FAQ ALGEMENE VERORDENING GEGEVENSBESCHERMING EN WETENSCHAPPELIJK ONDERZOEK

Versie november 2018

Introductie

Deze FAQ heeft tot doel om jou als onderzoeker op een beknopte wijze te informeren over het toepassingsgebied en de eisen van de Algemene Verordening Gegevensbescherming in het kader van wetenschappelijk onderzoek.

Inhoudsopgave

1 ALGEMENE INFORMATIE

In dit deel wordt het kader beknopt geschetst en overlopen we een aantal basisbegrippen die aan bod komen in de AVG. Deze wet stelt een aantal verplichtingen waar organisaties en onderzoekers aan moeten voldoen. Op de hoogte zijn van deze informatie is ook voor onderzoekers van groot belang: om de wet niet te overtreden, om recht te doen aan de fundamentele rechten van iedereen die betrokken is bij wetenschappelijk onderzoek en om ervoor te zorgen dat verzamelde data niet vernietigd hoeft te worden.

1.1 Wat is de Algemene Verordening Gegevensbescherming (AVG) of General Data Protection Regulation (GDPR)

De AVG is een nieuwe Europese privacy- en databeschermingswet die van kracht is sinds 25 mei 2018. De AVG zorgt voor een modernisering van de wetgeving rond privacy, creëert een uniform Europees wetgevend kader en geeft burgers verschillende rechten op het vlak van de verwerking van hun persoonsgegevens. De AVG stelt ook eisen aan organisaties die gegevens verwerken, op het gebied van bijvoorbeeld de informatie die hierover bekend gemaakt moet worden, de rechtmatigheid van het gebruik van verschillende gegevens en de beveiliging van deze gegevens.

Een belangrijke wijziging voor de verwerking van persoonsgegevens is dat elke organisatie nu zelf een register moet bijhouden van verwerkingen, waar vroeger een aangifteplicht bestond bij de Privacycommissie. Dit betekent dus ook dat de universiteit op de hoogte moet zijn van de vele verschillende manieren waarop onderzoekers omgaan met persoonsgegevens in het kader van hun werkzaamheden.

1.2 Wanneer is de AVG van toepassing op mijn onderzoek?

- Wanneer jij (of jouw organisatie) **persoonsgegevens verwerkt** in het kader van wetenschappelijk onderzoek (dwz. verzamelen, opslaan, ordenen, (her)structureren, corrigeren, opvragen, raadplegen etc.)
- Wanneer jij (of jouw organisatie) als **verantwoordelijke** valt aan te merken
- Wanneer jij of de onderzoeksobjecten zich **in de EU** bevinden.

1.3 Wat zijn persoonsgegevens?

Persoonsgegevens zijn alle informatie over natuurlijke personen op basis waarvan deze kunnen worden geïdentificeerd. Naast gegevens met voor de hand liggende 'identificatiegegevens', zoals naam en geboortedatum, omvat dit ook genetische, biometrische, locatie en online gegevens die uniek zijn voor een persoon (zoals een e-mailadres of IP-adres). Daarnaast kan ook een combinatie van variabelen ervoor zorgen dat personen geïdentificeerd kunnen worden.

Gevoelige persoonsgegevens/bijzondere categorieën van persoonsgegevens zijn persoonsgegevens die informatie bevatten over ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens, gegevens over gezondheid, gegevens over iemands seksueel gedrag of seksuele gerichtheid. Wanneer dit type gegevens verwerkt wordt, dient de onderzoeker aan strengere voorwaarden te voldoen, omdat het kenbaar worden van deze informatie (bv. als gevolg van een datalek, of door het onzorgvuldig delen van onderzoeksgegevens) zeer nadelige gevolgen kan hebben voor de betrokkenen.

Gepseudonimiseerde persoonsgegevens (in de Belgische Privacywetgeving van 1992 aangeduid als 'gecodeerde gegevens') zijn persoonsgegevens (al dan niet gevoelig) die slechts door middel van een niet-publieke sleutel in verband kunnen gebracht worden met een geïdentificeerde of identificeerbare persoon. Gepseudonimiseerde persoonsgegevens blijven persoonsgegevens die beschermd worden door de AVG. Gecodeerde gegevens zijn dus iets anders dan geanonimiseerde gegevens.

Bij **geanonimiseerde persoonsgegevens** werd door middel van een verwerkingstechniek de mogelijkheden tot identificatie 'irreversibel' verwijderd. Dit wil dus zeggen dat, in het geval van codering, zelfs de onderzoeker zelf niet langer toegang heeft tot de sleutel of op een andere wijze individuen zou kunnen herkennen of achterhalen. Wanneer sprake is van (werkelijk) anonieme gegevens, is de AVG niet van toepassing. (Anonieme gegevens betreft informatie die niet in verband kan gebracht worden met een geïdentificeerde of identificeerbare persoon. Anonieme gegevens zijn dus geen persoonsgegevens en vallen dus niet onder de bepalingen van de AVG. Let op: er kunnen altijd nog andere wetten dan de AVG van toepassing zijn.)

Opgepast, geanonimiseerde persoonsgegevens die met een redelijke inspanning terug te leiden zijn naar de oorspronkelijke individuen, blijven persoonsgegevens en zijn geen anonieme gegevens en vallen dus wel onder de AVG. Om die reden is het voor heel wat types onderzoeksdata (bv. kwalitatieve data) moeilijk om deze volledig te anonimiseren. Er moet dus zeer terughoudend worden omgesprongen met de term 'geanonimiseerde gegevens': vaak is dit *niet* het geval.

1.4 Wat wordt beschouwd als kwetsbare groepen?

Het invullen van het begrip 'kwetsbare personen' is sterk afhankelijk van de context van het onderzoek, minderheden wordt dan ook in zeer ruime zin begrepen. Hierbij kan de vraag gesteld worden of (het verwerken van) de informatie risico's oplevert voor de betrokkene wanneer deze kenbaar wordt voor anderen. Voorbeelden van kwetsbare personen zijn: minderjarigen, zwangere vrouwen, oudere personen, andersvaliden, etnische minderheden en LGBTQ+-minderheden, al hangt het antwoord op de vraag vaak af van de context. Om deze reden kan het verwerken van persoonsgegevens van kwetsbare personen of groepen aanleiding geven tot een risicoanalyse (zie 2.5). Daarnaast zal dit ook gevolgen hebben voor de manier waarop informatie wordt verstrekt (zie 4.1) en toestemming wordt verkregen (zie 4.2).

1.5 Wat zijn de basisprincipes van de AVG?

De AVG is gebaseerd op zes basisprincipes die nageleefd moeten worden wanneer persoonsgegevens verwerkt worden:

- **Rechtmatigheid, behoorlijkheid en transparantie**: persoonsgegevens worden verwerkt op een transparante manier met respect voor alle wetten, reglementen en regels die van toepassing zijn
- **Doelbinding** (finaliteit en proportionaliteit): persoonsgegevens worden enkel verwerkt voor het onderzoeksdoel en de verwerking is redelijk en proportioneel voor het bereiken van het doel van het onderzoek
- **Minimale gegevensverwerking**: enkel die persoonsgegevens worden gebruikt die noodzakelijk zijn voor het bereiken van de doelstellingen van het onderzoek
- **Juistheid**: de persoonsgegevens die verwerkt worden, moeten accuraat zijn
- **Opslagbeperking**: persoonsgegevens mogen niet langer dan nodig bewaard worden voor het huidig onderzoek of voor mogelijke verdere analyses op de data (zie ook 5.1)
- **Vertrouwelijkheid en integriteit**: onderzoekers moeten op een confidentiële manier omgaan met persoonsgegevens en de gepaste maatregelen nemen om de vertrouwelijkheid en integriteit van deze gegevens te garanderen

Als algemeen principe geldt daarnaast ook de **zelfverantwoordingsplicht.** Hiervoor is het belangrijk om jezelf volgende vragen te stellen: heb ik aan de start van mijn onderzoek de privacyaspecten van mijn onderzoek grondig overwogen en gedocumenteerd en ben ik in staat om aan te tonen dat ik op een actieve manier verantwoordelijkheid heb genomen om de verwerking van persoonsgegevens op een veilige manier te laten gebeuren.

1.6 Wat is er nieuw in de AVG?

Hoewel de basisprincipes van de vorig privacywetgeving dezelfde blijven, brengt de AVG een aantal belangrijke veranderingen en verplichtingen met zich mee:

- De vroegere "aangifteplicht" werd vervangen door een "zelfverantwoordingsplicht" waarbij onderzoekers in een **register** van de instelling moeten melden dat ze werken met persoonsgegevens
- Het aanstellen van een **functionaris voor gegevensbescherming** of data protection officer aan de instelling is verplicht gesteld voor organisaties die veel data verwerken (waaronder universiteiten)
- het uitvoeren van een **risico-analyses** (gegevensbeschermingseffectbeoordeling) voor verwerkingen met een hoog risico (bv. verwerking van gevoelige data, profiling, systematisch monitoring, combineren van datasets, gebruik van nieuwe technologieën,…)
- Het voldoen aan hogere eisen voor dataveiligheid door gebruik te maken van encryptie en **pseudonimisering**
- voldoen aan de nieuwe, strengere normen voor **informed consent**
- Het op een duidelijke en transparante wijze bekend maken van de **wettelijke rechtsgrond** voor de verwerking van persoonsgegevens aan de betrokkenen
- De verplichte melding van **datalekken** van persoonsgegevens aan de Gegevens-beschermingsautoriteit (GBA) binnen de 72 uur.
- voldoen aan de **nieuwe regels voor de transfer van persoonsgegevens buiten de Europese Economische Ruimte (EER)**
- De Gegevensbeschermingsautoriteit krijgt de mogelijkheid om **controles** uit te voeren en boetes uit te schrijven. Deze boetes kunnen zowel administratieve boetes omvatten als (persoonlijke) strafsancties
- **Uitbreiding van de rechten van de betrokkenen** zoals "het recht op inzage" en, onder voorwaarden, "het recht om vergeten te worden" en het recht op overdraagbaarheid van gegevens

1.7 Waarom is het belangrijk om mij aan de AVG te houden?

Voldoen aan de nieuwe vereisten voor onderzoek is om verschillende redenen belangrijk:

- Zorgvuldige en ethische omgang met data vergroot de **kwaliteit en de betrouwbaarheid van het onderzoek** en de onderzoeksresultaten
- Een goede en ethische omgang met data kan het **vertrouwen van burgers en onderzoeksobjecten** in de wetenschap vergroten
- Een schending van de wet kan leiden tot **reputatieschade** en negatieve media aandacht voor de instelling, betrokken onderzoekers en de academische gemeenschap als geheel
- Een schending van de wettelijke regels kan leiden tot **boetes** die kunnen oplopen tot 20 miljoen euro

- Vaak wordt de conformiteit met AVG expliciet opgelegd door **opdrachtgevers** (bv. Horizon 2020, ERC, FWO)
- Bij het indienen van publicaties vragen **tijdschriften** ook steeds vaker naar conformiteit met AVG.
- Als primaire data op een correcte wijze verzameld zijn, geeft dit ook rechtszekerheid om deze als **secundaire data** eventueel te gebruiken in verdere analyses. Gegevens die niet conform de AVG zijn verwerkt, kunnen onrechtmatig zijn waardoor ze verwijderd moeten worden.

2 HET ONDERZOEKSDESIGN

De vragen in dit deel moeten aan bod komen op het moment dat je als onderzoeker of promotor het onderzoeksdesign aan het uitwerken bent. Door in deze fase al een aantal basisvragen te overlopen en te beantwoorden, zorg je als onderzoeker ervoor dat er bij de start van het onderzoek geen onverwachte problemen opduiken die ultiem kunnen leiden tot het niet kunnen uitvoeren van het onderzoek omwille van het niet conform zijn met de AVG (zoals het niet kunnen publiceren van je onderzoek of het moeten verwijderen van je data).

2.1 Waaraan moet ik denken bij het design van mijn onderzoek?

Naast de inhoudelijke en methodologische aspecten van je onderzoek is het belangrijk om in de ontwerpfase ook de verzameling en de verwerking van persoonsgegevens grondig te overwegen en te beschrijven ("*privacy by design"*). Dit kadert ook binnen onderzoeksdatamanagement in brede zin.

- Heb ik persoonsgegevens nodig? Als dit niet noodzakelijk is, dan gebruik je best anonieme gegevens.
- Hoe minimaliseer ik deze gegevens? Probeer de gegevens te beperken tot die data die bijdragen tot het beantwoorden van de onderzoeksvraag.
- Gaat het om gegevens die ik zelf verzameld heb (primaire data) of bestaande gegevens uit ander wetenschappelijke onderzoek of uit bestaande databanken (bv. patiëntengegevens, Kruispuntbank, etc.) (verder verwerking, zie 2.3)
- Heb ik bij de verwerking ruwe persoonsgegevens nodig of kan ik na verzameling werken met gepseudonimiseerde gegevens? (Op welk punt kan ik welke gegevens pseudonimiseren?)
- Houdt de manier waarop ik persoonsgegevens verwerk risico's in voor de betrokkenen? Bv. verzamel ik gevoelige persoonsgegevens, verzamel ik persoonsgegevens bij kwetsbare groepen, is er sprake van systematische monitoring,… (zie 2.5)?
- Op welke rechtsgrond kan ik mij baseren om persoonsgegevens te mogen verwerken (zie 2.2)?
- Worden de persoonsgegevens gedeeld met andere personen buiten mijn instelling? Wat zijn de rollen van deze instellingen (zie 2.8) en zijn de nodige contracten hiervoor in orde?
- Werk ik samen met instellingen of organisaties van buiten de EER (zie 2.7)?

2.2 Hoe zorg ik ervoor dat de verwerking van persoonsgegevens rechtmatig gebeurt?

De verwerking van persoonsgegevens is alleen rechtmatig indien aan één van de zes rechtsgronden die vermeld worden in de AVG is voldaan.

Voor het wetenschappelijk onderzoek zijn volgende drie voornamelijk van belang:

1. De betrokkene heeft hiervoor **toestemming** gegeven (*informed consent*). Daarvoor is het nodig dat de betrokkene begrijpt waarvoor toestemming wordt gegeven en dat dit vrijwillig gebeurt.

2. De verwerking is noodzakelijk voor de **vervulling van een taak van algemeen belang**. Wetenschappelijk onderzoek kan als een taak van een algemeen belang worden gezien, maar hierbij moet worden gelet op verschillende zaken, zoals de vraag of het onderzoek plaatsvindt in het uitvoeren van een publieke taak, of er voor het kiezen van deze grondslag een wettelijke basis gevonden kan worden, en welke belangen het onderzoek dient. Lang niet ieder onderzoek dat plaatsvindt, kan onder deze noemer geschaard worden: de data protection officer voorziet je hierover graag van advies (dpo@vub.be).

3. De verwerking is noodzakelijk voor de **behartiging van de rechtvaardige belangen van de verwerkingsverantwoordelijke** of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

De andere drie rechtsgronden zijn de contractuele basis, wettelijke verplichting of vitaal belang. In de context van wetenschappelijk onderzoek zijn deze minder relevant.

Aan de start van het onderzoek is het belangrijk om grondig te overwegen welke van deze rechtsgronden het meest geschikt is. Het is ook mogelijk dat er meer dan één grondslag kan geïdentificeerd worden. In dit geval is het een goed idee om deze allemaal te documenteren.

Aangezien onderzoekers om ethische redenen bij het verzamelen van gegevens bij respondenten reeds een **geïnformeerde toestemming** moeten bekomen, is het in veel onderzoeksprojecten mogelijk om deze toestemming ook te gebruiken als legitieme grondslag voor het verwerken van persoonsgegevens. Als onderzoeker moet je er wel rekening mee houden dat deze toestemming in het kader van de GDPR aan een aantal voorwaarden moet voldoen om geldig te zijn (zie ook 4.2).

Toestemming is echter niet de enige manier om persoonsgegevens op een rechtmatige manier te verwerken. Zo kan je als onderzoekers ook het **vervullen van een taak van algemeen belang** of het **behartigen van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke** gebruiken als legitieme grondslag. Hierbij moet het wel duidelijk zijn dat deze rechtsgrond te verantwoorden valt voor het type onderzoek. Een tegenindicatie voor algemeen belang is dat het onderzoek niet gefinancierd is met publieke middelen, de resultaten niet of beperkt publiek gemaakt worden, of dat de resultaten worden overgemaakt aan een andere partij. De grondslag voor gegevensverwerking is niet algemeen belang indien de verworven kennis louter bedoeld is voor private belangen. De grondslag voor de gegevensverwerking is evenmin algemeen belang indien er industriële of commerciële belangen spelen.

Bv. Een rapport wordt geschreven in opdracht van een derde partij, het wordt overgemaakt en niet publiek gemaakt. Dit dient het private belang van de derde partij.

2.3 Wat moet ik doen bij een verdere verwerking van persoonsgegevens?

Naast een nieuwe verzameling van persoonsgegevens noemt de AVG nadrukkelijk de mogelijkheid van het ‘verdere verwerken’ van gegevens, die eerder zijn verzameld, voor wetenschappelijk onderzoek. Dit betekent het verwerken van de gegevens voor een ander doel dan waarvoor ze oorspronkelijk verzameld of verwerkt zijn. De vraag die hier centraal staat, is of de ‘verdere verwerking’ verenigbaar is met het doel van de verwerking van de oorspronkelijke verwerking.
n.b. Persoonsgegevens die je zelf verzameld hebt onder een bepaalde noemer, en die je vervolgens zelf in een ander onderzoek wil gaan verwerken, kunnen dus ook vallen onder de definitie van ‘verder verwerken’ van gegevens van de AVG.
(bv. In het kader van Onderzoek 1 heb je middels enquêtes gegevens verzameld van respondenten. Deze gegevens wil je nu gebruiken in Onderzoek 2. Voor dit ‘hergebruik’ moet ook een juridische

grondslag bestaan en als deze 'verdere verwerking' verenigbaar is met de doelstellingen die tijdens Onderzoek 1 aan de respondent zijn verteld.)

Het is hierbij belangrijk om grondig te evalueren of de verwerking van persoonsgegevens (in het kader van een nieuw onderzoeksproject of een nieuwe onderzoeksvraag) verenigbaar is met de doeleinden waarvoor de gegevens oorspronkelijk verzameld werden. We raden je aan om de informatie die bezorgd werd aan de betrokkenen en eventueel de geïnformeerde toestemming van de betrokkenen grondig na te lezen. Bij twijfel kunnen ook de ethische commissies een belangrijke rol spelen in deze beoordeling.

Ook bij een verdere verwerking van persoonsgegevens blijft het belangrijk om transparant te zijn naar de betrokkenen. Zo moeten de betrokken ook bij een verdere verwerking van hun persoonsgegevens over deze nieuwe verwerking geïnformeerd worden (zie 4.1).

2.4 Wat zijn de verschillende rollen en verantwoordelijkheden volgens de AVG?

Binnen de AVG worden verschillende rollen gedefinieerd bij de verwerking van persoonsgegevens. De belangrijkste rollen zijn: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke en verwerker.

Aangezien verwerkingsverantwoordelijken en verwerkers verschillende verantwoordelijkheden en verplichtingen hebben, is het belangrijk dat deze rollen aan de start van het onderzoek duidelijk vastgelegd worden.

De **verwerkingsverantwoordelijke** bepaalt het doel en de middelen van de verwerking. Doorgaans zal dit de Vrije Universiteit Brussel zijn. Er zijn echter ook situaties mogelijk waarin financiers de verantwoordelijkheid dragen voor de verwerkingen van de persoonsgegevens, of waarin een gezamenlijke verantwoordelijkheid bestaat.

Bij **gezamenlijke verwerkingsverantwoordelijken** worden het doel en de middelen bepaald door twee of meer organisaties of instellingen. Onderzoek binnen een (internationaal) consortium valt hier bijvoorbeeld onder. In deze situatie is het belangrijk dat de verschillende verwerkingsverantwoordelijken op een transparante wijze vastleggen wie verantwoordelijk is voor het verstrekken van informatie aan de betrokkenen en de uitoefening van de rechten van de betrokkenen (zie 2.8).

Tot slot kan een organisatie ook een **verwerker** zijn. In dit geval verwerkt een organisatie persoonsgegevens in opdracht van een andere organisatie. Contract onderzoek in opdracht van private bedrijven of sommige types van beleidsrelevant onderzoek kunnen hier onder vallen. Binnen een onderzoeksproject kan het ook voorkomen dat onderzoekers beroep doen op verwerkers voor het verzamelen, verwerken, opslaan of het beschikbaar maken van persoonsgegevens. Afspraken tussen verwerkingsverantwoordelijke(n) en verwerker(s) of tussen verwerkers en subverwerkers worden vastgelegd in een verwerkersovereenkomst (zie 2.8).

2.5 Wanneer verwerk ik persoonsgegevens met een hoog risico en waar moet ik dan rekening mee houden?

Wanneer de soort data of de aard van de verwerking een hoog risico inhoudt voor de betrokkenen, ben je volgens de AVG verplicht om voor de start van de verwerking een risicoanalyse uit te voeren, een zogenaamde gegevensbeschermingseffectenbeoordeling (GBE) ook DPIA genoemd.

Volgende vragen (waarvan een deel opgenomen is in het register) helpen om te bepalen over er sprake is van een groot risico.

Indien de gegevens openbaar gemaakt zouden worden, zou dit een grote impact hebben op de betrokkene(n)?	JA / NEEN
Werk je met bijzondere categorieën van persoonsgegevens?	JA / NEEN
Verwerk je persoonsgegevens van kwetsbare groepen?	JA / NEEN
Verwerk je gegevens op grote schaal? Hou voor het beantwoorden rekening met de absolute hoeveelheid persoonsgegevens, maar ook met de grootte van de steekproef t.a.v. de relevante populatie?	JA / NEEN
Worden de gegevens doorgegeven aan een land buiten de EU dat niet op de “witte lijst” staat?	JA/NEEN
Ga je verschillende (bijzondere categorieën van) persoonsgegevens aan elkaar koppelen?	JA / NEEN
Hebben de verwerkingen juridische gevolgen of een gelijkaardig effect voor de betrokkene zoals uitsluiting of discriminatie van de betrokkene?	JA / NEEN
Hebben de verwerkingen het gevolg dat de betrokkene wordt belet om zijn rechten uit te oefenen, of gebruik te maken van een dienst of contract?	JA / NEEN
Ga je op systematische wijze toezicht houden op personen in openbare ruimten?	JA / NEEN
Dienen de verwerkingen om profielen van personen op te stellen en voorspellingen te maken?	JA / NEEN
Maak je innovatief gebruik van technologische toepassingen zoals het gecombineerd gebruiken maken van vingerafdruk en gezichtsherkenning voor toegangscontrole?	JA / NEEN
Werk je met niet-gepseudonimiseerde persoonsgegevens?	JA / NEEN

Indien elke vraag met NEEN beantwoord wordt, houdt het onderzoek waarschijnlijk geen hoog risico in voor de betrokkenen.

Indien één of meerdere vragen met JA beantwoord worden, houdt het risico waarschijnlijk *wel* een hoog risico in voor de betrokkenen. Het is dan nodig om een uitvoerigere risicobeoordeling uit te voeren om de verwerking van je data (de GBE of DPIA). Tijdens een GBE vul je een formulier in waarmee je privacy-issues en daaruit voortvloeiende maatregelen kunt beoordelen om mogelijke privacyproblemen in een vroeg stadium op te lossen. Contacteer hiervoor de data protection officer (dpo[at]vub.be).

Het is belangrijk om deze GBE te documenteren en, indien nodig, in de loop van het project aan te passen.

2.6 Waar moet ik op letten wanneer ik data verzamel bij kinderen?

Kinderen hebben recht op specifieke bescherming, aangezien zij zich vaak minder bewust zijn van hun rechten, de mogelijke risico’s en gevolgen in verband met de verwerking van persoonsgegevens. Concreet heeft dit gevolgen voor de manier waarop informatie wordt verstrekt en geïnformeerde toestemming wordt verkregen.

Onderzoekers moeten kinderen **informeren** over welke data verzameld worden, waarvoor deze gebruikt zullen worden, wat de risico’s, regels, waarborgen en rechten in verband met de verwerking zijn en hoe ze hun rechten met betrekking tot de verwerking kunnen uitoefenen. Deze informatie moet op een duidelijke en begrijpbare manier gecommuniceerd worden gebruik makend van een medium dat aansluit bij de leefwereld en het onderscheidingsvermogen van het kind. Belangrijk om te

vermelden is dat kinderen hun recht op informatie niet verliezen indien voor het onderzoek toestemming moet gegeven worden door de ouders. In dat geval moeten zowel de ouders als de kinderen op een gepaste manier geïnformeerd worden.

Indien data verzameld wordt bij minderjarige kinderen zal hiervoor **toestemming** gevraagd worden bij de persoon die de ouderlijke verantwoordelijkheid draagt. Als het niet mogelijk is om te werken met toestemmingen, contacteer dan de data protection officer – dan kan er samen gekeken worden naar de mogelijkheden.

2.7 Waaraan moet ik denken bij de doorgifte van data naar andere landen of internationale organisaties?

De AVG zorgt voor een uniformering van databeschermingswetgeving binnen de EU, waardoor er vrij verkeer van persoonsgegevens **binnen de Europese Economische Ruimte** mogelijk is (de 28 EU lidstaten + Noorwegen, IJsland en Liechtenstein).

Doorgifte van persoonsgegevens naar landen **buiten de EER** of internationale organisaties is enkel toegestaan indien het land of de organisatie in kwestie een “passend beschermingsniveau” kan garanderen voor de verwerking van persoonsgegevens (‘adequacy’).

De Europese Commissie gaf aan een aantal landen reeds een **adequaatheidsbelsuit** waarmee bevestigd wordt dat het land een passend beschermingsniveau kent. De meeste recente lijst met landen is hier terug te vinden. Voor de Verenigde Staten in het algemeen geldt geen passend beschermingsniveau. De EU-US Privacy Shield wordt (vooralsnog) door de Commissie echter wel erkend als adequaat waardoor persoonsgegevens wel doorgegeven mogen worden naar organisaties en bedrijven die gecertificeerd zijn onder de Privacy Shield.

Indien een land niet op de lijst met adequaatheidsbesluiten staat, zijn er nog een aantal andere mogelijkheden om de doorgifte van data te regelen:

- Het **gebruik van standaardbepalingen** in een overeenkomst/contract tussen de eigen instelling en de ontvangende instelling (zie ook 2.8)
- Het **expliciet vragen van toestemming aan de betrokkenen** voor de incidentele doorgifte van data. Hierbij moet aan de betrokkenen ook gemeld worden welke risico’s deze doorgifte eventueel voor hem kunnen inhouden.

Het is hierbij belangrijk om zelf een inschatting te maken van de mogelijke risico’s voor de betrokkenen rekening houdend met enerzijds de aard van de persoonsgegevens, en anderzijds de geboden waarborgen van de betreffende organisatie en de privacywetgeving die bestaat in het betreffende land.

2.8 Waaraan moet ik denken wanneer ik samenwerk met anderen of mijn data deel?

Onderzoeksdata met persoonsgegevens kunnen **binnen je eigen instelling** gedeeld worden (tenzij je hierover andere zaken hebt beloofd aan bijvoorbeeld respondenten). We raden je wel aan om deze doorgifte van data te documenteren (in het register, of via een melding aan de data protection officer). Vergeet ook niet om voor elke nieuwe verwerking door jezelf of door collega-onderzoekers binnen je eigen instelling het register opnieuw in te vullen.

Indien de data gedeeld worden met personen **buiten je eigen instelling** is het vaak noodzakelijk om een contract op te stellen, of bestaande contracten aan te vullen met betrekking tot databescherming. Op basis van de rollen die deze instellingen of personen opnemen in de

verwerking van persoonsgegevens (zie 2.4) tijdens of na je onderzoek, worden een aantal mogelijke overeenkomsten onderscheiden:

- Indien je binnen een onderzoeksproject samenwerkt met een verwerker of indien je zelf de rol van verwerker opneemt, moet er een **verwerkersovereenkomst** opgesteld worden. In een verwerkersovereenkomst wordt vastgelegd hoe de persoonsgegevens kunnen worden verwerkt, wie toegang heeft en voor welk exacte doel ze gebruikt kunnen worden.
- Indien naast de VUB nog een andere organisatie of instelling verwerkingsverantwoordelijke is (dwz. Gezamenlijke verwerkingsverantwoordelijke) dien je in **(een addendum bij) het consortium agreement** vast te leggen wie verantwoordelijk is voor het verstrekken van informatie aan de betrokkenen en voor de uitoefening van de rechten van de betrokkenen.
- Wanneer (persoonlijke) gegevens worden overgedragen tussen twee instellingen waarbij de andere partij de gegevens opnieuw gebruikt voor de eigen doeleinden wordt een **data transfer agreement** opgesteld. Net zoals in een verwerkersovereenkomst wordt vastgelegd hoe de persoonsgegevens kunnen worden verwerkt, wie toegang heeft en voor welk exacte doel ze gebruikt kunnen worden.
- Wanneer andere onderzoekers je data (die persoonsgegevens bevatten) na je onderzoek willen hergebruiken zal er een **licentie of user agreement** opgesteld worden. In deze overeenkomsten wordt duidelijk vastgelegd onder welke voorwaarden jouw data hergebruikt kunnen worden.

Deze contracten worden opgemaakt door de betreffende juridische dienst (bv. juristen van het Departement Research en Datamanagement *(legalrd[at]vub.be), Tech Transfer (*techtransfer[at]vub.ac.be), verzekeringen[at]vub.be etc.). Zij zullen u helpen bij het opstellen van dergelijke contracten of het invoegen van privacy- en databeschermingsclausules in bestaande afspraken. Alle Vlaamse universiteiten werken momenteel samen aan het afsluiten van overkoepelende kaderovereenkomsten op dit onderwerp.

Naast de rollen die de instellingen en personen opnemen, kan ook het land waarin deze personen of instellingen gevestigd zijn, ervoor zorgen dat er voor de transfer van data een overeenkomst opgesteld moet worden. Aangezien de AVG enkel van toepassing is binnen de EER én landen met een adequaatheidsbesluit, bieden andere landen vaak geen passend beschermingsniveau. Transfer van persoonsgegevens naar deze landen is volgens de AVG dan ook enkel mogelijk mits passende waarborgen. Het opstellen van een overeenkomst is hier één van de mogelijkheden (zie 2.7). Belangrijk om te vermelden is dat het hier meestal gaat om standaardcontracten die opgesteld werden door de Europese Commissie. Hierbij is het niet toegestaan om zelf aanpassingen te doen.

2.9 Wat zijn de rechten van de betrokkenen, hoe respecteer ik deze en welke uitzonderingen gelden voor onderzoek?

Binnen de AVG hebben de betrokkenen verschillende rechten ten opzicht van hun data:

- **Recht op informatie**: de betrokkenen moeten op een duidelijke en transparante manier geïnformeerd worden indien er persoonsgegevens van hen verwerkt worden
- **Recht op inzage**: een betrokkene mag altijd vragen of er gegevens over hem worden verwerkt, welke gegevens dit zijn, waarom deze worden verwerkt en met wie ze gedeeld worden.
- **Recht op correctie**: als de gegevens niet correct zijn, mag de betrokkenen vragen om deze te corrigeren.

- **Recht op gegevenswissing:** Onder bepaalde omstandigheden (bv. het intrekken van toestemming in het kader van de AVG) hebben de betrokkenen het recht om hun persoonsgegevens te laten wissen. Op dit recht gelden in onderzoeksverband uitzonderingen.
- **Recht op beperking van de verwerking**: de betrokkenen mogen vragen om te stoppen met de gegevensverwerking. Op dit recht gelden in onderzoeksverband uitzonderingen.
- **Recht op overdraagbaarheid van gegevens**: de betrokkenen mogen vragen om hun gegevens mee te krijgen, in een gemakkelijk leesbaar en hanteerbaar formaat.
- **Bezwaar tegen geautomatiseerde besluitvorming en profilering**

In de informatie die onderzoekers meegeven aan de betrokkenen, moet duidelijk vermeld worden welke rechten de betrokkenen hebben en hoe zij deze kunnen uitoefenen.

3 HET INVULLEN VAN HET REGISTER

3.1 Wat is het register van verwerkingsactiviteiten?

Het bijhouden van een register van verwerkingsactiviteiten kadert binnen het principe van 'accountability': iedere organisatie draagt de verantwoordelijkheid voor het zorgvuldig verwerken van persoonsgegevens. Dit betekent dat iedere instelling alle verwerkingen van persoonsgegevens duidelijk moet documenteren in een intern register, omwille van het verkrijgen van overzicht en het kunnen inschatten van risico's.

3.2 Waarom moet ik dit register invullen?

Het register helpt de universiteit om overzicht te behouden over de persoonlijke informatie die zij verwerkt van de vele personen die met ons in contact komen, of dit nu onderzoekers, studenten, of respondenten zijn. Het register stelt de universiteit in staat om risico's te identificeren en vervolgens te beheren, zodat de verschillende categorieën persoonsgegevens passend beveiligd kunnen worden. Bij het uitvoeren van controles kan de Autoriteit Gegevensbescherming ook inzage vragen in dit register.

3.3 Wanneer moet ik het register invullen?

Onderzoekers die voor een onderzoeksproject persoonsgegevens verwerken in de rol van (gezamenlijke) verwerkingsverantwoordelijke of verwerker (zie 2.4), worden verwacht om dit register in te vullen aan de start van hun onderzoek. Daarnaast is het belangrijk om de informatie in dit register gedurende het onderzoek indien nodig aan te passen.

3.4 Welke informatie moet ik documenteren in het register?

Voor elke verwerking moet het register informatie bevatten over:

- Naam en contactgegevens van de verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming
- De verwerkingsdoeleinden (dit zal vaak "*wetenschappelijk onderzoek"* zijn)
- Een overzicht van de categorieën van de betrokkenen en van de categorieën van persoonsgegevens
- Een overzicht van de categorieën van ontvangers van de persoonsgegevens
- Indien van toepassing: of de persoonsgegevens gedeeld worden met andere instellingen, met instellingen buiten de EER, of met internationale organisaties en de waarborgen die genomen worden om de privacy van de betrokken te garanderen
- Hoe lang de persoonsgegevens bewaard zullen worden
- Een overzicht van de maatregelen die genomen worden om de persoonsgegevens te beschermen

4 TIJDENS HET ONDERZOEK

4.1 Hoe ben ik transparant naar de betrokkenen van mijn onderzoek?

Het informeren van de personen waarvan persoonsgegevens verwerkt worden is één van de basisprincipes van de AVG ('transparantie'). Het is hierbij belangrijk om deze informatie op een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal te communiceren naar de betrokkenen.

De AVG maakt een onderscheid tussen situatie waarbij de persoonsgegevens bij de betrokkenen zelf verzameld worden en wanneer deze gegevens niet van de betrokkenen zelf verkregen zijn.

Indien je als onderzoeker zelf persoonsgegevens verzamelt, is het belangrijk om volgende informatie mee te geven aan de betrokkenen:

- Contactgegevens van de onderzoeker/promotor (en de DPO van de instelling)
- Het doel waarvoor hun persoonsgegevens verwerkt zullen worden
- De wettelijke basis voor de verwerking van hun persoonsgegevens (zie 2.2)
- Indien de verwerking gebaseerd is op de rechtsgrond 'gerechtvaardigd belang': een argumentatie van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke
- Indien de verwerking gebaseerd is op de rechtsgrond 'toestemming': de vermelding dat de betrokkene het recht heeft de toestemming ten allen tijde in te trekken
- De personen of organisaties waarmee de persoonsgegevens gedeeld zullen worden
- Of er een transfer zal gebeuren van hun persoonsgegevens naar een derde land of een internationale organisatie. Indien er een transfer plaatsvindt, moet aangegeven worden welke waarborgen genomen worden om de privacy van de betrokkenen te beschermen (zie 2.7)
- Hoe lang de persoonsgegevens bewaard zullen worden (zie 5.1)
- Wat de rechten van de betrokken zijn en hoe deze uitgeoefend kunnen worden
- Dat de betrokkenen het recht heeft om klacht in te dienen bij de toezichthoudende autoriteit

Indien de persoonsgegevens die je gebruikt in je onderzoek niet rechtstreeks van de betrokkenen verkregen zijn (dwz. bij verder verwerking, zie 2.3), moet je daarnaast nog de volgende informatie meegeven:

- De bron waar de persoonsgegevens vandaan komen
- Indien van toepassing: het bestaan van geautomatiseerde besluitvorming of profilering

Indien het bij verdere verwerking van persoonsgegevens onmogelijk is of onevenredig veel inspanning vraagt om de betrokkenen te informeren, laat de AVG toe dat de betrokkenen niet rechtstreeks geïnformeerd worden. Het is in dit geval als onderzoeker wel belangrijk om inspanningen te doen om de informatie op een andere manier openbaar te maken. Dit kan bijvoorbeeld gebeuren door een mededeling op sociale media, websites, of kranten met een link naar een plaats waar meer uitleg gegeven wordt over het onderzoek. De afwijking op deze vereiste voor het verstrekken van informatie moet wel duidelijk gemotiveerd worden in het register.

4.2 Welke informatie moet ik opnemen op een *informed consent* formulier?

Indien toestemming de rechtsgrond is op basis waarvan je persoonsgegevens verwerkt (zie 2.2), moet deze toestemming aan een aantal voorwaarden voldoen.

- Respondenten moeten op een **begrijpelijke en gemakkelijke toegankelijke vorm en in een duidelijke en eenvoudige taal** geïnformeerd worden over de doelstellingen van het onderzoek en de manier waarop hun persoonsgegevens verwerkt zullen worden.
- De toestemming moet **ondubbelzinnig, vrijelijk en specifiek** zijn en de betrokkenen moeten worden geïnformeerd over elk doel waarvoor de gegevens worden verwerkt. vooraf aangevinkte vakjes of inactiviteit worden binnen de huidige wetgeving niet toegestaan. (n.b. op het dwingen van iemand tot het geven van diens toestemming, staat in de Belgische wetgeving een boete tot €20.000,-.)
- Toestemming moet verkregen worden **voor elke afzonderlijke verwerkingsactiviteit**. Toestemming is niet geldig als verschillende doeleinden gebundeld zijn, zodat een persoon ze allemaal moet accepteren of geen van hen.
- Onder de GDPR hebben betrokkenen het **recht om hun toestemming op elk moment in te trekken**. Het is belangrijk om de betrokkenen te informeren over hoe ze hun toestemming op een eenvoudige manier kunnen terugtrekken. In het geval het uitoefenen van dit recht fundamentele risico's inhoudt voor het onderzoek (zoals ook gemotiveerd in het register), dan dient dit ook vermeld te worden.
- De (geschreven of mondelinge toestemming) moet **gedocumenteerd worden**.
- **Een gegeven toestemming kan zijn waarde na verloop van tijd verliezen**. De 'houdbaarheidsdatum' van de toestemming zal afhankelijk zijn van de context van het onderzoeksproject en van de oorspronkelijke toestemming. Het is dan ook belangrijk om regelmatig te evalueren of de verkregen toestemming nog strookt met de huidige onderzoeksactiviteiten.

De AVG erkent dat het voor onderzoek niet altijd mogelijk is om op het moment van dataverzameling het doel van de gegevensverwerking volledig te omschrijven. Om die reden legt de AVG vast dat respondenten de mogelijkheid moeten hebben om hun toestemming te geven voor bepaalde terreinen van wetenschappelijk onderzoek ('broad consent'), waarbij erkende ethische normen voor wetenschappelijk onderzoek in acht worden genomen. Hierbij is het belangrijk ook oog te hebben voor andere regelgeving die relevant is zoals voor klinische studies, etc.

4.3 Wat moet ik doen wanneer er sprake is van een datalek (bv. verlies van data,…)?

Een datalek is een veiligheidsincident dat de vertrouwelijkheid, integriteit of beschikbaarheid van persoonlijke gegevens aantast. Mogelijke incidenten die kunnen leiden tot een datalek zijn:

- Toegang tot persoonlijke gegevens door een onbevoegde derde;
- opzettelijke of onopzettelijke actie (of nalaten) door een controller of een bewerker die de beveiliging van persoonlijke gegevens beïnvloedt;
- het verzenden van persoonlijke gegevens naar een onjuiste ontvanger;
- computerapparatuur met persoonsgegevens die verloren of gestolen zijn;
- het wijzigen van persoonlijke gegevens zonder toestemming;
- de beschikbaarheid van persoonlijke gegevens verliezen;

De AVG verplicht instellingen om (bepaalde) datalekken binnen 72 uur nadat er kennis van werd genomen te melden aan de GBA, of in sommige gevallen zelfs aan de betrokkenen wiens data is gelekt. Het is dan ook belangrijk dat onderzoekers een (vermoeden) van datalek steeds zo snel mogelijk melden, via de ICT Helpdesk (via Service Now).

4.4 Hoe beveilig ik mijn data op een correcte manier?

Er zijn verschillende manieren om je onderzoeksdata op een correcte manier te beveiligen. De gemakkelijkste manier is het beperken van het aantal mensen dat toegang heeft tot de data: deel data niet zonder na te denken over mogelijke consequenties hiervan. Uiteraard wordt van alle onderzoekers ook verwacht dat zij de informatieveiligheidsrichtlijnen van de universiteit naleven (te vinden op https://ivp.vub.be/). Door de wetgever worden ook pseudonimisering en encryptie van de gegevens naar voor geschoven als manieren om je data te beveiligen.

Het wordt aangeraden om, indien mogelijk, persoonsgegevens zo snel mogelijk te coderen (**pseudonimiseren**). Het codebestand moet hierbij op een aparte en veilige plaats bewaard worden. Enkel de betrokken onderzoekers hebben dagdagelijks toegang tot de gepseudonimiseerde gegevens. De toegang tot ruwe persoonsgegevens moet sterk beperkt worden. De toegangsrechten en –modaliteiten tot de (ruwe en gepseudonimiseerde) data moeten duidelijk vastgelegd worden in het register.

Het gebruik van **encryptie** voor de opslag of bij de transfer van data wordt ook sterk aanbevolen door de AVG. Als de gegevens of de harde schijf waarom de data staat geëncrypteerd is, is niet alleen de privacy van de betrokkenen beter beschermd – het verkleind ook aanzienlijk de kans dat een mogelijk datalek van die gegevens gemeld moet worden aan de bevoegde autoriteit en aan de personen zelf.

5 NA HET ONDERZOEK

5.1 Hoe lang mogen onderzoeksdata met persoonsgegevens bewaard worden?

De AVG vereist dat persoonsgegevens niet langer bewaard worden dan nodig is voor het bereiken van de doeleinden waarvoor ze worden verwerkt (zie principe ‘opslagbeperking’). Persoonsgegevens die uitsluitend voor onderzoeksdoeleinden worden verwerkt, kunnen echter voor langere tijd worden opgeslagen, op voorwaarde dat er passende waarborgen genomen worden, zoals pseudonimisering, en/of encryptie. Hoe lang onderzoeksdata bewaard moeten worden, kan per geval verschillen. Het is dan ook aan de onderzoekers om te argumenteren hoe lang de data bewaard zullen worden, deze argumentatie te documenteren en de betrokkenen hierover te informeren. Het is hierbij ook belangrijk om rekening te houden met de vereisten omtrent de bewaring van onderzoeksdata die de VUB, je onderzoeksfinancier(s), en journals waarin je de resultaten later wil publiceren stellen. In dit kader moet ook nagedacht worden over de eisen die hier aan gesteld worden in het kader van *research data management* en het bewaken van de wetenschappelijke integriteit.

5.2 Mag ik onderzoeksdata met persoonsgegevens delen met anderen wanneer mijn onderzoeksproject afgelopen is?

Wanneer het onderzoeksproject, of een deel ervan, is afgerond, kunnen de onderliggende gegevens worden gedeeld met derden ten behoeve van reproduceerbaarheid en hergebruik, mits is voldaan aan bepaalde voorwaarden zoals anonimisering, het afsluiten van *data protection agreements* als de data de VUB verlaat, en de gegevens passend beveiligd zijn. Het delen van onderzoeksdata kan enkel gebeuren indien er voldoende waarborgen bestaan voor het beschermen van de privacy (bv. opslag in een betrouwbaar repository dat gecertificeerd is met Data Seal of Approval of World Data System; met een overeenkomst). Om zowel ethische als juridische redenen is het ook belangrijk om in de toestemmingsformulieren ook altijd al te vragen of de betrokkenen akkoord gaan met het delen van bepaalde (gepseudonimiseerde) data en onder welke voorwaarden het delen van deze data gebeurt. Op die manier worden het recht op privacy van de betrokkenen verzekerd en maken universiteiten en

onderzoekers zich niet schuldig aan het heimelijk doorsluizen van persoonlijke informatie tegen de wil van de betrokkenen in.

Indien gepseudonimiseerde data gedeeld worden met derden ten behoeve van reproduceerbaarheid of hergebruik, moet dit ook in het register van verwerkingsactiviteiten beschreven worden, zodat ook de (technische en organisatorische) waarborgen bekeken kunnen worden om de bescherming van de rechten van de betrokkenen te verzekeren.

Bestanden met ruwe persoonsgegevens worden in beginsel niet gedeeld met derden. Het kan zijn dat dit noodzakelijk is met het oog op reproductie, hergebruik of beoordeling van wetenschappelijke integriteit. In dit geval moeten de modaliteiten van het delen van dit soort data besproken worden met de data protection officer (dpo[at]vub.be) en moet dit duidelijk vastgelegd worden in het register van verwerkingsactiviteiten.

6 BRONNEN

https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32016R0679&from=NL

https://researchsupport.admin.ox.ac.uk/policy/data/checklist

http://www.lancaster.ac.uk/research/research-services/research-integrity-ethics--governance/data-protection/gdpr-what-researchers-need-to-know/

https://www.insight.mrc.ac.uk/2018/04/16/gdpr-research-changes/

https://www.uu.nl/en/research/research-data-management/guides/handling-personal-data

https://blogs.openaire.eu/?p=3248

http://www.staffnet.manchester.ac.uk/gdpr/key-resources/researcher_guide/

https://www.exeter.ac.uk/gdpr/faq/

https://www.nottingham.ac.uk/governance/records-and-information-management/policies-and-guidance/general-data-protection-regulation-faq.aspx

https://warwick.ac.uk/services/idc/gdpr/faqandcontact/

https://www.strath.ac.uk/dataprotection/gdprfaq/

https://www.ucl.ac.uk/legal-services/guidance/reporting-loss-personal-data