zijn om na te gaan of toeristen etnocentrisch zijn. Bij het schrijven van de blogs hadden auteurs niet kunnen vermoeden hoe hun teksten gebruikt zouden gaan worden en zouden zij mogelijk geen toestemming hebben gegeven als daarom gevraagd zou zijn. Deze informatie mag dan niet*

gebruikt worden en de onderzoeker dient dan expliciete toestemming te vragen aan de auteurs van de blogs.

- *Indien een onderzoeker gebruik maakt van een openbare blog op Facebook waarin iemand schrijft over persoonlijke ervaringen bij kanker, met als doel lotgenoten en naasten te informeren. In dit geval mag de onderzoeker deze informatie wel gebruiken indien hij deze informatie gebruikt om ervaringen van patiënten te vergelijken.*
- *Indien een onderzoeker gebruik maakt van een blog op besloten forum die niet openbaar is (maar waar onderzoeker met het doel van het onderzoek tot krijgt) mag het niet gebruikt worden voor wetenschappelijk onderzoek (tenzij onderzoeker specifiek toestemming (informed consent) heeft van de betrokkene.*

In **bijlage 1** zijn een aantal voorbeelden opgenomen van soorten datasets waarin Persoonsgegevens verwerkt worden, waarbij specifieke richtlijnen worden aangegeven voor de diverse soorten onderzoek zoals:

- Video- en audio opnames
- Interviews
- Observaties
- Experimenten in Labs (inclusief virtual reality labs)
- Eye tracking
- ECG /EEG/MRI
- Wearables
- ….

De bovenstaande lijst is niet limitatief, andere voorbeelden die niet genoemd worden vallen vanzelfsprekend ook onder dit beleid.
TiU beschouwt de gegevens die in het kader van dergelijke onderzoeken worden verzameld als Persoonsgegevens. Deze beleidskeuze wordt gemaakt omdat patronen uit dergelijke onderzoeken mogelijk in toekomst wel herleidbaar zijn naar Personen.

Indien in een wetenschappelijk onderzoek Persoonsgegevens verwerkt worden dan dient eerst de zogenaamde Rechtmatigheid en Doelbinding te worden vastgesteld. Hierna dienen de zogenaamde Materiele vereisten in acht te worden genomen om te zorgen dat zorgvuldig met Persoonsgegevens wordt omgegaan.

2.2. Rechtmatigheid – Verwerkingsgrondslag

Elke verwerking van Persoonsgegevens dient rechtmatig te zijn, dat wil zeggen dat er een wettelijke Verwerkingsgrondslag en doel moet zijn voor de verwerking. In het **Beleid Privacy & Bescherming Persoonsgegevens** zijn de zes wettelijke Verwerkingsgrondslagen uitgebreid toegelicht.

Voor wetenschappelijk onderzoek gelden de volgende Verwerkingsgrondslagen die afhankelijk zijn van hoe de onderzoeker een dataset samenstelt:

- Opzetten nieuwe dataset direct van Respondenten
- Opzetten nieuwe dataset niet via Respondenten (bijvoorbeeld webscraping)
- Gebruik van Bestaande dataset.

Let op: indien ook Bijzondere Persoonsgegevens verwerkt worden, is **paragraaf 2.3** in plaats van **paragraaf 2.2** van toepassing. Daarvoor gelden striktere regels en minder mogelijke grondslagen.

Verwerkingsgrondslag NIEUWE DATASET DIRECT VAN RESPONDENTEN	Verwerkingsgrondslag is in het algemeen **toestemming van Betrokkene.** In **uitzonderingsituaties** kan er echter ook sprake zijn van een van de onderstaande Verwerkingsgrondslagen: • **Noodzakelijk voor taak van algemeen belang** • **Noodzakelijk voor gerechtvaardigd belang**: hierbij dient een belangenafweging gemaakt te worden tussen het belang van het wetenschappelijk onderzoek en het privacy belang van de betrokkene. Voor meer uitleg over de diverse Verwerkingsgrondslagen verwijzen we naar het **Beleid Privacy & Verwerking Persoonsgegevens – paragraaf 4.2.** Of en indien een dergelijke uitzondering van toepassing is, dient dit door Onderzoeker goed gedocumenteerd en gemotiveerd vastgelegd te worden in de vragenlijst Onderzoek. Eventueel kan Data Representative hierbij adviseren. Het is noodzakelijk dat bij het onderzoek de belangen van de Betrokkene goed gewaarborgd zijn qua onderzoeksopzet en beheer / beveiliging van Persoonsgegevens. Zie hiervoor de vereisten bij de diverse punten van de onderzoek levenscyclus. *Voorbeeld:* • *Bij bepaalde vormen van medisch onderzoek ten bate van de volksgezondheid kan er sprake zijn van verwerkingsgrondslag taak van algemeen belang.*
Verwerkingsgrondslag NIEUWE DATASET niet VIA Betrokkene – openbare data	Verwerkingsgrondslag bij wetenschappelijk onderzoek waarbij een nieuwe dataset wordt opgezet waarbij onderzoeksdata worden verzameld zonder deze direct van Respondenten te verkrijgen is: **Gerechtvaardigd belang**. De onderzoeksdata worden in dit geval verzameld aan de hand van door Respondent zelf openbaar gemaakte informatie. *Voorbeeld: opzetten nieuwe dataset aan de hand van webscraping. Zie ook **paragraaf 2.1.4.***

Bij secundair gebruik van reeds verzamelde dataset moet onderscheid worden gemaakt in een aantal scenario's om te bepalen welke verwerkingsgrondslag van toepassing kan zijn:

- Initiële dataverzameling is gebaseerd **op Toestemming**:
  i. Toestemming voor hergebruik voor toekomstig onderzoek & nieuw onderzoek vindt plaats in onderzoeksgebied waarvoor toestemming is gegeven
  ii. Toestemming voor hergebruik in toekomstig onderzoek & nieuw onderzoek vindt plaats in **ander onderzoeksgebied**

iii. **geen <u>Toestemming</u> voor hergebruik** voor toekomstig onderzoek.

- Initiële dataverzameling **is niet** gebaseerd op toestemming, maar **andere <u>Verwerkingsgrondslag</u>**

Verwerkingsgrondslag SECUNDAIR: Toestemming hergebruik Zelfde onderzoeksgebied	Verwerkingsgrondslag <u>is **Toestemming**</u> maar onderzoeker hoeft **geen nieuwe toestemming** te vragen. Wel geldt een informatieplicht: ○ Beschikt over contactgegevens van Betrokkene: persoonlijk informeren indien dit geen onevenredige inspanning vergt[4] ○ Beschikt niet over contactgegevens: openbaar informeren **Let op**: Bij toestemming mag een respondent deze altijd intrekken, indien dit gebeurt dan mag de data van deze respondent niet meer gebruikt worden voor vervolg onderzoek voor zover deze te herleiden is. Zie **paragraaf 2.9** voor richtlijnen inzake intrekken toestemming. *Voorbeeld: een onderzoeker gebruikt voor een vervolgonderzoek binnen hetzelfde onderzoeksgebied de data van een eerder onderzoek. Dit eerdere onderzoek is gebaseerd op toestemming en de Respondent is ermee akkoord gegaan dat zijn gegevens worden gebruikt in toekomstige onderzoeken.*
Verwerkingsgrondslag SECUNDAIR: toestemming hergebruik ANDER onderzoeksgebied	Verwerkingsgrondslag is **<u>Toestemming</u>**. Omdat bij primair onderzoek geen toestemming is gevraagd voor dit onderzoeksgebied dient indien dit redelijkerwijs mogelijk is als nog gevraagd te worden: ○ Beschikt over contactgegevens van Betrokkene: persoonlijk toestemming vragen ○ Beschikt niet over contactgegevens: verwerkingsgrondslag gerechtvaardigd belang: in verband met Recht op Informatie openbaar informeren. *Voorbeeld: een onderzoeker gebruikt voor een vervolgonderzoek binnen een ander onderzoeksgebied de data van een eerder onderzoek. Dit eerdere onderzoek vond plaats in onderzoeksgebied marketing en aan Respondent is toestemming gevraagd voor hergebruik maar alleen binnen onderzoeksgebied marketing. Het nieuwe onderzoek vindt plaats binnen onderzoeksgebied rechten.*
SECUNDAIR: geen toestemming voor hergebruik	Verwerkingsgrondslag is in principe toestemming maar zou in uitzonderingsgevallen ook een van de andere grondslagen zoals boven vermeld kunnen zijn (bijvoorbeeld gerechtvaardigd belang). De onderzoeker dient alsnog **<u>Toestemming</u>** te vragen voor het hergebruik van deze data als dit mogelijk is. *Voorbeeld: een onderzoeker gebruikt voor een vervolgonderzoek de data van een eerder onderzoek. Bij dit eerdere onderzoek is geen toestemming gevraagd voor hergebruik. Indien het mogelijk is (beschikking over contactgegevens) dan dient onderzoeker alsnog toestemming te vragen. Indien dit niet mogelijk is dan kan een andere verwerkingsgrondslag zoals gerechtvaardigd belang van toepassing zijn, waarbij onderzoeker een zorgvuldige afweging moet maken tussen belang van het onderzoek en*

[4] Onevenredige inspanning zou bijvoorbeeld van toepassing kunnen zijn als het hele grote databases zijn waarbij veel respondenten benaderd moeten worden. Indien voor deze uitzondering wordt gekozen dient dit wel vastgelegd te worden door de onderzoeker (gemotiveerd).

	het privacy belang van de Betrokkene. Hij dient deze afweging vast te leggen in de vragenlijst Onderzoek.
SECUNDAIR : primaire dataset NIET op basis van TOESTEMMING	Verwerkingsgrondslag voor hergebruik data zou in dit geval Gerechtvaardigd belang kunnen zijn, waarbij de onderzoeker een afweging dient te maken tussen het belang van het wetenschappelijk onderzoek en het privacy belang van de Betrokkene. Hij dient deze afweging vast te leggen in de vragenlijst Onderzoek.

2.3. Rechtmatigheid – Verwerkingsgrondslag Bijzondere persoonsgegevens

Bijzondere Persoonsgegevens mogen volgens de AVG alleen op strikte voorwaarden verwerkt worden. Voor Wetenschappelijk onderzoek geldt onder voorwaarden een opheffing van het verbod op het verwerken van bijzondere persoonsgegevens. Zie **Beleid Privacy & Bescherming persoonsgegevens paragraaf 4.3**.

Bijzondere Persoonsgegevens	Bijzondere Persoonsgegevens zijn: • Ras en etnische afkomst • Politieke opvattingen • Religieuze of levensbeschouwelijke overtuiging • Lidmaatschap van een vakbond • Genetische gegevens • Biometrische gegevens met het oog op identificatie • Gegevens over gezondheid (medische gegevens) • Gegevens m.b.t. seksueel gedrag of seksuele gerichtheid. Deze gegevens mogen enkel Verwerkt worden conform **paragraaf 2.3**. **Let op**: Als er Bijzondere Persoonsgegevens worden verwerkt dan zijn er extra eisen inzake beveiliging. Zie **hoofdstuk 9 van beleid privacy en verwerking persoonsgegevens**.
Gebruik Bijzondere Persoonsgegevens	Bijzondere Persoonsgegevens mogen bij wetenschappelijk onderzoek verwerkt worden indien er **expliciete toestemming** is. Specifiek voor wetenschappelijk onderzoek geldt **een uitzondering** welke enkel op gaat als: 1. **het vragen van toestemming onmogelijk blijkt of een onevenredige inspanning vergt**, 2. de verwerking **noodzakelijk is met het oog op het onderzoek** en 3. het **onderzoek een algemeen belang** dient. Ook dient er te zijn voorzien in zod**anige waarborgen dat de persoonlijke levenssfeer van de Betrokkene niet onevenredig wordt geschaad**. Voor de diverse soorten datasets volgt hieronder een uitwerking
NIEUWE dataset met Bijzondere Persoonsgegevens – DIRECT VAN RESPONDENT ontvangen (niet d.m.v.	**Toestemming verplicht** (informed consent): Respondent moet op Informed Consent formulier expliciete toestemming geven voor de Verwerking van de Bijzondere Persoonsgegevens.

webscraping of d.m.v. openbare data)	
NIEUWE dataset – WEBSCRAPING OF OPENBARE DATA	Toestemming verkrijgen is onmogelijk of kost onevenredig veel inspanning derhalve: • Openbaar informeren door middel van Privacy Statement (**paragraaf 2.10.1)**
HERGEBRUIK DATASET (SECUNDAIR GEBRUIK) met Bijzondere Persoonsgegevens	**Bij initiële onderzoek toestemming gegeven voor Bijzondere Persoonsgegevens én toestemming voor hergebruik data in zelfde/bepaalde onderzoeksgebied(en):** ○ Geen nieuwe toestemming nodig indien binnen aangegeven onderzoekgebied. Wel informeren**.** **Bij initiële onderzoek GEEN toestemming voor Bijzondere Persoonsgegevens of hergebruik (voor onderzoeksgebied nieuw onderzoek)** ○ Toestemming vragen voor Bijzondere Persoonsgegevens tenzij hierboven vermelde uitzondering geldt (onderzoeker dient toepassing uitzondering gemotiveerd vast te leggen) **Initieel onderzoek OPENBARE gegevens**: geen specifieke toestemming in verband met openbaarheid gegeven **Let op**: Informatieverplichting is altijd van toepassing

2.4. Doelbinding

Het tweede vereiste is dat er sprake moet zijn van doelbinding: er moet sprake zijn van een welbepaald, duidelijk omschreven doel (zie voor meer detail **Beleid Privacy & Bescherming Persoonsgegevens hoofdstuk 5**).

Doelbinding nieuwe dataset	Het doel van de Verwerking Persoonsgegevens: Het uitvoeren van wetenschappelijk onderzoek als bedoeld in de Wet op het Hoger onderwijs en Wetenschappelijk onderzoek en de Gedragscode Wetenschapsbeoefening naar (DOEL ONDERZOEK VERMELDEN)
Doelbinding – secundair gebruik dataset	• Wetenschappelijk onderzoek waarbij gebruikt wordt gemaakt van een bestaande dataset die Persoonsgegevens bevat dan wordt dit doel altijd als verenigbaar beschouwd met het originele doel waarvoor dataset verzamelt wordt. • Het doel van de nieuwe verwerking van Persoonsgegevens is: Het uitvoeren van wetenschappelijk onderzoek als bedoeld in de Wet op het Hoger onderwijs en Wetenschappelijk onderzoek en de Gedragscode Wetenschapsbeoefening naar (DOEL ONDERZOEK VERMELDEN)

2.5. Regeling Onderzoeksdatamanagement

Ten behoeve van goed databeheer en dataopslag is de **Regeling Onderzoeksdatamanagement** binnen TiU opgesteld en geïmplementeerd.

Regeling Onderzoeks-datamanagement	Op alle wetenschappelijk onderzoek waarbij Persoonsgegevens worden verwerkt is de **Regeling Onderzoeksdatamanagement** van toepassing ten behoeve van het waarborgen van een adequaat databeheer en dataopslag.

2.6. Ethische commissies

De richtlijnen inzake Bescherming Persoonsgegevens zijn minimale vereisten indien er sprake is van Persoonsgegevens bij wetenschappelijk onderzoek. De ethische commissie binnen de Schools kan aanvullende, meer stringente eisen stellen.

Ethische Commissie	De ethische commissie kan aanvullende (meer stringente) eisen stellen aan hetgeen in dit document inzake Bescherming Persoonsgegevens is beschreven.

2.7. Informed consent

Bij wetenschappelijk onderzoek is het van belang dat de Respondent vrijwillig meewerkt aan het onderzoek en daarnaast goed geïnformeerd wordt over de inhoud van het onderzoek (op basis van wetenschapsethiek). Hierbij wordt indien mogelijk gebruik gemaakt van het zogenaamde Informed consentformulier waarbij de Respondent wordt geïnformeerd en zijn Toestemming geeft voor deelname.

Indien de Verwerkingsgrondslag Toestemming is of er sprake is van Verwerking van Bijzondere Persoonsgegevens dan dient de Respondent hiervoor toestemming te geven. Deze toestemming moet aantoonbaar zijn en kan worden gecombineerd met het Informed consent formulier. Dit hoeft niet, het mag ook separaat.

Voor meer detail verwijzen we naar **paragraaf 3.1** waarin is toegelicht wanneer dit wel of niet noodzakelijk is.

2.8. Internationale onderzoeken

Het komt regelmatig voor dat onderzoekers van TiU samenwerken met andere universiteiten of onderzoek doen naar buitenlandse populaties. Dit heeft invloed op het toepassingsbereik van de AVG. De AVG en daarmee deze richtlijn is van toepassing bij:

Internationale Samenwerkingen	• **Wetenschappelijk onderzoek waarbij een onderzoeker van Tilburg University betrokken is.** Deze is immers (mede)verantwoordelijk en daarmee is de AVG van toepassing zelfs als onderzoek geen betrekking heeft op Persoonsgegevens van EU-burgers. **Let op**: in geval van internationale samenwerkingen kan er sprake zijn van doorgifte naar landen buiten de Europese Unie. Hiervoor gelden specifieke richtlijnen waarvoor we verwijzen naar **Beleid Privacy & Bescherming Persoonsgegevens.**

2.9. Intrekken van toestemming

Indien de Verwerking van Persoonsgegevens gebaseerd is op Toestemming dan heeft de Betrokkene het recht om deze toestemming in te trekken (naast de overige rechten zoals hieronder vermeldt in **paragraaf 2.10**). Hiervoor is ook geen uitzondering van toepassing voor wetenschappelijk onderzoek.

Het intrekken van deze toestemming moet voor Respondenten net zo eenvoudig zijn als het geven van deze toestemming. Dat betekent dat als dit door middel van een formulier is, dit ook kan plaatsvinden door middel van een formulier.

Indien een Respondent zijn toestemming intrekt dan betekent dit het volgende:

Intrekken toestemming voor het onderzoek	De Respondent neemt niet deel aan het onderzoek en al zijn gegevens dienen verwijderd te worden.
Tijdens het onderzoek	Hoofdregel hierbij is dat de data van de Persoon die zijn toestemming intrekt dient te worden verwijderd uit de onderzoeksdatabase TENZIJ dit het bereiken van het doel van het onderzoek onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In dat geval dient de onderzoeksdata volledig Geanonimiseerd te worden waardoor deze niet meer herleidbaar is naar de desbetreffende persoon. Indien een volledig cohort de Toestemming intrekt dan dient onderzoeker te overleggen met de ethische commissie en de Functionaris Gegevensbescherming. Voor controleerbaarheid van onderzoek is het in het kader van wetenschapsethiek vaak wel noodzakelijk dat data herleid kan worden. Door Anonimiseren is dit niet meer mogelijk, maar de onderbouwing hiervan (en daarmee controleerbaarheid) kan plaatsvinden door de intrekking van de toestemming (audit trail).
Na het onderzoek	Indien het onderzoek is gepubliceerd en daarmee afgerond: • Dient de onderzoeksdata, voor zover dat nog niet is gebeurd, volledig Geanonimiseerd te worden waardoor deze niet meer herleidbaar is naar de betreffende persoon; en • heeft de intrekking van de Toestemming gevolgen voor hergebruik van dataset in de toekomst: de onderzoeksdata van de personen die Toestemming hebben ingetrokken mogen NIET gebruikt worden voor toekomstig onderzoek. De onderzoeker dient te waarborgen dat dit niet gebeurt.

2.10. Rechten van respondent

De Respondent heeft voor, tijdens en na het onderzoek een aantal rechten. Voor meer informatie verwijzen we naar het **Beleid Privacy & Bescherming Persoonsgegevens hoofdstuk 10**. Een korte samenvatting van de rechten die Respondenten hebben:

Recht	Respondenten hebben het recht om
Recht op informatie	geïnformeerd te worden over welke Persoonsgegevens verwerkt worden.
Recht op inzage	te allen tijde de verzamelde Persoonsgegevens met betrekking tot hun persoon te mogen inzien.
Recht op rectificatie	te allen tijde te eisen dat onjuiste Persoonsgegevens gerectificeerd worden.
Recht op beperking	de verwerking van zijn Persoonsgegevens te beperken, bijvoorbeeld in afwachting op de uitkomst van een bezwaar. Beperking houdt in dat Persoonsgegevens worden gemarkeerd, en gedurende deze periode niet bewerkt of gedeeld mogen worden.
Recht op verwijdering	een aanvraag te doen om de gegevens van deelname inclusief de antwoorden die de Respondent gegeven heeft te verwijderen.
Recht op bezwaar	aan te geven dat zij niet (meer) willen dat hun gegevens verwerkt worden.

Voor de bovengenoemde algemene rechten van Betrokkene zijn voor wetenschappelijk onderzoek bepaalde uitzonderingen gemaakt in de AVG met betrekking tot:

- Inzage
- Verwijderen
- Corrigeren
- Beperken

Inzage, Verwijderen, beperken of corrigeren van Persoonsgegevens hoeven niet te worden gehonoreerd indien dit het wetenschappelijk onderzoek ernstig kan bedreigen én indien de nodige voorzieningen (denk bijvoorbeeld aan beveiliging in de vorm van autorisatie) zijn getroffen om te verzekeren dat Persoonsgegevens enkel voor wetenschappelijk onderzoek gebruikt kunnen worden. Het mag vanzelfsprekend wel.
Denk bijvoorbeeld aan onderzoek waarbij het verwijderen of aanpassen van de gegevens tot gevolg heeft dat de resultaten niet meer te gebruiken of te generaliseren zijn.

Verder is het van belang dat ethische commissies richtlijnen kunnen hanteren die strikter zijn dan in de wet staat en kunnen eisen dat respondenten geïnformeerd worden over alle gegevens die ten dienste van het onderzoek worden opgeslagen (niet enkel de Persoonsgegevens).

Rechten van Respondenten	Respondenten hebben de Rechten van Betrokkenen zoals in de AVG vernoemd (zie **Beleid Privacy & Bescherming Persoonsgegevens hoofdstuk 10**). Voor wetenschappelijk onderzoek gelden de volgende bijzonderheden: • Inzage, Rectificatie, Beperking en Verwijdering zijn niet van toepassing als dit het Wetenschappelijk onderzoek ernstig kan bedreigen. Respondenten kunnen zich hier niet op beroepen. Onderzoeker mag hier overigens wel aan meewerken. • Voorgaande uitzondering geldt enkel indien de nodige voorzieningen zijn getroffen om te verzekeren dat de Persoonsgegevens alleen voor wetenschappelijk onderzoek gebruikt kunnen worden. Indien het onduidelijk is dan dient overlegd te worden met de ethische commissie van de school.

	Let op: indien de Verwerkingsgrondslag Toestemming is, dan heeft Betrokkene altijd het recht om zijn **Toestemming in te trekken**. Zie meer detail **paragraaf 2.9**. **Let op**: voor beroep op rechten dient respondent gebruik te maken van de **standaardformulieren** inzake rechten betrokkene.
Verantwoordelijk rechten verwijdering, correctie en beperking.	• De onderzoeker stemt allereerst een beroep op de Rechten Verwijdering, Correctie en Beperking af met de Ethische commissie. • De onderzoeker informeert de Functionaris Gegevensbescherming over het verzoek van het recht en het besluit daarover ten behoeve van centrale registratie.

2.10.1. Recht op Informatie

Betrokken waarvan Persoonsgegevens worden verwerkt hebben het recht om vooraf goed geïnformeerd te worden.

Recht op informatie	Respondenten dienen vooraf duidelijk en goed geïnformeerd worden over het gebruik van Persoonsgegevens die verwerkt worden in het kader van onderzoek. Dit moet door: • Informed consent (zie voor bijzonderheden **paragraaf 3.1**) • Privacy Statement op website • Bij hergebruik bestaande dataset: door informatie (indien onderzoeker over contactgegevens beschikt dient deze persoonlijk toegestuurd te worden en anders openbaar vermeld te worden (internet)

3. ‘VOOR HET ONDERZOEK’

Dit hoofdstuk beschrijft de elementen van zorgvuldige omgang met data die van belang zijn voorafgaand aan elk onderzoek waarin Persoonsgegevens verwerkt worden en de manier waarop Tilburg University in deze fase van het onderzoek de zorgvuldige omgang met data waarborgt. Daarbij behandelt dit hoofdstuk achtereenvolgens de verwerkingsgrondslag voor het verwerken van persoonsgebonden data in onderzoek, het Informed Consent, het opstellen van een Data Management Plan (DMP) voorafgaand aan het onderzoek, inclusief het uitvoeren van de pre-Data Protection Impact Assessment (pre DPIA) als onderdeel van het DMP, en de toetsing van het DMP, de Data Protectie Impact Assessment (DPIA), het Verwerkingsregister en het verkrijgen van Informed consent.

3.1. Informed consent- TOESTEMMING

Een van de wettelijke Verwerkingsgrondslagen voor Wetenschappelijk onderzoek is TOESTEMMING van de Respondent. In uitzonderingsgevallen kunnen er echter ook andere Verwerkingsgrondslagen van toepassing zijn (**paragraaf 2.2).**
Indien Bijzondere Persoonsgegevens bij Wetenschappelijk onderzoek verwerkt worden dan dient hiervoor expliciete toestemming gegeven te worden.

Maar ook als er geen toestemming nodig is op basis van de AVG dan kiest Tilburg University er om ethische redenen wel voor om wel Informed consent te vragen aan Respondenten voor nieuwe Datasets en indien dit redelijkerwijs mogelijk is bij hergebruik van bestaande datasets. In het onderstaand overzicht is opgenomen hoe het voor de diverse situaties toestemming kan worden gegeven voor de Verwerking van Persoonsgegevens en/of Bijzondere Persoonsgegevens.

Deze toestemming dient bij voorkeur gecombineerd te worden met de informed consent die nodig is vanuit ethisch oogpunt om de Respondent niet te veel te belasten met de diverse formulieren. In onderstaand overzicht is opgenomen voor de diverse situaties wat deze toestemming in het kader van de AVG inhoudt.

Soort dataset	Verwerkings-grondslag	Bijz. Pers geg.	Informed consent ?
Nieuwe dataset – zelf verzamelen data van Respondenten	**Toestemming**	**nee**	**Ja**, Informed Consent voor alle Respondenten met toestemming voor: ○ Verwerking Persoonsgegevens ○ Toestemming voor hergebruik in toekomst ○ Wijzen op mogelijkheid intrekken toestemming **Tip:** omschrijf onderzoeksgebied zo ruim mogelijk voor eventueel hergebruik in toekomst.
	Toestemming	**ja**	Zie voorgaande aangevuld met: ○ Expliciete toestemming voor verwerking Bijzondere Persoonsgegevens
	Overige grondslagen	**nee**	**Ja,** Informed consent voor alle Respondenten vanuit wetenschapsethiek. Geen toestemming voor gebruik persoonsgegevens

	Overige grondslagen	**Ja**	Zie voorgaande aangevuld met: Expliciete toestemming voor verwerking Bijzondere Persoonsgegevens
Nieuwe dataset – NIET DIRECT RESPONDENTEN	Gerechtvaardigd belang	**nee**	**Nee**, alleen openbare informatie via privacy statement (**paragraaf 3.2**).
	Gerechtvaardigd belang	**Ja**	**Ja,** informed consent vragen met expliciete toestemming voor verwerking bijzondere Persoonsgegevens tenzij dit onmogelijk is of onevenredig veel inspanning kost. Altijd openbare informatie (Privacy Statement).
Hergebruik bestaande dataset	Initieel onderzoek toestemming voor onderzoeksgebied en hergebruik	**Nee/Ja**	**Nee**, wel informeren indien dit redelijkerwijs mogelijk is persoonlijk anders openbaar informeren (Privacy Statement) (**paragraaf 3.2**).
	Initieel onderzoek toestemming hergebruik **ander onderzoeksgebied of** **Initieel onderzoek geen toestemming voor hergebruik**	**Nee/Ja**	Beschikking over **contactgegevens**: informed consent met toestemming voor: ○ Verwerking Persoonsgegevens ○ Indien van toepassing: expliciete toestemming voor verwerking Bijzondere Persoonsgegevens ○ Toestemming voor hergebruik in toekomst ○ Wijzen op mogelijkheid intrekken toestemming **Geen contactgegevens**: openbaar informeren (Privacy Statement). (**paragraaf 3.2**). **Let op**: bij bijzondere persoonsgegevens gelden aanvullende eisen aan de uitzondering van geen expliciete Toestemming, zie paragraaf 2.3.
	Initieel onderzoek NIET toestemming	**Nee/ja**	Beschikking over **contactgegevens**: informed consent met toestemming voor: ○ Verwerking Persoonsgegevens ○ Indien van toepassing: expliciete toestemming voor verwerking Bijzondere Persoonsgegevens ○ Toestemming voor hergebruik in toekomst ○ Wijzen op mogelijkheid intrekken toestemming **Geen contactgegevens**: openbaar informeren (Privacy Statement) **Let op**: bij bijzondere persoonsgegevens gelden aanvullende eisen aan de uitzondering van geen expliciete toestemming, zie paragraaf 2.3

Inzake informed consent gelden de volgende richtlijnen.

Informed consent formulier	Voor elk wetenschappelijk onderzoek waarbij Informed Consent in bovenstaand schema van toepassing is, dient een zogenaamd Informed consent formulier aanwezig te zijn waarin o.a. is opgenomen de inhoud van

	de studie, duur, mogelijke consequenties, risico's en rechten die de respondent heeft. In geval **Verwerkingsgrondslag TOESTEMMING** is dan dient informed consent minimaal te bevatten: • Toestemming voor de Verwerking van Persoonsgegevens • Beschrijving van de wijze waarop de Respondent zijn Toestemming kan intrekken. • Bij voorkeur toestemming voor hergebruik voor toekomstig Wetenschappelijk onderzoek. • Rechten van Betrokkenen daarmee verwijzing naar de privacy statement op de website van Tilburg University. In geval bij het onderzoek Bijzondere Persoonsgegevens verwerkt te worden dan dient opgenomen te zijn: • Expliciete toestemming voor Verwerking van Persoonsgegevens. De Respondent dient de Informed consent te autoriseren (door middel van een handtekening, digitaal of op een audio-opname) zodat zijn toestemming reproduceerbaar is. De Informed consent kan door middel van een apart formulier of kan ook ook opgenomen zijn in een vragenlijst waarbij in geval van toestemming (voor verwerking persoonsgegevens en/of bijzondere persoonsgegevens) de Respondent een 'tic box' dient aan te klikken (actieve handeling).
Wettelijk vertegenwoordiger	Indien een persoon zelf niet in staat is om de toestemming te verlenen (e.g. verstandelijke of andersoortige handicap, na overlijden of andere reden) dient het Informed consent formulier geautoriseerd te worden door de wettelijk vertegenwoordiger van deze persoon.
Minderjarigen	Indien bij een onderzoek minderjarigen betrokken zijn gelden de volgende regels: • Jonger dan 16 jaar: toestemming van respondent (indien mogelijk) en ouder/voogd • Ouder dan 16 jaar en jonger 18 jaar: toestemming van respondent. Het is mogelijk dat binnen Schools afwijkende (strengere) afspraken zijn gemaakt. **Let op**: indien er Persoonsgegevens van minderjarigen worden verwerkt dan zijn er extra eisen inzake beveiliging van deze gegevens. Zie **hoofdstuk 9 Beleid Privacy & Bescherming Persoonsgegevens**.
Vereisten	• De Respondent dient voldoende tijd te krijgen voor het lezen en invullen van het Informed consent formulier. Bij voorkeur wordt dit formulier vooraf aan de Respondent gestuurd zodat hiervan kennis kan worden genomen • Ingevulde en geautoriseerde Informed consent formulieren dienen binnen de vastgestelde bewaartermijn (zie hoofdstuk 5.2) veilig bewaard te worden: ○ In een afgesloten kast / archief

	○ In een (digitale) map alleen toegankelijk voor onderzoeker(s) ○ Niet gekoppeld aan de overige data die in het onderzoek verzameld worden

3.2. Opstellen van een Data Management Plan

Voor aanvang van het wetenschappelijk onderzoek dient op basis van de **Regeling Onderzoeksdatamanagement** een Data Management Plan (DMP) te worden opgesteld. Hierin legt de onderzoeker onder andere vast welke data hij tijdens een onderzoeksproject gaat verzamelen, hoe hij deze data tijdens het project opslaat of beheert en wat er na afloop van het project met de data gebeurt, maar zijn ook de vereisten inzake Verantwoordingsplicht namelijk Data Protectie Impact Assessment en Verwerkingsregister gewaarborgd.

Data Protectie Impact Assessment (DPIA)

In sommige gevallen is brengt het verwerken van Persoonsgegevens een hoog risico voor betrokkene met zich mee. Om hier goed mee om te gaan dient op basis van de AVG de Data Protectie Impact Assessment (DPIA) wordt uitgevoerd om er zeker van te zijn dat de privacy risico's van de Respondenten goed gewaarborgd worden.
Een DPIA is meestal niet nodig voor wetenschappelijk onderzoek. Voor meer detail omtrent wanneer een DPIA verplicht is verwijzen we naar het **Beleid Privacy & Bescherming Persoonsgegevens paragraaf 11.2**.

Voor elk wetenschappelijk onderzoek waarbij Persoonsgegevens verwerkt worden dient een pre-DPIA (vragenlijst) ingevuld te worden om vast te stellen of het uitvoeren van een DPIA noodzakelijk is. Deze korte vragenlijst is opgenomen (geïntegreerd) in het Data Management Plan en wordt voor zover mogelijk gecombineerd met de vragenlijst voor de ethische toetsing.

Het doel van de DPIA is om tijdig de risico's van de gegevensverwerking in kaart te brengen. Welke Persoonsgegevens worden verwerkt, wat doet TiU ermee, wat zijn de consequenties en hoe gaan we ermee om?

Indien een DPIA noodzakelijk is, dan dient contact opgenomen te worden met de Data Representative (die vervolgens de Functionaris Gegevensbescherming consulteert). De vragenlijst voor het uitvoeren van een pré-DPIA is opgenomen in het Data Management Plan.

Verwerkingsregister

Alle Verwerkingen van Persoonsgegevens dienen op basis van de AVG vastgelegd te worden in het universitaire Verwerkingsregister in het kader van de verantwoordingsplicht. Het Verwerkingsregister wordt voor wetenschappelijk onderzoek gevuld op basis van de informatie die is opgenomen in het Data Management Plan (en indien mogelijk gecombineerd met de vragenlijst ethische toetsing). Aan de hand van het Verwerkingsregister wordt het Privacy Statement op de website geactualiseerd.

Datamanagement plan – Verwerkingsregister	Voor elk wetenschappelijk onderzoek **moet de onderzoeker een Data Management Plan opstellen** waarin vastgelegd is welke (Persoons)gegevens verwerkt worden. Dit Data Management Plan wordt zover het Persoonsgegevens bevat opgenomen in het universitaire Verwerkingsregister. Voor het format van het Data Management Plan verwijzen we naar de **Regeling Onderzoeksdatamanagement**.

Pre – DPIA	Voor elk wetenschappelijk onderzoek dient een pre-DPIA (vragenlijst) ingevuld te worden om vast te stellen of het uitvoeren van een DPIA noodzakelijk is. Deze vragenlijst is opgenomen (geïntegreerd) in het Data Management Plan en indien mogelijk gecombineerd met de vragenlijst ten behoeve van de ethische commissie.
Date Protectie Impact Assesment (DPIA)	In sommige situaties is het noodzakelijk dat een Data Protectie Impact Assessment (DPIA) wordt uitgevoerd. Of dit noodzakelijk is vloeit voort uit de Pre-DPIA vragenlijst. De onderzoeker is verantwoordelijk voor het uitvoeren van de DPIA indien dit noodzakelijk is. Hiervoor is een **procedure** beschikbaar. Hij wordt hierbij ondersteund door de Data Representative van de school.
Toetsing DPIA	De Functionaris Gegevensbescherming toetst de DPIA.
Toetsing Datamanagement Plan en toetsing door Ethische Commissie	In iedere School zijn nadere afspraken gemaakt over de toetsing van het Datamanagementplan (DMP) (door een wetenschappelijke en/of ethische commissie) en de opslag hiervan.

Een onderzoeker mag niet zonder meer alle Persoonsgegevens verwerken. Hieronder zijn een aantal bijzonderheden opgenomen:

Dataminimalisatie - Noodzakelijke gegevens	De onderzoeker mag **alleen Persoonsgegevens die noodzakelijk zijn voor het doel van het wetenschappelijk onderzoek verzamelen,** maar waarborgt wel dat er voldoende gegevens verzameld worden om de vraagstelling van het onderzoek te kunnen beantwoorden.
BSN	Het **Burgerservicenummer** (BSN) mag **nooit** verwerkt worden voor wetenschappelijk onderzoek.
Identiteitsbewijs	Een kopie Identiteitsbewijs mag **alleen worden ingezien**, maar niet bewaard worden tenzij het bewaren noodzakelijk is voor het wetenschappelijk onderzoek en foto en BSN nummer gemaskeerd zijn en op de kopie gemarkeerd is dat het is afgegeven ten behoeve van onderzoek. **Tip**: Noteer bij voorkeur alleen de noodzakelijke gegevens in plaats van een kopie ID.
Hulp bij opstellen	De facultaire Data Representative ondersteund bij het invullen van de pre-DPIA, de DPIA en het Verwerkingsregister

Privacy statement

Op basis van het recht op Informatie publiceert Tilburg University een Privacy-statement op de website, waarin TiU informeert over het gebruik van Persoonsgegevens in wetenschappelijk onderzoek. Het op deze wijze informeren is noodzakelijk omdat niet voor alle onderzoeken (denk bijvoorbeeld aan openbare database, hergebruik bestaande database of webscraping) met informed consent kan worden gewerkt, en het juist ook bij deze vormen van data transparant dient te zijn hoe TiU omgaat met Persoonsgegevens. Daarbij kan het zijn dat bepaalde onderzoeken niet opgenomen zijn in deze lijst in verband met vertrouwelijkheid of gevoeligheid van het onderzoek (bijvoorbeeld als we een onderzoek doen naar een indicator voor aanwezigheid van hennepkwekerijen).

Privacy Statement	Het Privacy Statement inzake wetenschappelijk onderzoek en de lijst met lopende wetenschappelijke onderzoeken waarin gebruik gemaakt wordt van

	Persoonsgegevens wordt samengesteld op basis van de informatie uit het Verwerkingsregister. Hiervoor is geen actie van de onderzoeker nodig. De ethische commissie kan besluiten om een onderzoek als vertrouwelijk te markeren waardoor de informatie over het desbetreffende onderzoek niet openbaar mag worden gemaakt in het privacy statement.

4. ‘TIJDENS HET ONDERZOEK’

Dit deel van het beleid beschrijft de elementen van zorgvuldige omgang met data die van belang zijn tijdens elk onderzoek waarin Persoonsgegevens verwerkt worden en de manier waarop Tilburg University juist in deze fase van het onderzoek de zorgvuldige omgang met data waarborgt. Daarbij behandelt dit hoofdstuk achtereenvolgens de omgang met contactgegevens van respondenten, de rechten van participanten tijdens het onderzoek, het gebruik van programma’s voor het verzamelen-, opslaan- en analyseren van data, het delen van data, het beveiligen van data en het rapporteren van de resultaten.

4.1. Contactgegevens van (potentiële) respondenten

Een onderzoeker van Tilburg University die contactgegevens verzamelt en bewaart in het kader van wetenschappelijk onderzoek dient deze volgens de AVG beveiligd op te slaan waarbij beperkte toegang verzekerd is. De onderzoeker is verantwoordelijk voor het separaat opslaan van het bestand met contactgegevens. De contactgegevens die gelinkt kunnen worden aan de dataset dienen zo snel als mogelijk (binnen 6 maanden tenzij langer noodzakelijk is) door de onderzoeker verwijderd te worden, zolang dit niet conflicteert met belangen van het wetenschappelijk onderzoek.

Opslag en toegang van contactgegevens	Bestanden met Contactgegevens mogen alleen toegankelijk zijn voor noodzakelijke Personen: de betrokken hoofdonderzoekers en leidinggevende.

4.1. Wijziging in verzamelde Persoonsgegevens

Een onderzoeker kan gedurende het onderzoek besluiten dat aanvullende Persoonsgegevens noodzakelijk zijn. Hiervoor gelden de volgende richtlijnen:

Wijziging persoonsgegevens	Indien er gedurende het onderzoek wijzigingen plaatsvinden in de Persoonsgegevens die verzameld worden dan dient de onderzoeker: • Datamanagementplan aan te passen door middel van een amendement zodat ook het Verwerkingsregister geactualiseerd wordt.

4.2. Toegang en beveiliging persoonsgegevens

Binnen Tilburg University krijgen zo min mogelijk personen toegang tot de Datasets (digitaal of fysiek) inzake onderzoek waarin Persoonsgegevens verwerkt zijn. Deze toegang beperkt zich meestal tot de betrokken onderzoekers, en zijn leidinggevende. We verwijzen hiervoor ook naar **hoofdstuk 9 Beleid Privacy & Bescherming Persoonsgegevens** en het **Informatiebeveiligings-beleid.**

Toegang tot bestanden Persoonsgegevens	Toegang is alleen toegestaan voor de betrokken onderzoekers (inclusief student onderzoekers) en de leidinggevende (in verband met back-up)
Toegang tot archieven	Toegang tot Datasets (digitaal en fysiek) met Persoonsgegevens is alleen toegestaan voor onderzoekers, de departementsvoorzitter en de beheerder van de digitale of fysieke dataset.

Datasets (digitaal en fysiek) met Persoonsgegevens dienen veilig opgeslagen te worden en zijn alleen toegankelijk voor degene voor wie dit in het kader van het onderzoek noodzakelijk is.

Veilige opslag Persoonsgegevens – digitaal	Datasets met Persoonsgegevens dienen veilig opgeslagen te worden. Dat wil zeggen: • Gepseudonimiseerd wat wil zeggen dat het koppel- of communicatiebestand op de universitaire netwerkschijf (M/O-drive) • Op de (beveiligde omgeving) van een server van TiU. • In een gecontracteerde clouddienst zoals Surf Drive. • Alleen in versleutelde of geëncrypteerde vorm op een opslagmedium (laptop, USB). Bij afwezigheid van de onderzoekers op de werkplek dienen computers gelockt te zijn en de werkruimte afgesloten.
Veilige opslag persoonsgegevens – fysiek	Documenten met Persoonsgegevens dienen veilig opgeslagen te worden in een afgesloten kast of archief Bij afwezigheid dienen de kasten of archieven afgesloten te zijn en niet toegankelijk voor onbevoegden.

4.3. Gebruik van programma's voor het verzamelen, opslaan, analyseren en delen van data

Het verzamelen van data gedurende het onderzoek kan op diverse manieren plaatsvinden, online, face-to-face, met een papieren vragenlijst, observaties, video-beelden, etc. De AVG heeft implicaties voor deze manieren van data verzamelen, het gebruik van bestaande of nieuwe data, de tools die gebruikt worden bij het verzamelen van data en eventuele veiligheidsaspecten voortkomend uit de AVG gedurende het onderzoek.

Bij gebruik van applicaties/programma's van externe leveranciers dient er een Verwerkersovereenkomst afgesloten om goede afspraken te maken over verantwoordelijkheden, beveiliging etc. Voor meer uitleg hierover verwijzen we naar het **Beleid Privacy & Bescherming Persoonsgegevens hoofdstuk 11.4**.

Verzamelen van data	Indien voor het verzamelen van Persoonsgegevens externe applicaties gebruikt worden: • Zie **Regeling Onderzoeksdatamanagement** voor aanvullende richtlijnen. • Gebruik bij voorkeur applicaties vermeld op de **lijst door TiU goedgekeurde applicaties**. Bij deze applicaties is vastgesteld dat ze voldoen aan alle vereisten van de AVG en dat er een Verwerkersovereenkomst is afgesloten.

	• Indien de onderzoeker een applicatie wil gebruiken die niet op deze lijst staat dan dient hij een **Verwerkersovereenkomst** af te sluiten (zie hieronder).

Opslaan van data	**Digitaal**:
	• Zie **Regeling Onderzoeksdatamanagement** voor aanvullende richtlijnen.
	• Alle (ruwe) data dient Gepseudonimiseerd opgeslagen te worden op de servers van TiU of surfdrive waarbij het koppel- of communicatiebestand wordt opgeslagen op de universitair netwerkschijf.
	• Indien onderzoeker van een andere (cloud)dienst gebruik wil maken:
	  ○ Gebruik bij voorkeur applicaties op de **lijst door TiU goedgekeurde applicaties**. Bij deze applicaties is vastgesteld dat ze voldoen aan alle vereisten van de AVG en dat er een Verwerkersovereenkomst is afgesloten.
	  ○ Indien de onderzoeker een applicatie wil gebruiken die niet op deze lijst staat dan dient hij een verwerkersovereenkomst af te sluiten (zie hieronder).
	Fysiek
	Alle Persoonsgegevens dienen fysiek opgeslagen te worden in een afgesloten kast of archief. Indien opslag op externe locatie/beheerder dan dient hiermee een **Verwerkersovereenkomst** afgesloten te worden.

Analyseren van data	Indien voor het analyseren van data applicaties zoals SPSS worden gebruikt: • Gebruik bij voorkeur applicaties op de **lijst door TiU goedgekeurde applicaties**. Bij deze applicaties is vastgesteld dat ze voldoen aan alle vereisten van de AVG en dat er een Verwerkersovereenkomst is afgesloten. • Indien onderzoeker een applicatie wil gebruiken die niet op deze lijst staat dan dient hij een **Verwerkersovereenkomst** af te sluiten (zie hieronder).
Delen van data	• Het delen van data met collega's voor een co-analyse of peer review van de analyse mag alleen indien dit op een veilige manier gebeurt, bijvoorbeeld door gebruik te maken van versleuteling (via Secure File Transfer: **procedure** op intranet). • Voor gebruik van clouddiensten verwijzen we naar opslaan van data hierboven. • Het delen van data via een cloud service of andere programma's buiten het beheer van TiU, is alleen toegestaan indien er een Verwerkersovereenkomst afgesloten is met de betreffende partij.
Anonimiseren of Pseudonimiseren	Indien Persoonsgegevens niet langer noodzakelijk zijn (dan wel op basis van de Gedragscode VSNU enkel in verband met controleerbaarheid bewaard moeten worden), maar de data nog niet verwijderd kunnen worden, dan moeten de Persoonsgegevens in een zo vroeg mogelijk stadium Geanonimiseerd of Gepseudonimiseerd worden.

4.4. Overeenkomst en Verwerkersovereenkomst

Het is wettelijke verplicht dat, wanneer een onderzoeker namens TiU Persoonsgegevens uitwisselt met, verstrekt aan of ontvangt van een andere organisatie, daar goede contractuele afspraken over worden gemaakt. Wat voor soort overeenkomst gesloten dient te worden is afhankelijk van de rol van TiU en de rol van de andere partij (Verwerkingsverantwoordelijke, Verwerker). Voor meer informatie verwijzen we naar het **Beleid Privacy & Bescherming Persoonsgegevens hoofdstuk 11.4.**
Indien in een onderzoek wordt samengewerkt met andere (externe) onderzoeksinstituten of partijen dan dient er een onderzoeksovereenkomst afgesloten te worden waarin afspraken worden gemaakt over de verdeling van verantwoordelijkheden etc. Hiervoor zijn **modelovereenkomsten** beschikbaar.

Situatie	Verplichte overeenkomst
TiU is Verwerkings-verantwoordelijke en derde partij is Verwerker	Verwerkersovereenkomst conform vastgesteld model. Zie **procedure** en toelichting voor meer informatie Voorbeeld: opslag of bewerking van persoonsgegevens in applicatie die draait in de cloud (bijv. Qualtrics)
TiU is Verwerker voor andere Verwerkings-verantwoordelijke	Verwerkersovereenkomst conform vastgesteld model. Voorbeeld: opdrachtonderzoek waarbij de opdrachtgever het doel en de middelen voor het onderzoek bepaalt en TiU de persoonsgegevens verzamelt en analyseert.
TiU is samen met andere Verwerkings-verantwoordelijke	Afspraken in **onderzoeksovereenkomst** of in aparte overeenkomst over verdeling van verantwoordelijkheden. Denk aan: • Wie regelt de rechten van Betrokkenen (inzage, correctie etc.), wie informeert over de Verwerking (privacy statement) en eventueel een verhaal regeling. • Wat mogen partijen met de gegevens doen en geldt er bijvoorbeeld geheimhouding? Voorbeeld: opdrachtonderzoek waarbij de opdrachtgever samen met TiU het doel en de middelen voor het onderzoek bepaalt.
Afwijken van model verwerkingsovereenkomst	Het verdient in verband met risico's de voorkeur om de standaard model overeenkomst af te sluiten. Toch kan het nodig zijn dat er afgeweken[5] wordt. Indien de onderzoeker wil afwijken van het vastgestelde model dan dient hij dit af te stemmen met de Data Representative van de School. De Data Representative kan om advies vragen bij de werkgroep Data Protectie gecoördineerd door de Functionaris Gegevensbescherming, De verwerkersovereenkomst dient geautoriseerd te worden door een tekeningsbevoegde, dit is meestal de decaan, faculteitsdirecteur of College van Bestuur.
Verantwoordelijk voor totstandkoming en inhoud overeenkomst	De onderzoeker dient voor het afsluiten van de overeenkomst de Data Representative te consulteren. De Data Representative ondersteunt hierbij en kan advies vragen van de Functionaris Gegevensbescherming of Legal Affairs. De Verwerkersovereenkomst dient centraal opgeslagen te worden.

[5] Bij de model overeenkomst is een uitgebreide toelichting geschreven. Hierin staat ook op welke aspecten je eventueel kunt afwijken en wat het risico daarvan is.

Registratie / audit trail	De Verwerkersovereenkomst (inclusief motivatie in geval van afwijking) dient centraal gearchiveerd te worden. Zie voor meer detail **procedure Verwerkersovereenkomst**.

4.5. Schrijven en publiceren van artikel

Bij het schrijven van het artikel moet de onderzoeker voorkomen dat er Herleidbare Persoonsgegevens worden opgenomen in het artikel. Het komt voor dat de onderzoeker wil citeren uit het onderzoek. Dit is mogelijk indien het anoniem kan. Citaten die voortkomen uit Webscraping kunnen herleidbaar (eenvoudig te zoeken op internet) en daardoor niet Anoniem. Bij voorkeur worden deze geparafraseerd. Aandachtspunt is de mogelijkheid dat een combinatie van Persoonsgegevens herleidbaar is naar individuele personen. Denk bijvoorbeeld aan het uitlichten van een manager van een groot ziekenhuis in de regio Eindhoven in de leeftijdscategorie 45 tot 55 jaar.

Persoonsgegevens in artikel	De onderzoeker dient te waarborgen dat er geen Herleidbare Persoonsgegevens opgenomen worden in het artikel door:
	• Onderzoeksresultaten te Anonimiseren / Pseudonimiseren
	• Bij citeren:
	  ○ Anonimiseren;
	  ○ In geval citaat via Webscraping is verkregen: parafraseren.

Data delen ten behoeve van review

Tijdens het publicatieproces kan het voor komen dat data gedeeld dienen te worden met peer-reviewers. Hierbij dienen de Persoonsgegevens vanzelfsprekend zoveel mogelijk beschermd te worden.
Indien er datasets gedeeld worden zonder dat er herleidbare Persoonsgegevens zijn, dan is dit beleid niet van toepassing. Hiervoor gelden de volgende regels:

Data delen met peer reviewers	Indien Persoonsgegevens gedeeld moeten worden met peer reviewers:
	• Indien mogelijk Anonimiseren of Pseudonimiseren (waarbij sleutel niet wordt meegestuurd naar de reviewer). (**paragraaf 4.2).**
	• Indien dit niet mogelijk is:
	  ○ Controleer of er reeds een Verwerkersovereenkomst is afgesloten met de uitgever (zie lijst intranet).
	  ○ Indien er nog geen Verwerkersovereenkomst is: Sluit Verwerkersovereenkomst af met uitgever van het tijdschrift. (**paragraaf 4.3**)
	• Indien ruwe dataset wordt vereist. Aanleveren vrij van Herleidbare Persoonsgegevens.
	• Afspreken (contractueel) dat de dataset na de review procedure vernietigd worden.

4.6. Rechten van respondenten tijdens het onderzoek

Respondenten mogen zich ook tijdens het onderzoek beroepen op een aantal rechten, zie hiervoor **paragraaf 2.10**.

5. ‘NA HET ONDERZOEK’

Dit deel van het beleid beschrijft de elementen van zorgvuldige omgang met data die van belang bij de afronding van elk onderzoek waarin Persoonsgegevens verwerkt worden en de manier waarop Tilburg University juist in deze fase van het onderzoek de zorgvuldige omgang met data waarborgt. Daarbij behandelt dit hoofdstuk achtereenvolgens de bewaartermijnen, de datapackage en de rechten van respondenten.

5.1. Bewaartermijnen

De verzamelde data dienen zorgvuldig bewaard te worden en indien ze niet langer noodzakelijk zijn verwijderd te worden. Hiervoor gelden de volgende regels

Bewaartermijn	• De bewaartermijn van onderzoeksgegevens is minimaal 10 jaar na datum laatste publicatie. Voor medische gegevens geldt een bewaartermijn van minimaal 15 jaar. Zie ook **Regeling Onderzoeksdatamanagement**. • De **direct herleidbare Persoonsgegevens** (voornamelijk contactgegevens en Informed Consent) mogen separaat bewaard blijven zolang noodzakelijk, maar maximaal 10 jaar, en voor medische gegevens maximaal 15 jaar, na datum laatste publicatie[6]. • Er kunnen landelijk discipline specifieke afspraken gemaakt zijn die van deze standaarden afwijken, indien van toepassing zijn deze omschreven in de richtlijnen voor wetenschappelijk onderzoek van de betreffende discipline. • Indien onderzoek niet tot een publicatie heeft geleid is de maximale bewaartermijn van de Herleidbare Persoonsgegevens (zoals contactgegevens en Informed Consent) 15 jaar na afronding onderzoek. Na de maximale bewaartermijn voor de Herleidbare Persoonsgegevens (Informed Consent) dienen deze op een veilige manier vernietigd onder verantwoordelijkheid van de leidinggevende.

5.2. Bewaren data

Het is van belang dat data na afronding van het onderzoek zorgvuldig bewaard worden in lijn met de **Regeling Onderzoeksdatamanagement**. Hiervoor gelden de volgende richtlijnen:

Ruwe data	Na afloop van een onderzoek dienen de ruwe data zorgvuldig bewaard te worden. Dit kan op de servers van TiU of met anderen indien hier een verwerkersovereenkomst mee afgesloten is.
Data package	Alle onderzoeksdata (met uitzondering van Herleidbare Persoonsgegevens) dienen volgens het universitaire **Regeling Onderzoeksdatamanagement** beleid opgenomen te worden in een

[6] Voor wetenschappelijk onderzoek is het van belang dat er verantwoording kan worden afgelegd in het kader van wetenschapsethiek. Hiervoor is het van belang dat inzichtelijk is met welke Respondenten is gewerkt. In verband met minimale bewaartermijn voor wetenschappelijk onderzoek, is maximale bewaartermijn van informed consent formulieren hieraan gerelateerd.

	data package. De data package (inclusief analysebestanden en andere relevante gegevens) wordt voorzien van een volledige metadatering en daarna opgeslagen in een Trusted Digital Repository (TDR). DataverseNL, met indien gewenst een koppeling naar DANS EASY. Indien een onderzoeker **een andere TDR** wil gebruiken en er Persoonsgegevens in de dataset aanwezig zijn, zijnde geen Herleidbare Persoonsgegevens, dient hiertoe een **Verwerkersovereenkomst** afgesloten te worden met de aanbieder van de TDR.

5.3. Rechten van respondenten na afloop het onderzoek

Respondenten mogen zich ook tijdens het onderzoek beroepen op een aantal rechten, zie hiervoor **paragraaf 2.10**.

BIJLAGE 1: Soorten datasets

Audio- en video opnames

Audio en video opnames worden regelmatig gebruikt bij wetenschappelijk onderzoek. Soms zullen deze opnames te anonimiseren zijn, bijvoorbeeld door blurren van gezichten, of alleen filmen van handen, maar dit is sterk afhankelijk van het doel van het onderzoek.
Opnames kunnen gebruikt worden voor presentaties of publicaties (bijvoorbeeld bij onderwijs) en het is van belang dat de Respondent hierover goed geïnformeerd is en toestemming geeft.

Informeren en toestemming van Respondenten	• Betrokkene wordt vooraf duidelijk geïnformeerd over het maken van opname door middel van informed consent. • Betrokkene vooraf goed geïnformeerd wordt over eventueel gebruik van opnames voor presentaties en publicaties en hier specifiek toestemming voor geeft.
Gebruik audio of video data	In geval van audio – of video opnames bij wetenschappelijk onderzoek is het van belang dat de Onderzoeker alleen Persoonsgegevens verzamelt die noodzakelijk zijn voor het doel van het wetenschappelijk onderzoek, maar wel voldoende Persoonsgegevens verzameld om de vraagstelling van het onderzoek te beantwoorden. Vastlegging van onderzoeksresultaten gebeurt indien mogelijk (voor het doel van het onderzoek) te voldoen aan onderstaande richtlijn. • Geen vermelding van namen (of deze later 'maskeren') • Geen gezichten filmen indien dit niet noodzakelijk is (bijvoorbeeld alleen handbewegingen). Het is in verband met integriteitsrichtlijnen wel van belang dat de data controleerbaar is bijv. wie heeft deelgenomen aan het onderzoek. Dit kan door te Pseudonimiseren, in de vorm van communicatie-/ koppelbestand en de informed consent formulieren. **Let op**: indien stem van Respondent herkenbaar is dan is dit nooit Geanonimiseerd maar Gepseudonimiseerd, het is immers herleidbaar naar persoon.

Interviews en observaties, experimenten in LABS

Van interviews en observaties worden vaak door onderzoekers verslagen gemaakt. Bij sommige onderzoeken worden experimenten met proefpersonen gedaan in labs. Soms worden hierbij Bijzondere Persoonsgegevens gemeten bijvoorbeeld bloeddrukmeting om te zien of er sprake is van stress.

Het is van belang dat hier zo veel mogelijk vermeden wordt dat er direct Herleidbare Persoonsgegevens worden opgenomen (bijvoorbeeld namen).

Informeren en toestemming van Respondenten	Betrokkene vooraf duidelijk geïnformeerd wordt over het doel en de wijze van wetenschappelijk onderzoek door middel van informed consent. Indien het vooraf informeren vanwege het doel van het onderzoek niet wenselijk is (bijvoorbeeld onderzoek naar etnische discriminatie) dan mag informatie in informed consent algemeen zijn. Bij debriefing van het onderzoek dient deze informatie echter wel (achteraf) verstrekt te worden.
Administratieve afhandeling	Het komt voor dat deelnemers aan LABS of Respondenten betaald worden voor een deelname van een onderzoek. In dit geval wordt voor de betaling Persoonsgegevens verwerkt (onderbouwing financiële administratie. Dit betreft een Verwerking van Persoonsgegevens en derhalve dient dit proces vastgelegd te worden in het Verwerkingsregister (niet verbijzonderd per onderzoek) door F&C.
Interviews observaties, en experimenten	In geval van interviews en observaties bij wetenschappelijk onderzoek is het van belang dat de vastlegging (uitwerking) hiervan voldoet aan de onderstaande richtlijn: • Niet vermelden van namen of andere herleidbare Persoonsgegevens bij vastlegging van het interview en de observaties of de lab resultaten. Het is in verband met integriteitsrichtlijnen wel van belang dat de data controleerbaar is bijv. wie heeft deelgenomen aan het onderzoek. Dit kan door te Pseudonimiseren, in de vorm van communicatie-/ koppelbestand en de informed consent formulieren. **Let op**: bij verwerking van Bijzondere Persoonsgegevens gelden aanvullende eisen aan beveiliging. Zie hiervoor **hoofdstuk 9 Beleid Privacy & Bescherming Persoonsgegevens** en **paragraaf 4.2** inzake bijzondere Persoonsgegevens bij wetenschappelijk onderzoek.

Eye tracking

Bij sommige wetenschappelijke onderzoeken (zoals bijvoorbeeld naar hoe personen naar websites kijken) wordt gebruik gemaakt van eye-tracking om de oogbewegingen te volgen. Afhankelijk van de wijze waarop deze Eye tracking wordt vastgelegd kan er sprake zijn van een verhoogd privacy risico voor Betrokkene. Dit is het geval indien er sprake is van een iris-scan, omdat een irisscan gebruikt wordt als identificatiemiddel (en daarmee risico op identiteitsfraude groot is voor Respondent.

Informeren en toestemming van Respondenten	Betrokkene vooraf duidelijk geïnformeerd wordt over de wijze en het doel van het onderzoek door middel van informed consent.
Eye tracking	In geval van Eye tracking bij wetenschappelijk onderzoek is het van belang dat: • Alleen oogbeweging gevolgd wordt, hierbij dient de iris niet gefotografeerd of gescand te worden in verband met verhoogd Privacy Risico van Betrokkene.

Medische screening (MRI/EEG/ECG….)

Bij een aantal wetenschappelijke onderzoeken wordt gebruik gemaakt medische screening zoals MRI, EEG en ECGs. Dit zijn Bijzondere Persoonsgegevens. Hiervoor gelden de volgende richtlijnen:

Informeren en toestemming van Respondenten	Betrokkene vooraf duidelijk geïnformeerd wordt over de wijze en het doel van het onderzoek door middel van Informed Consent.
Medische screening EEG ECG MRI etc	In geval van gebruik van medische gegevens worden bijzondere Persoonsgegevens verwerkt waarvan het van belang dat vastlegging (uitwerking) hiervan voldoet aan de onderstaande richtlijn: • Niet vermelden van namen of andere herleidbare persoonsgegevens bij vastlegging van de MRI/ EEG of ECG Het is in verband met integriteitsrichtlijnen wel van belang dat de data controleerbaar is wie heeft deelgenomen aan het onderzoek. Dit kan door te Pseudonimiseren, in de vorm van communicatie-/ koppelbestand en de Informed Consent formulieren. **Let op**: bij verwerking van Bijzondere Persoonsgegevens gelden aanvullende eisen aan beveiliging. Zie hiervoor **hoofdstuk 9 Beleid Privacy & Bescherming Persoonsgegevens** en **paragraaf 2.4** inzake bijzondere Persoonsgegevens bij wetenschappelijk onderzoek.

Wearables

Indien bij een wetenschappelijk onderzoek gebruikt wordt gemaakt van zogenaamde wearables (bijvoorbeeld fitbit) dan gelden de volgende richtlijnen.

Informeren en toestemming van Respondenten	Betrokkene vooraf duidelijk geïnformeerd wordt over de wijze en het doel van het onderzoek door middel van informed consent.
Wearables	In geval van gebruik van wearables bij wetenschappelijk onderzoek is het van belang dat vastlegging (uitwerking) hiervan voldoet aan de onderstaande richtlijn: • Niet vermelden van namen of andere herleidbare persoonsgegevens bij vastlegging van de resultaten van de wearables Het is in verband met integriteitsrichtlijnen wel van belang dat de data controleerbaar is met wie de onderzoek is uitgevoerd. Dit kan door te Pseudonimiseren, in de vorm van communicatie-/ koppelbestand en de Informed Consent formulieren. **Let op**: bij verwerking van Bijzondere Persoonsgegevens gelden aanvullende eisen aan beveiliging. Zie hiervoor **hoofdstuk 9 Beleid Privacy & Bescherming Persoonsgegevens** en **paragraaf 4.2** inzake bijzondere Persoonsgegevens bij wetenschappelijk onderzoek.

BIJLAGE 2: Verantwoordelijkheden (RASCI)

RASCI matrix for Research projects

Task	Sub	Deliverable	Accountable	Responsible	Supportive	Consulted	Informed
Monitoring upcoming law and legislation		See general RASCI in Beleid Privacy & Bescherming Persoonsgegevens					
Definition of Data Protection Strategy		See general RASCI in Beleid Privacy & Bescherming Persoonsgegevens					
Definition TiU Data Protection Regulation		See general RASCI in Beleid Privacy & Bescherming Persoonsgegevens					
Definition TiU Research Data Management Regulation		TiU Research Data Management Regulation	Executive Board	• Taskforce Data Protection • Director LIS • Research Data Office (RDO)	• Data Protection Officer (DPO) • CISO and ITSO	• POZ • Scientific/Ethical committee	• Researchers • Research Support teams (RST)
Define Pre-Data Protection Impact Assessment		Pre-DPIA	Dean	Researcher	Data Representative (DR)		
Define Data Management Plan (including DPIA assessment[7])		Data Management Plan	Dean	Researcher	Data Representative (DR)	Scientific/ ethical committee	Data Protection Officer if DPIA is necessary
Execution DPIA		Research Data Protection Impact Assessment	Dean	Researcher	Data Representative (DR)	Data Protection Officer (DPO)	Data Protection Officer (DPO)
Close Data Processing Agreement	Standard model	Data processing agreement	Dean	Researcher	Data Representative (DR)		Data Protection Officer (DPO)
	Adjusted standard model		Dean	Researcher	Data Representative (DR)	• Data Protection Officer (DPO) • Legal Affairs (only mandatory in case	Data Protection Officer (DPO)

[7] In the datamanagement plan an assessment must be made whether a DPIA is required / mandatory.

Task	Sub	Deliverable	Accountable	Responsible	Supportive	Consulted	Informed
						of authorization by the Executive Board). • Security: • Chief Information Security Officer (CISO) and IT Security Officer (ITSO)	
	Supplier version (exceptional)		Dean	Researcher	Data Representative (DR)	• Data Protection Officer (DPO) • Legal Affairs (only mandatory in case of authorization by the Executive Board). • Security : CISO and ITSO	Data Protection Officer (DPO)
Register Data processing for research project	Special category of personal data	Record of Processing Activities	Dean	Researcher	Data Representative (DR)	Data Protection Officer (DPO)	
	Special circumstances		Dean	Researcher	Data Representative (DR)	Data Protection Officer (DPO)	
	Major personal data		Dean	Researcher	Data Representative (DR)	Data Protection Officer (DPO)	
	Other		Dean	Researcher	Data Representative (DR)		Data Protection Officer (DPO)
Advice regarding Data Protection research	Contractual Agreements	Advise	Legal Affairs	Legal Affairs	Data Protection Officer (DPO)		

Task	Sub	Deliverable	Accountable	Responsible	Supportive	Consulted	Informed
	Research projects	Advise	Data Representative (DR)	Data Representative (DR)	• Data Protection Officer (DPO) • Research Data Office		
Report Research data breaches or incidents		Reported incident/ data breach	Researcher	Researcher		Data Protection Officer (DPO)	Taskforce Data Protection
Analyze data breaches and report (if necessary) to AP		See general RASCI in General Policy Privacy & Data Protection.					
Raise Awareness		Awareness – knowledge data protection	Dean	Data Representative (DR)	• Data Protection Officer (DPO) • Legal Affairs • Research Data Office (RDO)		
Organize Research Data Protection Training and Education		Training and awareness	Dean	Research Data Office (RDO)	• Data Representative (DR) • Data Protection Officer (DPO) • Legal Affairs		
Monitoring and checks on compliance to law and legislation for research projects		See general RASCI in General Policy Privacy & Data Protection.					

BIJLAGE 3: Definities

Begrip	Definitie
Anonimiseren / Anonieme gegevens	Gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op Persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is (bijvoorbeeld voor statistische of onderzoeksdoeleinden)
Betrokkene	een geïdentificeerde of identificeerbare natuurlijke persoon op wie een persoonsgegeven betrekking heeft. Wordt bij wetenschappelijk onderzoek respondent genoemd.
Bijzondere Persoonsgegevens of bijzondere categorieën van Persoonsgegevens	Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid
Biometrische gegevens	Persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedrag gerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens
Datalek (ook wel: "Inbreuk in verband met Persoonsgegevens")	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens
Derde	Ieder ander, niet zijnde betrokkene, verwerkings-verantwoordelijke, verwerker, noch enig persoon die onder rechtstreeks gezag van verwerkingsverantwoordelijke of verwerker gemachtigd is om de Persoonsgegevens te verwerken
Data Protection Impact Assessment (DPIA) of Privacy Impact Assessment (PIA)	Een beoordeling van het effect van de beoogde verwerkingsactiviteiten op de bescherming van Persoonsgegevens die helpt bij het identificeren van privacy risico's en handvaten geeft om de risico's te verkleinen tot een acceptabel niveau. Wordt in de AVG Gegevensbeschermingseffectbeoordeling genoemd.
Herleidbaar Persoonsgegeven	Alle persoonsgegevens die leiden tot een identificeerbar persoon. Dit kunnen unieke persoonsgegevens zijn (zoals bijvoorbeeld BSN nummer) maar ook een combinatie van persoonsgegevens (bijvoorbeeld naam in combinatie met adres)
Identiteitsdocument	De wettige identiteitsbewijzen (paspoort, Nederlandse identiteitskaart, ID-kaart of paspoort uit een EER-land of een Nederlands vreemdelingendocument). Bij TiU kunnen medewerkers en studenten zich ook identificeren met een rijbewijs en de TiU-kaart met pasfoto.
Informed consent	Toestemmingsformulier waarmee de Respondent duidelijk geïnformeerd wordt over o.a. de inhoud van het wetenschappelijk onderzoek, zijn rechten

Persoonsgegeven	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, voornamelijk aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon
Pseudonimiseren	Het verwerken van Persoonsgegevens op zodanige wijze dat de Persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de Persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld
Recht op beperking van de Verwerking	Het recht op beperking houdt in dat de Persoonsgegevens (tijdelijk) niet verwerkt mogen worden en niet gewijzigd mogen worden. Het feit dat de verwerking van de Persoonsgegevens beperkt is, moet door de verwerkingsverantwoordelijke duidelijk in het bestand zijn aangegeven zodat dit ook duidelijk is voor ontvangers van de Persoonsgegevens. Wanneer de beperking weer wordt opgeheven, moet de betrokkene hiervan op de hoogte worden gebracht. (artikel 18 AVG)
Recht van bezwaar	Een betrokkene kan vanwege redenen die verband houden met zijn specifieke situatie gebruik maken van dit recht van bezwaar (dat niet vergelijkbaar is met bezwaar op grond van de Awb) tegen de verwerking van hem betreffende Persoonsgegevens, als voldaan aan de in de verordening genoemde eisen. Als een betrokkene bezwaar maakt staakt de verwerkingsverantwoordelijke de verwerking, tenzij dwingende gerechtvaardigde gronden anders bepalen. (artikel 21 AVG)
Recht op dataportabiliteit / overdraagbaarheid	Dit recht houdt in dat een betrokkene de gegevens van een verwerkingsverantwoordelijke moet kunnen verkrijgen in gestructureerde, gangbare en machine-leesbare vorm en het recht heeft deze gegevens aan een andere verwerkingsverantwoordelijke over te dragen of rechtstreeks te laten overdragen, zonder daarbij te worden gehinderd tenzij dit afbreuk doet aan rechten en vrijheden van anderen. Een betrokkene heeft recht op overdraagbaarheid voor zover het gaat om door hem zelf verstrekte gegevens. (artikel 20 AVG)
Recht op gegevenswissing / vergetelheid	De verwerkingsverantwoordelijke is verplicht Persoonsgegevens van de betrokkene zonder onredelijke vertraging te wissen, onder andere indien Persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt; de betrokkene zijn toestemming intrekt en er geen andere rechtsgrond voor verwerking bestaat; betrokkene bezwaar maakt tegen de verwerking; de Persoonsgegevens onrechtmatig verwerkt zijn.(artikel 17 AVG)
Recht op informatie	Een betrokkene moet op de hoogte worden gesteld van het feit dat verwerking van zijn Persoonsgegevens plaatsvindt of zal plaatsvinden en wat de doeleinden hiervan zijn. De AVG geeft aan welke informatie in ieder geval verstrekt moet worden, bijvoorbeeld informatie over de periode, de rechten van betrokkene, de bron van gegevens en de juridische grondslag voor de verwerking. Verandert het doel van de verwerking, dan moet ook daarover informatie worden verstrekt. (artikel 13-14 AVG)

Recht op inzage	Betrokkenen hebben het recht te weten of hun betreffende Persoonsgegevens worden verwerkt door de verantwoordelijke. De AVG bevat een opsomming van de informatie waarvoor het recht van inzage geldt. De verwerkingsverantwoordelijke moet betrokkene een kopie verstrekken van de Persoonsgegevens die worden verwerkt. (artikel 15 AVG)
Recht op rectificatie	Betrokkene heeft recht op rectificatie van hem betreffende onjuiste Persoonsgegevens dan wel het recht een aanvullende verklaring te verstrekken wanneer de verwerking plaatsvindt op basis van onvolledige gegevens. De rectificatie moet meteen plaatsvinden. De verwerkingsverantwoordelijke is verplicht iedere ontvanger aan wie Persoonsgegevens zijn verstrekt in kennis te stellen van elke rectificatie, tenzij dit onmogelijk is of onevenredig veel inspanning vraagt. (artikel 16 AVG).
Respondent	is natuurlijk persoon dat een bijdrage levert aan het onderzoek. Betreft in de AVG degene die Betrokkene wordt genoemd.
Toestemming (van de betrokkene)	Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van Persoonsgegevens aanvaardt (artikel 4 onder 11 AVG)
Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke Persoonsgegevens verwerkt
Verwerkers-overeenkomst	De overeenkomst tussen een verwerkingsverantwoordelijke en verwerker waarin afspraken worden gemaakt over de verwerking van Persoonsgegevens ter waarborging van de gegevensbescherming van betrokkenen (artikel 28 lid 3 AVG).
Verwerking	Een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens
Verwerkingsgrondslag	Een grondslag voor de verwerking zoals limitatief opgenomen in artikel 6 AVG (bijvoorbeeld: toestemming of wettelijke verplichting).
Verwerkingsregister	Het register van de verwerkingsactiviteiten als bedoeld in artikel 30 AVG waarin een aantal gegevens worden vastgelegd ten behoeve van de verantwoordingsplicht.
Verwerkings-verantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van Persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lid statelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen
Webscraping	een computertechniek waarbij software wordt gebruikt om informatie van webpagina's te extraheren en al dan niet te analyseren. Meestal probeert de software een deel van het world wide web te onderzoeken via gebruik van het op codes gebaseerde Hypertext Transfer Protocol (HTTP), of door het surfgedrag met een webbrowser te simuleren