RICHTLIJN VOOR DATAMANAGEMENT (VERZAMELEN, OPSLAG EN VERWERKEN VAN DATA) IN STUDENTGEBONDEN ONDERZOEK.

Studenten moeten bij het verzamelen, verwerken en opslaan van de data in het kader van hun opleiding voldoen aan de wet- en regelgeving. Dit geldt met name wanneer er gewerkt wordt met persoonsgegevens. Hieronder schetsen we drie veel voorkomende situaties, namelijk:

a) Nieuwe dataverzameling;
b) Gebruik van bestaande data;
c) Naturalistische observatie;

We geven daarbij richtlijnen voor verantwoord gebruik van data in alle fasen van de dataverzameling.

Situatie A. Nieuwe dataverzameling

Stap 1: toestemming vragen

Zorg dat je aan de participanten die je wilt betrekken bij het onderzoek toestemming vraagt voor het verzamelen van de data. Actieve toestemming (toestemmingsformulier met handtekening; *informed consent*, zie bijlage) is vereist als sprake is van het verzamelen van *(bijzondere) persoonsgegevens* (voor definitie, zie bijlage), video-opnamen, geluidsopnamen of invasieve vragenlijsten.
Zie voor het opstellen van een adequate *informed consent* ons instructiedocument [link].

Stap 2: data verzamelen

Zorg dat vragenlijsten anoniem worden ingevuld, dus geen naam, geboortedatum of leerlingnummer op het voorblad of daarnaar vragen in de (*online*) vragenlijsten; bij *online* vragenlijsten: zorg ervoor dat je bij de uitdraai van de antwoorden op de vragenlijst de IP-adressen uitvinkt (bijv. Qualtrics heeft die functie).
Bij dataverzameling van gegevens van het web: vergewis je ervan dat het verzamelen van de data die een persoon online zet, niet indruist tegen de redelijke verwachtingen van die persoon t.a.v. zijn/haar privacy.
- Bij videodata: zie onze instructiedocumenten [link]. Maak voor video-opnamen zoveel mogelijk gebruik van daartoe beveiligde *devices* die je bij de desk van Techsupport https://Techsupport.fss.uu.nl/ kunt afhalen. En zorg dat je de videodata z.s.m. op het beveiligde deel van de facultaire server opslaat (advies en toegang tot facultaire server kan via Techsupport worden verkregen) en verwijdert van de *device*.
- Voor je begeleider: indien de data worden verzameld bij een externe instantie zoals een school/instelling/organisatie: check bij de privacy-officer van de faculteit (privacy-fsw@uu.nl) of het nodig is om een **verwerkersovereenkomst** af te sluiten met deze externe instantie.

Stap 3: verwerken en opslaan van de verzamelde data

Anonimiseer

Anonimiseren houdt in dat je de data ontdoet van alle tot de persoon herleidbare informatie (zie ook bijlage). Doe dit in overleg met je begeleider. Je begeleider kan desgewenst nader advies vragen aan Techsupport: https://Techsupport.fss.uu.nl/ of via privacy-fsw@uu.nl .

- Sla de geanonimiseerde data z.s.m. op op de daartoe bestemde map op de facultaire server. Een map kun je laten aanmaken via de medewerkers van Techsupport.
- Verwijder vervolgens de data van de *device* waarop ze oorspronkelijk stonden, verwijder ook de documenten uit "de prullenbak" van je *device*. Sla de data in ieder geval niet op in de *cloud*!
Is het niet mogelijk om de data te anonimiseren (bijvoorbeeld omdat je participanten opnieuw moet kunnen benaderen voor vervolgonderzoek), pseudonimiseer dan.

Pseudonimiseer
Bij pseudonimiseren van de data ken je een unieke code toe aan iedere persoon in de data. Vervolgens maak je twee data sets: één met de code en de identificerende informatie, de zgn. *sleutel,* en één met de code zonder de identificerende informatie, de zgn. *gepseudonimiseerde data* (zie bijlage). De twee datasets worden apart van elkaar opgeslagen. Analyses vinden plaats op de gepseudonimiseerde data. Door de unieke code is op een later tijdstip de sleutel te koppelen aan de gepseudonimiseerde data, zodat je de participanten opnieuw kunt benaderen als dit nodig is. Doe dit pseudonimiseren in overleg met je begeleider. Je begeleider kan desgewenst nader advies vragen aan Techsupport [link].
- Sla de gepseudonimiseerde data z.s.m. op op de daartoe bestemde map op de facultaire server. Een map kun je laten aanmaken via de medewerkers van Techsupport.
- Sla de sleutel z.s.m. op op de hiertoe beveiligde facultaire server.
- Verwijder vervolgens de gepseudonomiseerde data en de sleutel van de *device* waar ze oorspronkelijk op stonden, verwijder ook de documenten uit "de prullenbak" van je *device*. Sla de data in ieder geval niet op in de *cloud*!

Het koppelen van nieuw verzamelde data aan reeds bestaande data
Soms dien je nieuw verzamelde data van personen te koppelen aan reeds bestaande data van deze personen. Denk bijvoorbeeld aan het koppelen van nieuw verzamelde data van leerlingen aan hun op school reeds aanwezige CITO-scores. Dit koppelen zal naar alle waarschijnlijk gebeuren met behulp van persoonsgegevens. Zorg ervoor dat het gebruik van de persoonsgegevens zoveel mogelijk plaatsvindt op de locatie waar de dataverzameling plaatsvindt.
Het heeft de voorkeur na dit koppelen de data te anonimiseren, en anders te pseudonimiseren.

Bewaartermijnen
Uitgangspunt is dat data die de student verzamelt voor het schrijven van een opdracht of thesis worden bewaard. Voor de bewaartermijn gelden de termijnen voor het bewaren van studieresultaten (voor papers 2 jaar en voor thesis 7 jaar). Als er op basis van de data een wetenschappelijke publicatie plaatsvindt, dan gelden de bewaartermijnen genoemd in de Richtlijn archivering wetenschappelijk onderzoek voor Nederlandse faculteiten Maatschappij- en Gedragswetenschappen, Versie 2, Juli 2017.

Stap 4: datatransport
Als je de data van de school/instelling meeneemt naar de universiteit om hier verder aan te kunnen werken, doe dit dan:
- via een beveiligde verbinding, zoals Surffile sender:
https://www.surf.nl/surffilesender-veilig-en-versleuteld-grote-bestanden-versturen.

- door een daartoe beveiligde *device* van de faculteit via Techsupport te lenen: https://Techsupport.fss.uu.nl/ .
- door de data op te slaan op Surfdrive: www.surfdrive.nl (en van de *device* te verwijderen).
Zorg ervoor dat alleen jijzelf en je begeleiders toegang tot de data (kunnen) hebben.
- Zie dataopslagrichtlijn: https://la0171.its.uu.nl/

B. BESTAANDE DATA GEBRUIKEN

Student maakt gebruik van data op de UU (project van begeleider).

Check toegang tot de data

- Ga na of en hoe de toegang tot de data voor jou is geregeld.
Zorg ervoor dat je alleen toegang hebt tot data die je nodig hebt voor je onderzoek. Concreet: alleen tot anonieme data, of, als voor pseudonimiseren goede redenen zijn, de gepseudonimiseerde data.
- Als je vanuit huis toegang tot de data nodig hebt, regel dit dan via een beveiligde verbinding. Voor advies hierover neem je contact op met Techsupport.
Zorg ervoor dat je data niet downloadt op je eigen laptop.

C. NATURALISTISCHE OBSERVATIE

Student verzamelt data op straat, in het veld, online door het observeren van participanten of andere zaken. Van belang is dat je hierbij geen persoonsgegevens noteert, en ook geen video- of audio-opnamen maakt. Dataopslag is verder hetzelfde als hierboven beschreven bij anonieme data.

Bijlage:

1. Voorbeeld van *Informed consent* formulier
2. definities basisbegrippen v.w.b. datamanagement en privacy

Bijlage 1:

Voorbeeld informatiebrief/template

Proefpersoneninformatie voor deelname aan (sociaal)-wetenschappelijk onderzoek

<Titel onderzoek>

<Datum, plaats>

Geachte heer, mevrouw,

Introductie
Middels deze brief willen we u toestemming vragen om mee te doen aan het onderzoek "<titel>". Dit onderzoek heeft tot doel….

Opzet/uitvoering van het onderzoek

Achtergrond onderzoek
<beschrijving achtergrond van het onderzoek>

Wat wordt van u als participant verwacht
<beschrijving van wat het meedoen aan het onderzoek betekent; wat wordt precies van de participant verwacht in termen van taken, vragen, tijdsinspanning, duur/frequentie, andere vormen van belasting>

Mogelijke voor- en nadelen van het onderzoek

Vergoeding/beloning

Vertrouwelijkheid verwerking gegevens
Voor dit onderzoek is het nodig dat wij een aantal persoonsgegevens van u verzamelen. Deze gegevens hebben wij nodig om de onderzoeksvraag goed te kunnen beantwoorden, dan wel om u te kunnen benaderen voor vervolgonderzoek. De persoonsgegevens worden op een andere computer opgeslagen dan de onderzoeksgegevens zelf (de zgn. ruwe data). De computer waarop de persoonsgegevens worden opgeslagen is volgens de hoogste normen beveiligd en alleen betrokken onderzoekers hebben toegang tot deze gegevens. De gegevens zelf zijn ook beveiligd d.m.v. een beveiligingscode.
Uw gegevens zullen voor minimaal 10 jaar bewaard worden. Dit is volgens de daartoe bestemde richtlijnen van de VSNU. Meer informatie over privacy kunt u lezen op de website van de Autoriteit Persoonsgegevens:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving

Procedure toevalsbevindingen
Indien van toepassing: <iets schrijven over toevalsbevinding en bijbehorende procedure; zie hierover ook onze FAQ>

Vrijwilligheid deelname
Deelname aan dit onderzoek is vrijwillig. U kunt op elk gewenst moment, zonder opgave van reden en zonder voor u nadelige gevolgen, stoppen met het onderzoek. De tot dan toe verzamelde gegevens worden wel gebruikt voor het onderzoek, tenzij u expliciet aangeeft dit niet te willen.

Onafhankelijk contactpersoon en klachtenfunctionaris
Als u vragen of opmerkingen over het onderzoek heeft, kunt u contact opnemen met <onafhankelijk contactpersoon; Onafhankelijk wil zeggen: niet betrokken bij de studie zelf. De contactpersoon mag in principe een collega-onderzoeker zijn (al dan niet van een andere afdeling) die inhoudelijk kan ingaan op de vraag of klacht. >

Als u een officiële klacht heeft over het onderzoek, dan kunt u een mail sturen naar de klachtenfunctionaris via klachtenfunctionaris-fetcsocwet@uu.nl

Als u na het lezen van deze informatiebrief besluit tot deelname aan het onderzoek verzoek ik u bijgevoegd antwoordstrookje te ondertekenen en in te leveren bij de onderzoeker(s).

Vriendelijke groet,

Naam onderzoeker(s)

Toestemmingsverklaring:

Hierbij verklaar ik de informatiebrief m.b.t. onderzoek <titel> gelezen te hebben en akkoord te gaan met deelname aan het onderzoek.

Naam <Hier verder geen identificerende informatie opnemen, zoals proefpersoonnummer of andere codes, geboortedatum, etc.>

Datum

Bijlage 2:

Definities privacy, datamanagement en ethiek

Definitie persoonsgegevens
Ieder gegeven over een persoon dat kan leiden tot identificatie van die persoon, zoals naam, adres, telefoonnummer, emailadres, geboortedatum, identificatoren en locatiegegevens (IP-adressen, IMEI nummer van Smartphone, cookies, MAC-adres) en vingerafdruk. Er kan ook identificatie plaatsvinden bij een combinatie van deze gegevens, bijvoorbeeld, alleen een voornaam is in principe niet identificerend, tenzij deze erg zeldzaam is.

Definitie bijzondere persoonsgegevens
Bijzondere persoonsgegevens zijn extra gevoelige gegevens over een persoon die, als zij verwerkt worden, extra nadelige invloed op iemand kunnen hebben. Voorbeelden van bijzondere persoonsgegevens zijn: iemands gezondheid, genetische gegevens, biometrische gegevens, etniciteit, godsdienst, politieke opvattingen, lidmaatschap vakbond, strafrechtelijk verleden of seksuele leven. Van bijzondere persoonsgegevens is alleen sprake als ze tot personen herleidbaar zijn. Dit gebeurt bijvoorbeeld door ze in combinatie met persoonsgegevens uit te vragen. Een combinatie van bijzondere persoonsgegevens kan in een bepaalde context ook (indirect) identificerend zijn.

Definitie “verwerken” in de zin van de AVG (ruim op te vatten)
Iedere handeling die met de persoonsgegevens verricht kan worden, valt onder de juridische term “verwerken”. Voorbeelden zijn raadplegen, verzamelen, vastleggen, ordenen, opslaan, opvragen, gebruiken, verspreiden of vernietigen. Als studenten bijvoorbeeld op school stage lopen en zij krijgen een klassenlijst onder ogen, dan verwerken zij persoonsgegevens en worden zij geacht hier vertrouwelijk mee om te gaan, de lijst bijvoorbeeld niet te kopiëren en alleen te gebruiken voor het doel van dat moment. Hetzelfde geldt voor (patiënten)dossiers.

Grondslag verwerking persoonsgegevens
Het gaat hier om de vraag of er toestemming van de participanten is om hun persoonsgegevens te verwerken. Participanten kunnen deze toestemming geven in een zgn. Informed consent formulier (zie hieronder). Indien deze toestemming er niet is, kan men zich mogelijk beroepen op de grondslag “gerechtvaardigd belang” of één van de andere grondslagen uit de AVG[1].

Informed consent
Het adequaat informeren van participanten over het onderzoek, waarna zij toestemming kunnen geven voor deelname en gebruik van hun gegevens.

Dataminimalisatie
Het uitvragen van alleen díe persoonsgegevens die nodig zijn voor het doel van het onderzoek. Denk er goed over na welke persoonsgegevens je vraagt aan participanten. Zijn deze allemaal echt nodig voor het doel van je onderzoek? Bijvoorbeeld: als de leeftijd van de participant noodzakelijk is voor het beantwoorden van je onderzoeksvraag, vraag dan geen

[1] https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken#hoe-weet-u-of-u-persoonsgegevens-mag-verwerken-6310

geboortedatum maar alleen het geboortejaar of de leeftijd. Heb je de adresgegevens echt nodig, bijvoorbeeld voor het opnieuw benaderen van de participant? Kan dit niet per email?

Anonimiseren/pseudonimiseren

Als persoonsgegevens volledig zijn verwijderd, dan is er sprake van anonimiteit van personen, en is de AVG niet meer van toepassing. Als regel werken we met *anonieme* data. Indien de data (nog) niet anoniem zijn, anonimiseren we de data. Anonimiseren is meer dan het weglaten van namen en contactgegevens. Het gaat erom dat het met geen enkel middel dat redelijkerwijze kan worden ingezet, mogelijk is om iemand te identificeren. Het beroep tandarts van iemand in de stad Appingedam zal met een redelijk grote kans tot bepaalde personen leiden.

Soms is het noodzakelijk om persoonsgegevens te bewaren, omdat participanten opnieuw benaderd moeten kunnen worden (denk aan longitudinaal onderzoek). Dan worden data *gepseudonimiseerd* (dit is het toekennen van een code aan participanten in de data, waarbij de identificerende informatie vervangen wordt door deze code (een sleutel) en de identificerende informatie samen met de sleutel separaat van de originele data bewaard wordt). Onder gepseudonimiseerde *data* verstaan we de onderzoeksdata met de code. Onder de *sleutel* verstaande we de persoonsgegevens met de code. Pseudonimiseren betekent dat er nog steeds sprake is van persoonsgegevens, omdat immers de data toch nog te herleiden zijn, zij het lastiger, omdat men om te kunnen identificeren de sleutel en de gepseudonimiseerde data moet hebben. De sleutel wordt op een beveiligde server bewaard.

Opslag van de data

Persoonsgegevens worden bij voorkeur verwijderd, maar als ze worden bewaard dan worden ze gescheiden opgeslagen van de onderzoeksdata. Zie ook de definitie voor anonimisering en pseudonimisering. Beschrijf hoe de opslag van de data plaatsvindt. Geef ook aan als je van plan bent de data op termijn open access te maken.

Bewaartermijn

De persoonsgegevens worden vernietigd zodra zij niet meer nodig zijn voor het uitvoeren van het onderzoek. De ruwe data worden minimaal 10 jaar bewaard (en minimaal 15 jaar als het WMO-plichtig onderzoek betreft)

Toegang

Er wordt aangegeven wie toegang tot de data hebben en of de uiteindelijk geanonimiseerde data beschikbaar zullen worden gesteld voor open access.
Participanten hebben in principe recht op inzage zolang zijn/haar persoonsgegevens worden bewaard.
Participant hebben in principe recht heeft op het laten verwijderen van zijn/haar persoonsgegevens. Dit kan alleen als deze nog niet zijn vernietigd.