Beleid inzake Research Data Management Faculteit der Rechtsgeleerdheid

Versie: 2.0
Datum: 29 maart 2021

Achtergrond

De Vrije Universiteit Amsterdam (VU) hanteert een beleid inzake Research Data Management (VU RDM Policy)[1] dat de algemene universiteitsbrede principes voor de zorgvuldige omgang met onderzoeksdata beknopt weergeeft. Elke faculteit binnen de Vrije Universiteit wordt geacht faculteitsspecifieke beleidsmaatregelen te formuleren die overeenstemmen met het overkoepelende beleid. Dit document: Beschrijft het beleid inzake Research Data Management van de Faculteit der Rechtsgeleerdheid van de Vrije Universiteit (hierna het "Beleid") en geeft tekst en uitleg bij de verantwoordelijkheden van onderzoekers ten aanzien van hun onderzoeksdata.

Datamanagement omvat het ordenen, vastleggen, beschermen en verspreiden van gegevens. Goed onderzoek staat of valt met verantwoord datamanagement. U moet wellicht eerst het advies van de Facultaire Commissie Ethiek Rechtswetenschappelijk & Criminologisch Onderzoek (CERCO) inwinnen voordat u uw data gaat verzamelen.

Het beleid van de Vrije Universiteit inzake Research Data Management definieert onderzoeksdata als ten behoeve van onderzoek gebruikte bronnen of informatiemiddelen die bijdragen tot de resultaten van het onderzoeksproject. Hierbij valt te denken aan tekst, afbeeldingen, geluid, databases, statistische gegevens, geografische gegevens, etc. Het beleid van de Vrije Universiteit inzake Research Data Management definieert onderzoeksdata in de brede zin van het woord.

Er zijn grofweg drie soorten onderzoeksdata:

- Bestaande gegevens uit voor het publiek toegankelijke bronnen. Hierbij valt te denken aan artikelen in vakbladen, wetgeving, jurisprudentie en materiaal uit voor het publiek toegankelijke archieven. [2]
- Bestaande gegevens uit (tijdelijk) niet voor het publiek toegankelijke bronnen. Hierbij valt te denken aan bronnen die niet toegankelijk zijn voor het publiek, of nieuwsberichten.[3]
- Unieke gegevens: door de onderzoeker aangemaakte gegevens. Hierbij valt te denken aan enquêtes, interviews, experimenten, veldonderzoek, simulaties, theoretische modellering, etc.

Bestaande gegevens uit voor het publiek toegankelijke bronnen kunnen door iedereen worden geraadpleegd. De gegevens omvatten expliciete verwijzingen in publicaties en kunnen derhalve worden nagetrokken. Sommige bepalingen van dit Beleid gelden dan ook niet voor onderzoekers die werken

[1] https://libguides.vu.nl/ld.php?content_id=32045526

[2]Niet alle voor het publiek beschikbare gegevens mogen voor onderzoeksdoeleinden worden gebruikt. Zo zijn gegevens van Facebook of Twitter weliswaar voor het publiek beschikbaar, maar deze mogen niet voor onderzoek worden gebruikt. Voorbeelden van voor het publiek beschikbare gegevens zijn: *data.overheid.nl, www.rechtspraak.nl*. Onderzoekers kunnen te allen tijde terecht bij de Privacy Champion van de faculteit om te bepalen welke gegevens ze wel en niet mogen verzamelen.

[3]Onderzoekers kunnen de Privacy Champion om advies vragen over het toepassingsgebied van deze definitie.

met data uit voor het publiek toegankelijke bronnen. De faculteit hecht echter belang aan goed datamanagement voor alle onderzoekers, om hun wetenschappelijke integriteit en de controleerbaarheid van hun onderzoek te waarborgen.

Binnen onze faculteit besteden we speciale aandacht aan onderzoekers die werken met vertrouwelijke en privacygevoelige gegevens.
Vertrouwelijke gegevens zijn gegevens die beschermd moeten worden tegen toegang door onbevoegden. Dit kunnen door de onderzoeker aangemaakte onderzoeksdata zijn (unieke gegevens) of gegevens uit bronnen die (tijdelijk) niet voor het publiek toegankelijk zijn.

Privacygevoelige gegevens zijn gegevens die persoonsgegevens: 'Of bijzondere categorieën van persoonsgegevens: '*bijzondere categorieën van persoonsgegevens*'). Niet alle privacygevoelige gegevens zijn vertrouwelijke gegevens, bijvoorbeeld wanneer persoonsgegevens kennelijk door de betrokkene openbaar zijn gemaakt. Onderzoekers die werken met (bijzondere categorieën van) persoonsgegevens wordt geadviseerd om de Privacy Champion van de faculteit te raadplegen voor informatie over de verwerking van (bijzondere categorieën van) persoonsgegevens voor onderzoeksdoeleinden.

Definities

Vertrouwelijke gegevens: Gegevens die moeten worden beschermd tegen toegang door onbevoegden. Hierbij valt te denken aan door de onderzoeker aangemaakte onderzoeksdata (unieke gegevens) of gegevens uit bronnen die (tijdelijk) niet voor het publiek toegankelijk zijn.

Gegevens over criminaliteit: Persoonsgegevens die betrekking hebben op strafrechtelijke veroordelingen en strafbare feiten. Gegevens over criminaliteit mogen alleen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden (art. 10, lid 1, AVG).

Nederlandse uitvoeringswet: Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) van 16 mei 2018 en van kracht sinds 25 mei 2018, houdende regels ter uitvoering van de AVG.

EER: De Europese Economische Ruimte, bestaande uit de lidstaten van de Europese Unie, IJsland, Liechtenstein en Noorwegen.

Datum van inwerkingtreding: 22 april 2021

AVG: Algemene verordening gegevensbescherming (EU) 2016/979 van het Europees Parlement en de Raad van de Europese Unie van 27 april 2016, van kracht sinds 25 mei 2018.

Lopend onderzoek: *Onderzoek dat nog altijd gaande is en/of voortduurt.*

Persoonsgegevens: Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (art. 4, lid 1, AVG).[4]Een natuurlijke persoon kan rechtstreeks worden geïdentificeerd op basis van identificatoren zoals de naam, geboortedatum, adres, foto's en/of stemopnames van de natuurlijke persoon. De identificatie kan ook indirect zijn. Dit betekent dat gegevens die niet leiden tot directe

[4] NEDERLANDS: *persoonsgegevens' (art. 4, lid 1, AVG)*

identificatie van een persoon maar aan de hand waarvan een persoon redelijkerwijs toch kan worden geïdentificeerd, ook moeten worden aangemerkt als persoonsgegevens. Bijvoorbeeld: een onderzoeksdeelnamenummer, of de combinatie van postcode en huisnummer.

Pseudonymisation: 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 (art. 4, lid 5, AVG).

Privacygevoelige gegevens: Gegevens die persoonsgegevens bevatten (art. 4, lid 1, AVG) of bijzondere categorieën van persoonsgegevens (art. 9, LID 1, AVG),[5]

Bijzondere categorieën van persoonsgegevens: Gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, maar ook genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid (art. 9, LID 1, AVG).[6]

Onderzoeksdata: ten behoeve van onderzoek gebruikte bronnen of informatiemiddelen die leiden tot de resultaten van het onderzoeksproject

Doel van dit beleid

1. The Doel van dit beleid is to help researchers of the Faculteit der Rechtsgeleerdheid ensure:
    i. wettelijke en ethische vereisten ten aanzien van hun onderzoeksdata na te leven, waaronder de Nederlandse gedragscode wetenschappelijke integriteit;[7]
    ii. de bepalingen van de AVG en de Nederlandse uitvoeringswet betreffende persoonsgegevens na te leven;[8]
    iii. gedurende de levenscyclus van de gegevens over betrouwbare, traceerbare en veilig opgeslagen onderzoeksdata te beschikken;
    iv. te voldoen aan de vereisten van onderzoeksfinanciers en wetenschappelijke vakbladen wat betreft de kwaliteit en traceerbaarheid van gegevens.

---

[5] Behalve wanneer persoonsgegevens kennelijk door de betrokkene openbaar zijn gemaakt (art. 9, lid 2, punt e, AVG).
[6] Nederlands: bijzondere categorieën van persoonsgegevens (art. 9, lid 1, AVG).
[7] Zie http://www.vsnu.nl/files/documents/Netherlands%20Code%20of%20Conduct%20for%20Research%20Integrity%202018.pdf
[8] Zie https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/gdpr.pdf (AVG) en https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/uavg.pdf (Nederlandse uitvoeringswet; alleen Nederlandse versie).

Toepasselijkheid, verantwoordelijkheid

1. Dit Beleid geldt voor alle onderzoekers die in dienst zijn van of verbonden zijn aan de Faculteit der Rechtsgeleerdheid, waaronder alle (interne en externe) promovendi.

2. Dit Beleid geldt voor al het wetenschappelijk onderzoek dat wordt uitgevoerd na de datum van inwerkingtreding, en dat bestemd is voor (online) publicatie, bijvoorbeeld in een wetenschappelijk tijdschrift of vakblad, boek of hoofdstuk van een boek, website of onderzoeksplatform.

3. De bepalingen in dit document zijn relevant voor onderzoek dat gebruikmaakt van vertrouwelijke en privacygevoelige gegevens. Als onderzoekers betrokken zijn bij empirisch-juridisch onderzoek (in de breedste zin, zowel kwantitatief als kwalitatief onderzoek), zijn de bepalingen zonder meer van toepassing. Voor onderzoekers die alleen werken met gegevens uit voor het publiek toegankelijke bronnen, bijvoorbeeld bij rechtswetenschappelijk onderzoek, zijn een aantal van de bepalingen mogelijk toch relevant.

4. Elke onderzoeker wordt geacht dit Beleid en de algemene richtlijnen van de Vrije Universiteit betreffende datamanagement na te leven. Als het Beleid voor bepaalde gevallen specifieke richtlijnen ontbeert, worden onderzoekers geacht in de geest van het Beleid te handelen of om advies te vragen over de juiste interpretatie ervan.
   Om binnen onze faculteit goed datamanagement ten uitvoer te leggen, moeten onderzoeksafdelingen en onderzoeksprogramma's hun medewerkers voorlichten over RDM. Directeuren van bachelor- en masterprogramma's moeten duidelijke RDM-instructies geven aan hun studenten, en studentenbegeleiders geven hun studenten tekst en uitleg over goed beheer van onderzoeksdata.
   Voor onderzoeksdata die enkel worden gebruikt voor een bachelor- of masterscriptie of paper (en niet voor onderzoeksprojecten van personeelsleden) moeten studenten en begeleiders bovenal de specifieke richtlijnen in de scriptie of de instructies voor de paper naleven.
   De verplichting om onderzoeksdata te archiveren (artikel 12) geldt niet voor onderzoeksdata die enkel worden gebruikt voor een bachelor- of masterscriptie of paper. De specifieke instructies voor de scriptie of paper kunnen desalniettemin voorzien in de toepassing van artikel 12.

5. Onderzoek dat in het verlengde ligt van eerder onderzoek waarvoor de gegevensverzameling reeds voor de datum van inwerkingtreding van start ging, is vrijgesteld van de archiveringsplicht. Onderzoekers moeten dit Beleid voorzover redelijkerwijs mogelijk naleven. Niettegenstaande het voorgaande moeten onderzoekers wettelijke beperkingen (bijv. voor privacygevoelige gegevens) te allen tijde in acht nemen.

Principes van de faculteit

6. De faculteit hanteert de volgende principes als het gaat om datamanagement: Veiligheid, verantwoording en naleving. In het resterende deel van dit Beleid worden deze principes nader toegelicht.

    i. **Veiligheid** wordt tot stand gebracht door ervoor te zorgen dat gegevens veilig (om toegang door onbevoegden te voorkomen) en met een zekere mate van redundantie (gegevens gaan niet blijvend verloren in het geval van een defect apparaat, onopzettelijke verwijdering, verlies van een gegevensdrager, brand of waterschade) worden opgeslagen.
    ii. **Verantwoording** wordt tot stand gebracht door veilige gegevensopslag. Dit betekent dat een onderzoeker indien nodig in staat is om gepubliceerde resultaten aan de hand van de oorspronkelijke gegevensbronnen te reproduceren. Ook veronderstelt dit dat gegevens op overzichtelijke wijze worden opgeslagen, waarbij voldoende metadata beschikbaar zijn om de gegevens snel te kunnen hergebruiken of het experiment, de simulatie of de analyse te kunnen repliceren.
    iii. **Naleving** van wettelijke en ethische normen inzake onderzoeksdata vereist onder meer dat persoonsgegevens alleen worden verwerkt met inachtneming van strenge voorwaarden zoals vastgelegd in de AVG en de Nederlandse uitvoeringswet.

    Dit beleid bevordert de **herbruikbaarheid** en zelfs de **deelbaarheid** van onderzoeksdata volgens het principe: *Zo open mogelijk, maar indien nodig afgeschermd*.[9]

7. Terwijl de meeste financieringsorganisaties vooraf een schriftelijk **Data Management Plan** *vereisen* om hun goedkeuring te verlenen, *moedigt* dit Beleid alle onderzoekers die werken met vertrouwelijke of privacygevoelige gegevens slechts aan DMP's op te stellen.[10] Werk maken van datamanagement bespaart tijd, geld en moeite.

8. Onderzoekers die betrokken zijn bij een complex onderzoeksproject met omvangrijke datasets doen er goed aan in het onderzoeksbudget middelen vrij te maken voor informatiebeveiliging.

Ethische toetsing

9. De Facultaire Commissie Ethiek Rechtswetenschappelijk & Criminologisch Onderzoek (CERCO) waarborgt de ethische normen van al het aan de Faculteit der Rechtsgeleerdheid uitgevoerde onderzoek waarbij menselijke deelnemers betrokken zijn. Onderzoekers worden aangemoedigd hun onderzoeksvoorstel ethisch te laten toetsen door de CERCO voordat ze experimenten gaan uitvoeren en/of interviews met menselijke respondenten afnemen. Onderzoekers moeten hun correspondentie met de CERCO documenteren en de actieve instemming van hun respondenten verkrijgen en vastleggen. Respondenten kunnen op elk moment hun actieve instemming intrekken

[9] Zie ook de H20 Online Manual inzake Open Access and Data Management: http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-dissemination_en.htm

[10] Vraag de Data Steward van de faculteit om hulp bij het opstellen van een Data Management Plan.

en hun medewerking aan het experiment stopzetten. Intrekkingen moeten worden vastgelegd in de datadocumentatie.

Verzamelen en vastleggen van gegevens

10. Zowel gegevens als het gegevensverzamelingsproces moeten zodanig worden vastgelegd dat ze beide (in principe) controleerbaar zijn. De documentatie moet bij voorkeur deel uitmaken van het gepubliceerde onderzoek zelf, bijv. een onderdeel 'Materialen en Methoden' in de publicatie of (online) aanhangsels bij het gepubliceerde werk. Zo niet, dan moet de onderzoeker gedetailleerde aanvullende README-bestanden meeleveren en deze evenals de onderzoeksdata veilig archiveren. De documentatie over het gegevensverzamelingsproces moet voldoende gedetailleerd zijn en ten minste bestaan uit:

    i. i. informatie over het verzamelen van de ruwe data (inclusief gegevens van vragenlijsten, interviews, video-opnames, scripts van experimenten, details/code over website-extractie, etc. (in voorkomend geval);
    ii. ii. gedetailleerde metadata, waaronder beschrijvingen van de variabelen (mogelijk ook met database tickers/acroniemen indien databases van derden zijn gebruikt, en met informatie over de interpretatie van de inputvariabele (bijv. staat 1 voor mannelijke of vrouwelijke geslachtsaanduiding?);
    iii. informatie over filters en manipulaties die zijn toegepast om de ruwe data om te zetten in de gegevens die zijn gebruikt zijn voor empirische analyse, zoals informatie over hoe opgenomen interviews werden getranscribeerd en gecodeerd, hoe gegevens werden gepseudonimiseerd, en hoe de antwoorden op de vragenlijsten zijn opgeschoond;
    iv. ethische beoordeling (indien nodig; zie punt 9 hierboven en de gedragscode van de Faculteit der Rechtsgeleerdheid[11]);
    v. informatie over hoe wordt omgegaan met privacykwesties (indien sprake is van "bijzondere categorieën van persoonsgegevens");
    vi. informatie over hoe de toegang tot de gegevens wordt geregeld en gewaarborgd (in ieder geval voor interne doeleinden) voor de minimumperiode van 10 jaar.
    vii. Indien nodig een leeg 'informed consent'-formulier.

Opslag en archivering van gegevens

11. Vertrouwelijke of privacygevoelige gegevens moeten op veilige en professionele wijze worden opgeslagen. De hoofdonderzoeker die met vertrouwelijke gegevens werkt wordt geacht een Data Management Plan te schrijven alvorens een onderzoeksproject te starten.[12] De hoofdonderzoeker moet zorg dragen voor de continuïteit van het onderzoek door de data, documentatie en

[11] Zie https://vunet.login.vu.nl/_layouts/SharePoint.Tridion.WebParts/download.aspx?cid=tcm%3a164-300366-16 (alleen Nederlandse versie)

[12] Onderzoekers kunnen de Data Steward van de faculteit raadplegen om na te gaan of een Data Management Plan voor hen verplicht is.

toegangsrechten gedurende het hele project te actualiseren. Onderzoekers moeten regelmatig **back-ups** maken van de onderzoeksdata.
Door de VU aangeboden opslagmethoden (Group Folder, Home Folder, projectfolder, SciStor, SURFdrive Research Drive) worden dagelijks gebackupt maar als u uw eigen apparaat gebruikt, zoals een laptop of USB-stick, moet u handmatig back-ups maken. Als u hulp nodig hebt, neem dan contact op met de IT Servicedesk of de RDM Support desk.

12. Bij publicatie archiveren onderzoekers hun ruwe data en verwerkte onderzoeksdata, tenzij zich nalevingsproblemen voordoen (bijv. licentieaspecten) of de opslag problemen oplevert (voor een aantal omvangrijke datasets; zie verderop in dit document). Onder archivering wordt verstaan: gegevens opslaan op een beveiligd systeem, samen met de datadocumentatie (zie punt 11 hierboven). Krachtens het beleid van de Vrije Universiteit moeten vertrouwelijke onderzoeksdata die niet relevant zijn voor verder onderzoek gedurende een periode van **10 jaar** veilig worden gearchiveerd. Gegevens die niet kunnen worden gearchiveerd, bijv. vanwege wettelijke beperkingen, moeten desondanks (in principe) controleerbaar zijn door de datadocumentatie te archiveren (punt 11 hierboven).

13. Veilige opslag en archivering veronderstellen dat er maatregelen zijn genomen zodat gegevens niet verloren kunnen gaan (gebruik van back-upfaciliteiten en behoorlijk onderhoud van de hardware) of kunnen lekken. Aanbevolen methoden (tegen vergoeding) voor *opslag (en uitwisseling) van gegevens van lopende onderzoeken* zijn te vinden in **Bijlage 1**. Aan NSCR verbonden onderzoekers die persoonsgegevens verwerken wordt geadviseerd om gebruik te maken van NSCR Secure Analytics Lab (SAL), een offline opslagfaciliteit.

14. Draagbare media zoals USB-sticks, externe harde schijven en opnamemedia mogen niet voor *langdurige* opslag worden gebruikt. Het *kortstondige* gebruik van deze gegevensdragers is wel toegestaan (bijv. voor de overdracht van gegevens), op voorwaarde dat de gegevens versleuteld zijn. Draagbare media moeten altijd in een afgesloten kast worden bewaard. Vertrouwelijke of privacygevoelige gegevens moeten uit deze gegevensdragers worden verwijderd wanneer u ze niet langer nodig hebt.

15. Wanneer het onderzoek is afgerond moet u de definitieve versie van uw onderzoeksdata en -documentatie archiveren. Slechts bevoegde personen kunnen verzoeken om toegang tot de gegevens, d.w.z. de oorspronkelijke onderzoeker of een onderzoekscoördinator. Aanbevolen methoden (tegen vergoeding) voor het *archiveren van onderzoeksdata* zijn te vinden in **Bijlage 2**.

    We raden archiveringsmethoden af waarbij de individuele onderzoekers een vergoeding betalen om de door de opslagfaciliteit verleende diensten te verlengen: in dit geval hangt de opslag namelijk af van de vraag of de individuele onderzoeker gedurende de periode van 10 jaar voor de faculteit werkzaam blijft. Een onderzoeker mag deze faciliteit alleen gebruiken wanneer de financiële verbintenis wordt overgeheveld naar de afdeling waar de onderzoeker werkzaam is.

16. Onderzoeksdata worden zoveel mogelijk in digitaal formaat opgeslagen, niet op papier. Bestandsformaten en andere standaarden moeten compatibel zijn met langdurige bewaring en

toegankelijkheid, de zogenaamde voorkeursformaten: .pdf, .txt, .csv, etc. Also, for picture or movie material the most long-term resistant format should be used. De datadocumentatie bevat informatie over de gebruikte bestandsformaten en softwareversies. Voor een lijst van open standaarden verwijzen we u naar de website *Forum Standaardisatie*.[13]

17. Gegevens die eigendom zijn van de onderzoeker moeten voor de minimale duur van 10 jaar in licentie worden gegeven aan de Vrije Universiteit, zodat het verrichte onderzoek in ieder geval kan worden gecontroleerd.

18. Afdelingshoofden worden geacht afspraken te maken met onderzoekers over het beheer van hun onderzoeksdata en documentatie in geval laatstgenoemden hun dienstverband bij de Vrije Universiteit opzeggen.

Uitwisseling van gegevens

19. Vertrouwelijk of privacygevoelige gegevens mogen alleen veilig en op 'need to know' basis worden uitgewisseld met derden. Aanbevolen methoden voor het *uitwisselen van onderzoeksdata* zijn te vinden in **Bijlage 1**.

20. Daarnaast mogen vertrouwelijke of privacygevoelige gegevens worden overgedragen via **SURF Filesender** (https://www.surffilesender.nl/, voor versleutelde bestanden < 2GB), **Zivver** (een encryptietool voor e-mailberichten, per mei/juni 2019 beschikbaar binnen de Vrije Universiteit), via SFTP (Secure File Transfer Protocol) of door gebruik te maken van een beveiligde USB-stick of ander opslagmedium.[14] Aan ontvangers buiten de Vrije Universiteit overgedragen vertrouwelijke bestanden moeten altijd worden versleuteld.

21. Vertrouwelijke of privacygevoelige gegevens mogen binnen het netwerk van de Vrije Universiteit per e-mail worden uitgewisseld, maar niet daarbuiten zonder aanvullende beveiligingsmaatregelen (zoals encryptie met Zivver).

Persoonsgegevens

22. Onderzoek dat gepaard gaat met de verwerking (bijv. verzameling, opslag, analyse, uitwisseling) van: Persoonsgegevens[15] is onderworpen aan de AVG en de Nederlandse uitvoeringswet. Onderzoekers moeten te allen tijde de AVG en de Nederlandse uitvoeringswet naleven.

---

[13] https://www.forumstandaardisatie.nl/open-standaarden

[14] https://vunet.login.vu.nl/services/pages/categorydetail.aspx?cid=tcm%3a164-884697-16&k=TCP:category=tcm:164-854736-1024&

[15] Wetenschappelijk onderzoek gaat vaak gepaard met de verwerking van persoonsgegevens. Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon wordt aangemerkt als persoonsgegevens. Een natuurlijke persoon kan direct worden geïdentificeerd aan de hand van een identificator zoals naam, geboortedatum, adres, foto's en/of stemopnames. De identificatie kan ook indirect zijn. Dit betekent dat gegevens die niet leiden tot directe identificatie van een persoon maar aan de hand waarvan een persoon redelijkerwijs nog altijd kan worden geïdentificeerd, ook moeten worden aangemerkt als persoonsgegevens. Met andere woorden: ook gepseudonimiseerde gegevens zijn persoonsgegevens.

Onderzoekers die in het kader van hun onderzoek persoonsgegevens verzamelen en verwerken moeten dit melden aan de Privacy Champion van de faculteit. Als onderzoekers werken met respondenten, kan het noodzakelijk zijn om een 'informed consent'-document op te stellen.

23. Overeenkomstig de AVG moeten onderzoekers altijd het beginsel van minimale gegevensverwerking in acht nemen; ze moeten het verzamelen van persoonsgegevens beperken tot gegevens die direct relevant en noodzakelijk zijn om het nagestreefde doel te bereiken.

24. Onderzoekers die voor hun onderzoek persoonsgegevens verzamelen en verwerken moeten dit vastleggen in een gegevensverwerkingsregister, met daarin onder meer (i) de verwerkte categorieën van persoonsgegevens, (ii) de doelstellingen en rechtsgrondslagen voor het verwerken van persoonsgegevens, (iii) de ontvangers van de gegevens, en (iv) de getroffen technische en beveiligingsmaatregelen om een passend beschermingsniveau van de verwerkte persoonsgegevens te waarborgen. De Vrije Universiteit gebruikt hiervoor Privacy Perfect. Neem contact op met de Privacy Champion van de faculteit als u hulp nodig hebt.

25. Naast 'reguliere' persoonsgegevens onderscheidt de AVG ook: *bijzondere categorieën van persoonsgegevens*). De verwerking van bijzondere categorieën van persoonsgegevens is verboden, behalve in de in de AVG en de Nederlandse uitvoeringswet genoemde gevallen. Bijzondere categorieën van persoonsgegevens zijn onder meer gegevens die betrekking hebben op ras of etnische afkomst, politieke opvattingen, religieuze overtuigingen, gezondheid of strafrechtelijke veroordelingen en strafbare feiten. Tot slot is het verboden om gegevens op te slaan die *BurgerServiceNummers* (BSN) bevatten.

26. Wanneer gegevensverwerking waarschijnlijk leidt tot een verhoogd privacyrisico, moet de onderzoeker een privacy-effectbeoordeling (PIA) uitvoeren om het institutionele risico van de gegevens en het vereiste beveiligingsniveau voor opslag te beoordelen. Neem contact op met de Privacy Champion van de faculteit als u hulp nodig hebt.

27. Persoonsgegevens moeten te allen tijde op een beveiligd netwerk en in overeenstemming met wettelijke richtlijnen worden opgeslagen. Computers moeten altijd worden vergrendeld als de onderzoeker afwezig is. De onderzoeker is bekend met de VUnet-pagina over de omgang met onderzoeksdata waarin persoonsgegevens zijn opgenomen.[16] Bij het verwerken van bijzondere categorieën van persoonsgegevens zijn aanvullende beveiligingsmaatregelen vereist voor de opslag ervan. De onderzoeker en zijn/haar onderzoeksgroep zijn verantwoordelijk voor gegevens die de maatschappij of onze faculteit in gevaar kunnen brengen. Persoonsgegevens mogen nooit worden opgeslagen op onbeschermde gegevensdragers (waaronder niet-versleutelde harde schijven in met een wachtwoord beveiligde computers) of op gesynchroniseerde cloud-diensten (Dropbox, Google drive), met name als deze 'spiegelen' met lokale, niet-versleutelde harde schijven. Na het onderzoek kunnen de gegevens op een beveiligde offline server zoals DarkStor worden gearchiveerd om zowel veiligheidsvereisten als de minimale archiveringstermijn in acht te nemen.

[16] https://vunet.login.vu.nl/services/pages/categorydetail.aspx?cid=tcm:165-849244-16&category=tcm:165-851780-1024

28. Onderzoekers moeten persoonsgegevens indien mogelijk **pseudonimiseren** voordat ze gegevens uitwisselen of opslaan. De encryptiesleutels die gepseudonimiseerde gegevens koppelen aan de persoonsgegevens moeten veilig en apart worden bewaard en te allen tijde toegankelijk zijn voor ten minste drie personen die verbonden zijn aan de Vrije Universiteit, vooral na het vertrek van de oorspronkelijke onderzoeker. Ook de hoofdonderzoeker en twee afdelingssecretarissen (van gerelateerde afdelingen) moeten toegang hebben tot de encryptiesleutels, die op ten minste twee beveiligde locaties met beperkte toegang moeten worden bewaard. De locaties waar de encryptiesleutels worden bewaard moeten fysiek (kluis) of elektronisch (H-schijf of ander beveiligd medium) afdoende worden beveiligd. Het ID-nummer van personen in de database mag geen elementen bevatten waaruit iemands identiteit kan worden afgeleid (waaronder initialen, geboortedatum, postcode).

29. **Encryptie** is een andere beveiligingsmaatregel waar onze voorkeur naar uitgaat. Aanvullende beveiligingsmaatregelen moeten voldoen aan de hierboven vermelde algemene vereisten: gegevens mogen niet verloren gaan door het verlies van een gegevensdrager, het vertrek van een onderzoeker of het verlies van één van de encryptiesleutels. Dit betekent met name dat ten minste twee aan de Vrije Universiteit verbonden personen te allen tijde toegang moeten hebben tot encryptiesleutels, ook na het vertrek van de oorspronkelijke onderzoeker, en dat gegevens en encryptiesleutels op ten minste twee locaties worden opgeslagen, beide met strikt beperkte en gereguleerde toegang. Aanbevolen encryptietools zijn Zivver (om e-mailberichten te versleutelen), SURFfilesender (om grote bestanden versleuteld te versturen), Veracrypt (om harde schijven, folders of opslagmedia te versleutelen), en Bitlocker (om delen van een harde schijf te versleutelen, voor computers met als besturingssysteem Windows). U kunt indien nodig de IT Servicedesk om hulp vragen.

30. Nadat het onderzoek is afgerond en/of de archiveringstermijn is verstreken, moeten alle gegevensdragers met daarop persoonsgegevens worden verwijderd met inachtneming van de wettelijke vereisten.

31. Als een onderzoeker persoonsgegevens die eigendom zijn van de Vrije Universiteit wil uitwisselen met derden (waaronder medeauteurs die niet aan de Vrije Universiteit verbonden zijn), moet de onderzoeker een zogenaamde **gegevensverwerkingsovereenkomst** aangaan. Dit is een wettelijke verplichting die waarborgt dat persoonsgegevens overeenkomstig de AVG worden verwerkt. De juridische afdeling van de Vrije Universiteit heeft hiertoe een model-gegevensverwerkingsovereenkomst opgesteld. De onderzoeker moet bij de Privacy Champion van de faculteit informeren naar de voorwaarden voor het uitwisselen van persoonsgegevens met personen buiten de Vrije Universiteit.

32. Overeenkomstig artikel 5, lid 1, punt f, en artikel 89, lid 1 van de AVG mogen persoonsgegevens langer dan 10 jaar worden opgeslagen als ze enkel voor wetenschappelijke doeleinden worden verwerkt en op voorwaarde dat passende technische en organisatorische maatregelen zijn genomen.

33. Als een onderzoeker aan de Vrije Universiteit persoonsgegevens van derden verwerkt, is hij of zij verantwoordelijk voor de veilige opslag zoals hierboven beschreven. De onderzoeker moet ervoor zorgen dat zijn/haar rol als verwerker naar behoren gedocumenteerd is in de "gegevensverwerkingsovereenkomst" die doorgaans wordt opgesteld door de eigenaar van de gegevens. Ook met eventuele vragen op dit punt kunt u bij de Privacy Champion van de faculteit terecht.

Internationale doorgifte van persoonsgegevens

34. Persoonsgegevens mogen alleen worden doorgegeven aan landen buiten de EER ("**internationale doorgifte**") als aan specifieke wettelijke voorwaarden wordt voldaan. Van een internationale doorgifte is bijvoorbeeld sprake wanneer persoonsgegevens worden opgeslagen op een server die zich in een land buiten de EER bevindt of wanneer iemand in een land buiten de EER de persoonsgegevens ontvangt of zich er toegang toe verschaft. De onderzoeker moet bij de Privacy Champion van de faculteit informeren naar de voorwaarden voor internationale doorgiften van persoonsgegevens.

35. Onderzoekers moeten persoonsgegevens verwijderen van hun mobiele apparaten (gegevensdragers) wanneer ze buiten de EER op reis zijn. Onderzoekers mogen zich daarnaast vanaf een locatie buiten de EER geen toegang verschaffen tot persoonsgegevens die opgeslagen zijn op door de Vrije Universiteit aangeboden of aanbevolen systemen. Vraag de IT Servicedesk om advies over passende beveiligingsmaatregelen wanneer u op reis bent.

36. Voor het verwerken van in niet-EER-landen verzamelde persoonsgegevens gelden mogelijk aanvullende regels. De onderzoeker wordt geacht de regels na te leven en contact op te nemen met de Privacy Champion van de faculteit.

Scripts, codes, specifieke soorten gegevens

37. Onderzoekers archiveren codes en scripts die ze hebben gebruikt om hun onderzoek uit te voeren. Hiertoe behoren C-codes, Matlab, SPSS, SAS, STATA, Eviews scripts, etc., waaronder een README-bestand over de taalversie of het pakket waarin de codes werden uitgevoerd. Tot slot moeten onderzoekers een lijst opnemen van alle bestanden, met een korte beschrijving (register of inhoudsopgave).

38. **Secundaire gegevens** zijn gegevens die door bijvoorbeeld derden worden verzameld ten behoeve van hun eigen onderzoek; gegevens die intern worden verzameld door bedrijven; of gegevens die worden verzameld door instellingen die gespecialiseerd zijn in gegevensverzameling, zoals CBS, Data Archiving and Networked Services (DANS), Nationaal Cyber Security Centrum (NCSC), het Korps Landelijke Politiediensten, de Nederlandse Raad voor de rechtspraak, etc. Als de gegevensaanbieder archivering van de secundaire gegevens toestaat, dan is dit de voorkeursoptie. Secundaire gegevens hoeven echter niet te worden gearchiveerd als de gegevens (in principe) kunnen worden hersteld (eventueel na het betalen van een vergoeding of het leggen van de juiste contacten). De datadocumentatie moet nog altijd worden gearchiveerd, waaronder het verzamelen van de ruwe en opgeschoonde data. Onderzoekers moeten verwijzen naar de bron van

de (secundaire) gegevens en DOI en voldoende informatie opnemen over hoe de gegevens zijn verkregen en ontsloten. Tot slot zijn details (en mogelijk scripts) over hoe ruwe data (mogelijk gepatenteerd of commercieel) wordt omgezet in gegevens die worden gebruikt voor de empirische analyse, zoals bij de normale gang van zaken, van belang om inzicht te krijgen in het proces. Dit omvat het vermelden van zakelijke relaties als de gegevens zijn verkregen door contacten met het bedrijfsleven of als overeenkomsten met de organisatie het lokaal archiveren van de gegevens binnen de Vrije Universiteit verbieden.

39. **Omvangrijke datasets** Sommige datasets zijn te omvangrijk voor (standaard)opslag. In dit geval zullen onderzoekers de beste praktijken binnen hun vakgebied toepassen en deze expliciet delen met de Data Steward van de faculteit, Thomas Hoogenboom <t.m.hoogenboom@vu.nl> of de RDM Support Desk <rdm@vu.nl>, zodat de faculteit op dit gebied concreet beleid kan ontwikkelen. In alle gevallen, waaronder studies met grote datasets, moet de gegevensverzameling worden gedocumenteerd en gearchiveerd en voldoende informatie bevatten, zodat het gepubliceerde onderzoek (in principe) kan worden gecontroleerd.

Slotbepaling

40. Eventuele uitzonderingen op dit Beleid moeten door het faculteitsbestuur worden goedgekeurd na het advies van het onderzoeksbestuur, de Data Steward van de faculteit en de Privacy Champion te hebben ontvangen.

Praktische tips en ondersteuning

41. Raadpleeg de onderzoekscyclus in **Bijlage 3** voor een stapsgewijze benadering van Research Data Management.

42. Kijk op de website van de Universiteitsbibliotheek voor *beste praktijken* en richtlijnen als het gaat om het beheer van onderzoeksdata. Meer informatie over de omgang met onderzoeksdata die deels bestaan uit persoonsgegevens is te vinden op VUNet. Voor advies over de opslag van onderzoeksdata kunnen onderzoekers te rade gaan bij Thomas Hoogenboom, Data Steward van de Faculteit der Rechtsgeleerdheid < t.m.hoogenboom@vu.nl>. Met vragen over onderzoek dat gepaard gaat met persoonsgegevens kunt u terecht bij de Privacy Champion van de faculteit, Jacqueline Draaisma: <j.a.draaisma@vu.nl>. Tot slot biedt de RDM Support Desk <rdm@vu.nl> ondersteuning aan alle onderzoekers die verbonden zijn aan de Vrije Universiteit.

BIJLAGEN

Bijlage 1 Aanbevolen methoden voor het opslaan en uitwisselen van gegevens tijdens het onderzoek											
	Persoonlijk apparaat	VU Home Folder (H:)	VU Group Folder (G:)	Projectfolder van VU-netwerk (3GB)	Google Apps VU (onbeperkt)	SURF ResearchDrive (> 250 GB ; max. 2 TB)	VU SQL Database	SURF drive (<250 GB)	EDUgroepen (250 Dagelijks	Draagbare gegevensopslag	SciStor (eenheden van 100
Niet-vertrouwelijke gegevens	X	√	√	√	√	√	√*	√	√	√	√
Gepseudonimiseerde gegevens	X	X	√	√	X	√	√*	√*	√*	√*	√
Vertrouwelijke of privacygevoelige gegevens	X	X	√*	√*	X	√	√*	√*	X	X	√
		* Op voorwaarde dat aanvullende beveiligingsmaatregelen van kracht zijn, zoals beheer van toegangsrechten voor gebruikers, antivirus & encryptie									
Uitwisseling ja/nee	X	X	√	√	√	√	X	√	√	X	√

Bijlage 2 Aanbevolen methoden voor het archiveren van gegevens na het onderzoek				
	ArchStor	DarkStor	DataverseNL	
Vertrouwelijkheidscategorie				
Niet-vertrouwelijke gegevens	√	√	√	
Gepseudonimiseerde gegevens	X	√	X	
Vertrouwelijke gegevens	X	√	X	

Bijlage 3 Onderzoekscyclus	
1	Beginfase onderzoek: ga na of u een Data Management Plan moet schrijven waarin u vermeldt welke gegevens u gaat (her)gebruiken. Overweeg het gebruik van de online tool DMP. Gaat u (bijzondere categorieën van) persoonsgegevens verwerken? Ja: ga naar 2. Nee: ga naar 4.
2	Ga te rade bij de Privacy Champion en stel indien nodig samen een PIA op. Gaat u werken met respondenten en hebt u hun toestemming nodig? Ja: ga naar 3 Nee: ga naar 4.
3	Stel een 'informed consent'-formulier op in overeenstemming met de AVG.
4	Is een ethische toetsing vereist? Benader CERCO en breng uw Data Management Plan ter sprake. Ga naar 5.
5	Tijdens onderzoek: archiveer alle documenten, Data Management Plan, CERCO-aanvraag en -advies, toestemmingen van derden, algemene voorwaarden van diensten die u gaat gebruiken, etc. Archiveer uw gegevens en beschrijf welke opslagmedia u gebruikt, welke bestanden u aanmaakt (bestandenlijst) en welke variabelen u hebt. Gebruik versies. Ga naar 6.
6	Sla uw gegevens op overeenkomstig het door de Faculteit der Rechtsgeleerdheid van de Vrije Universiteit gehanteerde beleid inzake RDM. Als u gebruikmaakt van andere gegevensdragers, vermeld dan waarom, volgens het principe 'toepassen of uitleggen'. Ga naar 7.
7	Na het onderzoek: zorg ervoor dat uw gegevens en documenten volledig zijn en los van elkaar kunnen worden begrepen. Archiveer uw gegevens en documenten op betrouwbare wijze, volgens het motto "zo open mogelijk, maar indien nodig afgeschermd".

Bijlage 4 Beschrijving van methoden voor opslag, uitwisseling en archivering	
Methode	**Beschrijving**
ArchStor	Methode voor archivering. Een archief met onderzoeksdata die 10 jaar lang worden bewaard. In ArchStor opgeslagen data zijn alleen toegankelijk voor verificatiedoeleinden. Enkel niet-vertrouwelijke gegevens.
DarkStor	Methode voor archivering. Een offline archief voor het opslaan van vertrouwelijke of privacygevoelige gegevens. DarkStor is alleen bestemd voor gegevens die specifiek extra beveiliging behoeven. Eenmaal gearchiveerd zijn de gegevens enkel toegankelijk voor bevoegde personen, d.w.z. de oorspronkelijke onderzoeker of een onderzoekscoördinator.
DataverseNL	Methode voor archivering. Een online platform voor de analyse en publicatie van onderzoeksdata in een halfopen omgeving. Met DataverseNL kunnen gebruikers publicaties rechtstreeks koppelen aan datasets, en delen via online archieven zoals DANS. Enkel niet-vertrouwelijke gegevens.
EDUgroepen	Methode voor uitwisseling en samenwerking. Hulpmiddel voor het hoger onderwijs in Nederland. EDUgroepen is gebaseerd op Microsoft SharePoint Server 2016. Gebruikers werken samen via een teamsite. Met teamsites kunt u onder andere documenten uitwisselen, bijeenkomsten plannen, projecten documenteren en taken verdelen. U beschikt over een totale opslagcapaciteit van 5 GB. Toegankelijk via https://www.edugroepen.nl – log in met uw VU e-mailaccount.
Google Apps VU	Opslagmethode. Kan ook worden gebruikt om data binnen de VU uit te wisselen, maar niet met derden. De Vrije Universiteit heeft een institutionele overeenkomst met Google gesloten over Google Drive/Docs. Deze is toegankelijk via

	http://accounts.google.com – log in met uw VU e-mailaccount > selecteer VU. Enkel niet-vertrouwelijke gegevens.
Group Folder (G://)	Methode voor opslag en uitwisseling. De Group Folder kan worden gebruikt om onderzoeksdata te delen met een groep, hetzij binnen de rechtenfaculteit of met onderzoekers binnen andere faculteiten van de Vrije Universiteit. De standaard opslagcapaciteit is 1 GB per medewerker, maar dit kan worden verhoogd.
Home Folder (H://)	Opslagmethode. De standaard opslagcapaciteit is 3 GB. Deze capaciteit kan worden verhoogd; de kosten daarvan worden in rekening gebracht aan de faculteit.
Projectfolder	Methode voor opslag en uitwisseling. Medewerkers en gasten die binnen de Vrije Universiteit samenwerken aan een project kunnen gegevens opslaan in een projectfolder. De kosten van een projectfolder worden in rekening gebracht aan de aanvrager/manager (bijvoorbeeld de faculteit of afdeling die het project opzet). Er is een opslagcapaciteit van 3 GB beschikbaar per persoon; dit kan worden verhoogd. Een projectfolder kan worden aangevraagd via VUNet.
SURF ResearchDrive	Een gezamenlijke online omgeving waar onderzoekers grote hoeveelheden onderzoeksdata (> 250 GB; max. 2 TB) veilig kunnen opslaan en uitwisselen met partners in binnen- en buitenland. SURF ResearchDrive is een betaalde dienst.
SciStor	Methode voor opslag en uitwisseling. SciStor is een door de VU beheerde faciliteit voor de opslag van onderzoeksdata. Het is een betaalde dienst die tevens kan worden gebruikt voor de opslag van vertrouwelijke of privacygevoelige gegevens. Niet geschikt voor archivering. Het minimale gebruik is 100 GB voor ten minste drie maanden. De capaciteit kan worden verhoogd of verlaagd in eenheden van 100 GB. SciStor kan worden aangevraagd via VUNet.
SURFDrive	SURFdrive is een gepersonaliseerde cloud-opslagdienst voor het Nederlandse hoger onderwijs en onderzoek waarmee medewerkers en onderzoekers eenvoudig data kunnen opslaan, synchroniseren en uitwisselen. U kunt met behulp van uw VUnetID en wachtwoord inloggen op https://surfdrive.surf.nl. Elke medewerker krijgt 250 GB opslagcapaciteit.
VU SQL Database	Veelal gebruikt voor de opslag van statistische gegevens. De standaard opslagcapaciteit is 1 GB. U kunt extra capaciteit aanvragen. Een VU SQL Database kan worden aangevraagd via VUNet.

Versienummer	**Datum**	**Auteur**	**Opmerkingen**
0.10	18 juni 2019	Joost Meijer Marieke Polhout	Aan het faculteitsbestuur voorgelegde definitieve ontwerp
0.11	27 juni 2019	Joost Meijer	Een nalevingsclausule is ingevoegd op verzoek van het faculteitsbestuur
1.0	9 juli 2019	Joost Meijer	Beleid goedgekeurd door het faculteitsbestuur
2.0	2 november 2020	Jacqueline Draaisma	Voorgelegd aan het OGV
2.1	22 april 2021	Jacqueline Draaisma	Voorgelegd aan het OGV