Hogeschool van Amsterdam

Dataprotocol *Research Data Management*

Kenniscentrum FDMCI

Auteur: Thierry P.F. Verburgh

Datum: 01-07-2019

Versie: 1.2

Tot stand gekomen in samenwerking met:

- Jan Meijer en Gerald Stap, Servicemanagement bij FDMCI (HvA)
- Ben Kröse, lector Digital Life bij FDMCI (HvA)
- Miriam Rasch, docent-onderzoeker lectoraat Netwerkcultuur bij FDMCI (HvA)
- Pavel van Deutekom, Office Manager MediaLAB bij Studio HvA (HvA)
- Bernadette Schrandt, docent-onderzoeker lectoraat Crossmedia bij FDMCI (HvA)
- Maarten Groen, docent-onderzoeker lectoraat Visual Methodologies bij FDMCI (HvA)
- Riemer van Roozen, projectleider Live Game Design bij lectoraat Play & Civic Media (HvA)
- Mariëtte van Selm, projectmanager RDM-support (UvA/HvA)
- Janna Toebosch, RDM-specialist (HvA)
- Maarten Sloëtjes, Information Security Officer bij FDMCI (HvA)
- Maarten Rottschäfer, Hoofd Bedrijfsvoering Onderzoek, Kenniscentrum FDMCI (HvA)

Managementsamenvatting

Met dit document wordt het verantwoord verzamelen, beheren, verwerken, opslaan, en delen van onderzoeksdata binnen onderzoeksprojecten aan specifieke voorwaarden verbonden door middel van facultair beleid in de vorm van een dataprotocol.

Het eerste deel van dit protocol is toegespitst op onderzoekers om hen kort en bondig te laten weten wat *research datamanagement* is. In de handreiking (deel 2) is nadere informatie te vinden over het beheren van onderzoeksdata, zoals welke specifieke ethische en juridische kwesties belangrijk zijn om rekening mee te houden, verantwoordelijkheden, het opstellen van een Data Management Plan, versiebeheer en het maken van *back-ups*, het beveiligen van onderzoeksdata, veilige omgang met privégevoelige persoonsgegevens, het verantwoordelijk publiceren van onderzoeksdata, het correct archiveren van onderzoeksdata, en richtlijnen omtrent intellectueel eigendom. Hierbij is uitgegaan van de algemeen geldende gedragscode praktijkgericht onderzoek voor het hbo.

Een nieuwe voorwaarde rond *research datamanagement* behelst een intakegesprek bij het opstarten van nieuwe projecten waarbij onderzoekers een Data Management Plan (DMP) invullen.

Inhoudsopgave

INTRODUCTIE

In alle fasen van datagebruik – van het creëren en verzamelen van onderzoeksdata tot en met het archiveren en openstellen van hiervan – spelen ethische, organisatorische, juridische en privégevoelige aspecten een belangrijke rol. In april 2015 heeft het CvB centrale richtlijnen vastgesteld voor *research datamanagement* (**RDM**), oftewel het proces voor, tijdens en na een onderzoekstraject van systematisch en verantwoord organiseren, beschrijven, opslaan, bewaren, delen, hergebruiken en citeren van onderzoeksdata bij de UvA en HvA. De centrale RDM-richtlijnen zijn per faculteit uitgewerkt in een dataprotocol, ook met het oog op de nieuwe Algemene verordening gegevensbescherming (AVG). Dit dataprotocol voor Kenniscentrum FDMCI helpt je als onderzoeker om voor, tijdens, en na je onderzoek op een verantwoorde manier je onderzoeksdata te beheren.

Het eerste deel van dit protocol betreft een beknopte handleiding voor onderzoekers om onderzoeksdata zo snel en efficiënt mogelijk te beheren. Het is daarom toegespitst op onderzoekers. In de handreiking (deel 2) kun je nadere informatie vinden over het beheren van onderzoeksdata, zoals welke specifieke ethische en juridische kwesties belangrijk zijn om rekening mee te houden, alsook de specifieke eisen en uitzonderingen voor het verwerken en opslaan van onderzoeksdata.

Het dataprotocol is een levend document en wordt geactualiseerd door de datasteward. De datasteward is verantwoordelijk voor de toezicht op de uitvoering van *research datamanagement* binnen het Kenniscentrum FDMCI. Voor vragen en advies over RDM kun je bij de datasteward terecht.[1]

Dit protocol is gebaseerd op de protocollen van het Amsterdams Kenniscentrum voor Maatschappelijke Innovatie (AKMI), het Kenniscentrum Onderwijs en Opvoeding, en vorige versies van het dataprotocol van Kenniscentrum FDMCI. Het is aangepast op basis van gesprekken met de verschillende lectoraten en onderzoekers binnen FDMCI, alsook gesprekken met de RDM-specialisten van de Hogeschool van Amsterdam en de Universiteit van Amsterdam.

---

[1] Thierry P.F. Verburgh (t.p.f.verburgh@hva.nl) is de datasteward van Kenniscentrum FDMCI.

Hogeschool van Amsterdam

Deel 1. Research datamanagement in vogelvlucht

RESEARCH DATAMANAGEMENT-DOELEN

Met dit dataprotocol worden door middel van *research datamanagement* zes doelen nagestreefd om vóór, tijdens, en na het onderzoek op een verantwoorde manier om te gaan met onderzoeksdata. Deze doelen zijn in onderstaande hoofdstukken uitgewerkt.

1. Verantwoordelijkheid

Onderzoekers zijn verantwoordelijk voor hun onderzoeksdata:

- Zij weten waar het te vinden is.
- Zij weten hoe het georganiseerd is.
- Zij zorgen ervoor dat het veilig opgeslagen en verwerkt is.
- Zij maken het toegankelijk en overzichtelijk voor zichzelf en eventueel anderen.
- Zij zorgen ervoor dat persoonsgegevens geanonimiseerd of gepseudonimiseerd ontsloten worden.

Voor iedere *dataset* zijn tenminste twee onderzoekers verantwoordelijk. Dit is ook het geval wanneer het onderzoek alleen is uitgevoerd – in dat geval heb je een 'gegevensmaatje' in de vorm van een waarnemer nodig. Voor verdere informatie over de verantwoordelijke omgang met onderzoeksdata, zie pagina 16.

Voor ieder nieuw onderzoek wordt een Data Management Plan (DMP) ingevuld en bijgehouden, waarin opgenomen wordt hoe de omgang met onderzoeksdata eruit zal gaan zien. De hoofdonderzoeker is verantwoordelijk voor het DMP. Zie voor verdere uitleg pagina 18.

2. Veilige opslag

Onderzoeksdata moeten veilig opgeslagen worden. Om een veilige opslag van onderzoeksdata te garanderen moeten er altijd twee digitale reservekopieën worden aangemaakt van de data, verdeeld over twee digitale platformen. Reservekopieën moeten regelmatig geactualiseerd en gecontroleerd worden zodat er altijd een recente kopie beschikbaar is. Zie hiervoor pagina's 10 en 17-20.

3. Efficiënte documentatie

Onderzoeksdata moeten goed en efficiënt georganiseerd en gedocumenteerd worden. Dit doe je door in verschillende documenten te omschrijven waar alles is gearchiveerd, door te omschrijven hoe archiveringsstructuren in elkaar zitten, en door te omschrijven waar afkortingen, termen, en andere waarden voor staan in onderzoeksbestanden. Hiermee kunnen toekomstige onderzoekers sneller en makkelijker gebruik maken van je onderzoeksdata. Zie hiervoor pagina's 10-11.

4. Vertrouwelijke omgang privégevoelige data

Onderzoekers gaan op een vertrouwelijke manier met beheren van privégevoelige gegevens om. Hiervoor wordt dataminimalisatie toegepast op de onderzoeksdata, en daarnaast worden overeenkomsten en *informed consents* (instemmingsverklaringen) ondertekend. Dataminimalisatie wordt nagestreefd door irrelevante persoonsgegevens *niet* te verwerken in het onderzoek, en zeker niet in gedeelde en publieke *output*, zoals publicaties en publiek opengestelde databeses. Indien persoonsgegevens van onderzochte personen anoniem moeten blijven zorgt de onderzoeker ervoor dat deze gegevens geanonimiseerd of gepseudonimiseerd worden. Tevens is de onderzoeker zoveel mogelijk op de hoogte van (vernieuwde) wetgeving en richtlijnen rond het verzamelen en verwerken van persoonsgegevens. Zie voor nadere uitleg hoe om te gaan met privégevoelige persoonsgegevens pagina's 12-15 en 19-20.

5. Langdurige opslag

Onderzoeksdata moeten langdurig opgeslagen worden. Hiermee wordt de duurzaamheid van naarstig verzamelde en bewerkte waardevolle data gewaarborgd zodat dit voor een langere periode beschikbaar en toegankelijk blijft. Hierdoor hoeven tijdens en na de periode dat de data zijn opgeslagen niet opnieuw dezelfde gegevens verzameld worden. De HvA hanteert voor het archiveren en opslaan een standaardbewaartermijn van 10 jaar. Wanneer subsidiegevers andere bewaartermijnen eisen worden hun tijdslimieten gehanteerd. Zie hiervoor pagina's 11 en 21-22.

6. Delen: kennisdisseminatie, transparantie, samenwerking, en hergebruik

Onderzoeksdata moeten na, en in sommige gevallen tijdens, het onderzoek gedeeld worden. Dit kan via het *online*-systeem UvA/HvA figshare. Dit wordt dan automatisch geïmporteerd naar Pure. Toegang kan variëren van openbaar tot en met privé (waarbij buiten de onderzoeker om

niemand toegang krijgt tot de data). De HvA hecht groot belang aan het openbaar maken van onderzoeksdata door middel van het *open access*-beleid, al dan niet geanonimiseerd of gepseudonimiseerd. Daarom is het uitgangspunt van de faculteit dat onderzoeksdata altijd openbaar beschikbaar worden gemaakt – hou hierbij wel rekening met dataminimalisatie, anonimisering en pseudonimisering. Zie hiervoor pagina's 11 en 20-22.

Onderzoeksdata spelen een belangrijke rol in verschillende onderzoeksfasen. In het beleidsstuk RDM van het CvB worden de volgende definities van onderzoeksdata geciteerd:

> '[…] research data are defined as factual records (numerical scores, textual records, images and sounds) used as primary sources for scientific research, and that are commonly accepted in the scientific community as necessary to validate research findings. A research data set constitutes a systematic, partial representation of the subject being investigated'.

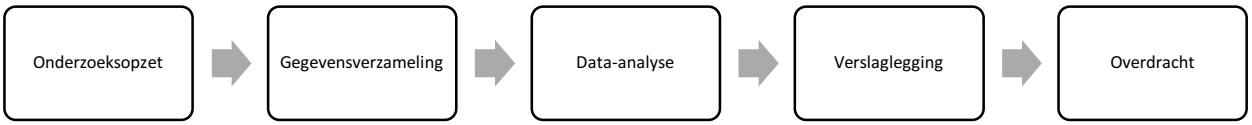
Daarnaast wordt de term '*big data*' ook vaak in de context van RDM gebruikt. Het betreft een onderdeel van onderzoeksdata, en om het verschil te verduidelijken kan *big data* als volgt gedefinieerd worden:

> '[…] The term "big data" refers to large amounts of different types of data produced with high velocity from a high number of various types of sources. Handling today's highly variable and real-time datasets requires new tools and methods, such as powerful processors, software and algorithms'

De onderzoekscyclus

De rol van onderzoeksdata wordt in het onderstaande schema weergegeven in een zogenoemde onderzoekscyclus. Hierin zijn verschillende onderzoeksfasen gedefinieerd van het opstellen van de onderzoeksvraag tot het publiceren van de eindresultaten van het onderzoek. Gedurende deze onderzoekscyclus zal de onderzoeksdata een *datamanagement*-cyclus doorlopen van planning; verzamelen, opslaan, beheren, beschrijven; interpreteren, combineren, anonimiseren; en uiteindelijk delen, citeren, hergebruiken en archiveren.

Er zijn verschillende verwerkings- en opslagactiviteiten nodig gedurende een onderzoekscyclus:



Tijdens en na iedere stap in deze onderzoekscyclus moeten een aantal praktische zaken geregeld zijn. Alle stappen zijn verplicht tenzij gemarkeerd als 'aanbevolen'.

Onderzoeksopzet

1. **Het samenstellen van een Datamanagementplan**
   Met een Datamanagementplan leg je vast hoe je je onderzoeksgegevens zal beheren (zie hiervoor pagina 16).

2. **Het aanwijzen van digitale opslagplaatsen**
   Voordat onderzoek verricht zal worden moeten er diverse digitale opslagplekken geregeld worden om *voor* en *tijdens* het onderzoek data op te kunnen slaan. Aangeraden wordt om tijdens het onderzoek data op minimaal twee verschillende soorten digitale dragers op te slaan (gelieve de keuze van deze drie digitale dragers te verantwoorden in je DMP). Denk hierbij aan de volgende mogelijkheden:
   1. (Aanbevolen) SURFdrive: op Surfdrive kun je een onderzoeksmap aanmaken die toegankelijk is voor jezelf of andere deelnemende onderzoekers. HvA SURFdrive heeft veel dezelfde mogelijkheden als Dropbox. Het kan daarnaast geïntegreerd worden op je computer, waardoor je makkelijker via je computer kan werken met de gegevens zonder bestanden over te hoeven zetten, ook offline. Nu wordt er veel gebruik gemaakt van Dropbox. Vanuit het beleid van de HvA moet echter in plaats hiervan gebruik gemaakt worden van SURFdrive, waarvan de servers in Nederland gesitueerd zijn. Dropbox staat op een Amerikaanse server en hun kantoor is in de VS gesitueerd. Hierdoor valt Dropbox onder de Patriot Act, waardoor de federale overheid van de Verenigde Staten beslag kan leggen op hun gegevens. Hierdoor kunnen we niet garant staan voor de bescherming van privégevoelige informatie.
   2. (Aanbevolen) HvA V:-schijf: op de HvA V:-schijf van het kenniscentrum kun je een onderzoeksmap aanmaken die je kan beveiligen, zodat alleen jij (of mensen waar je toestemming aan hebt gegeven) de bestanden kan raadplegen, wijzigen en aanvullen. De V:-schijf kan geïntegreerd worden op Windows en Apple computers/laptops, waardoor je makkelijker via je computer kan werken met de gegevens zonder bestanden over te hoeven zetten, ook offline.
   3. (Aanbevolen) UvA/HvA figshare: middels UvA/HvA figshare kunnen diverse soorten bestanden opgeslagen worden, zoals publicaties, maar ook *datasets*. Tijdens en na je onderzoek heb je de mogelijkheid om je bestanden af te schermen of openbaar te maken. Tevens kan UvA/HvA figshare gebruikt worden om onderzoeksgegevens met partners te delen die geen toegang hebben tot SURFdrive of je HvA V:-schijf.
   4. (Niet aanbevolen) Eigen computer, laptop of HvA Windows-account: het opslaan van onderzoeksgegevens op de interne harde schijf van een eigen computer of laptop is niet toereikend genoeg omdat dit niet voldoende veiligheid en back-upmogelijkheden geeft. Deze apparaten kunnen gestolen worden of kwijtraken, ze kunnen kapotgaan of het begeven, de HvA kan gegevens moeilijk achterhalen

wanneer een onderzoeker uitvalt of vertrekt, en ze bieden vaak van zichzelf geen tweede back-upmogelijkheid aan. Onderzoeksgegevens opslaan in de eigen 'documenten-map' op de eigen HvA Windows-account zal het ook moeilijker maken om gegevens te achterhalen voor de HvA.

5. (Niet aanbevolen) losse opslagmedia: een usb-stick of externe harde schijf kan makkelijk kwijtraken, gestolen worden, of kapotgaan.
6. Als je niet genoeg hebt aan bovenstaande opties neem dan contact op met de datasteward van je kenniscentrum om via die persoon een maatwerkoplossing te verkrijgen bij ICTS.

3. Omschrijvingen documentatie en archivering ten behoeve van efficiënt gebruik

Vooraf aan het onderzoek wordt een README-bestand aangemaakt op het hoogste niveau van de projectmap. Dit bestand geeft gedurende en na het onderzoek op een toegankelijke manier weer hoe de hoofd- en deelmappen gedocumenteerd en gearchiveerd zijn. Als het project een complexe mappenstructuur heeft zou het bestand deze moeten weergeven. Gedurende het onderzoek wordt het README-bestand bijgehouden en aangevuld. Door het README-bestand in platte tekstopmaak op te slaan kan het nu en in de toekomst makkelijk gelezen en ingevoegd worden in andere systemen. Microsoft Word lijkt nu handig, maar is misschien over vijftien jaar niet meer gemakkelijk te lezen.

Verder moet vooraf aan het onderzoek het volgende goed en efficiënt georganiseerd en gedocumenteerd worden ten behoeve van toekomstig gebruik door jou of anderen:

- een heldere hiërarchie van mappen en bestanden in projectmappen van papieren archieven, alsook op digitale dragers;
- een taxonomie voor papieren archieven om de indeling van de papieren *dataset* te beschrijven.
- een logboek voor de duiding van ruwe onderzoeksdata;
- een codeboek voor bewerkte data en kwantitatieve *datasets* die voor digitale *software* bedoeld zijn. In dit codeboek worden de variabelen, methoden en analyses beschreven, en het moet voldoende gedetailleerd zijn om het onderzoek in de toekomst te kunnen controleren en herhalen.

4. Het regelen en opslaan van overeenkomsten en instemmingsverklaringen

Vooraf aan de gegevensverzameling van ieder onderzoeksproject regelt de onderzoeker indien van toepassing dat er overeenkomsten worden afgesloten met partners en de te onderzoeken personen. De hoofdonderzoeker regelt de volgende overeenkomsten en slaat dit vervolgens op in de onderzoeksmap:

- Ethisch protocol en toetsing van de ethische commissie.

- *Informed consent*-formulieren (toestemmingsformulieren en instemmingsverklaringen), inclusief voorlichtingsdocumenten voor deelnemers.
- Samenwerkingsovereenkomsten, inclusief afspraken over eigenaarschap en publiceren.
- Gebruikersovereenkomsten van systemen en platformen.

Gegevensverzameling

Alvorens de data-analyse slaat de hoofdonderzoeker de volgende materialen op het gekozen opslagmedium op:

i. De originele, ruwe *datasets* zoals ze verzameld zijn. Wat dit voor bestanden zijn is afhankelijk van het onderzoek (audiobestanden, gescande vragenlijsten, de gedownloade bestanden van een enquête etc.)
ii. Vragenlijsten, itemlijsten, observatieschema's, etc. die gebruikt zijn om de data te verzamelen.
iii. (Aanbevolen) onderzoeksgegevens gereedgemaakt voor analyse, zoals gespreksverslagen voor interviews.
iv. In geval van kwantitatieve *data*: een codeboek met een beschrijving van alle variabele namen en *labels* in voldoende detail zodat zowel de ruwe als verwerkte gegevens te begrijpen zijn.
v. Contactgegevens van mensen die zijn onderzocht worden apart bewaard en opgeslagen, waarnaast een apart sleutelbestand wordt gehanteerd voor eigen gebruik om de codes die aan deze deelnemers zijn toebedeeld te kunnen ontcijferen.

NB Sla ook de onderzoeksgegevens die studenten hebben verzameld en bewerkt op.

Data-analyse en verslaglegging

Na de data-analyse slaat de hoofdonderzoeker de volgende bestanden op:

i. Alle syntaxen/codeerschema's die gebruikt zijn om de onderzoeksdata te analyseren.
ii. (Aanbevolen) een bestand met aantekeningen over de data-analyse van specifieke onderzoekselementen (respondenten/organisaties/etc.)
iii. (Aanbevolen) een lijst van deelnemers die niet in de analyses zijn meegenomen, plus de reden van exclusie.
iv. *Datasets* zoals gebruikt voor de uiteindelijke analyses.
v. (Aanbevolen) statistische *output*-bestanden (bijv. SPSS) of codeboeken (bedenk dat niet iedereen beschikt over de bijbehorende analyseprogramma's, dus gelieve *output*-bestanden toevoegen die ook zonder het programma gelezen kunnen worden).

Let op: na het onderzoek worden contactgegevens vernietigd en persoonsgegevens in verslaglegging geanonimiseerd of gepseudonimiseerd.

Overdracht: delen en archiveren

1. Na ieder project moeten de onderzoeksdata worden opgeslagen in Uva/HvA figshare. Daarvoor moeten **metadata** en databestanden worden aangeboden volgens de eisen van UvA/HvA figshare.
2. Nogmaals: na het onderzoek worden persoonsgegevens geanonimiseerd of gepseudonimiseerd, zeker wanneer dit gedeeld wordt.

DISCLAIMER wanneer iets onduidelijk is vraag dan aan de datasteward of je de persoonsgegevens die je op het oog hebt voor je onderzoek mag verwerken, alsook op welke manier.

1. Grondslagen voor de verwerking van persoonsgegevens

Voor de verwerking moet er expliciet aan de volgende aanvullende voorwaarden worden voldaan.

Grondslag 1. Algemeen belang:
In combinatie met het expliciet voldoen aan grondslagen 2 en/of 3 mogen er in beginsel binnen de wetenschap persoonsgegevens verwerkt worden omdat:

- de verwerking gebaseerd kan worden op de grondslag taakvervulling van een algemeen belang;[2] doordat
- de verwerking binnen en door instellingen en diensten wordt verricht die wetenschappelijk onderzoek of statistiek verrichten.[3]

Grondslag 2. Wel of geen instemmingsverklaring regelen van een individu:
Als onderzoeker moet je je kunnen beroepen op de volgende grondslag:

- Uitdrukkelijke toestemming van de onderzochte persoon (en/of diens ouder of voogd) middels een ondertekende *informed consent* (instemmingsverklaring).

Uitzonderingen hierop zijn als volgt, en moeten goed beargumenteerd kunnen worden in het onderzoeksplan:

- Voor de verwerking van persoonsgegevens die door het individu zelf reeds openbaar zijn gemaakt hoeft geen uitdrukkelijke toestemming worden gevraagd.[4] Er is in zulke gevallen geen informatieplicht om iedereen gelijk afzonderlijk te informeren. Zorg in deze gevallen er wel voor dat informatie over de verwerking van persoonsgegevens openbaar kan worden gemaakt wanneer onderzochte personen hierom vragen.[5] Hierdoor kunnen zij alsnog verwittigd worden waarom hun persoonsgegevens worden onderzocht. Doe dit door hen binnen een maand per e-mail te beantwoorden.[6]
- Wanneer het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost, zoals het analyseren van duizenden Twitter-accounts, dan

---

[2] Eerste Kamer der Staten-Generaal, *Uitvoeringswet Algemene Verordening Gegevensbescherming* (’s-Gravenhage 2018), art. 24; Bart W. Schermer, Dominique Hagenauw & Nathalie Falot, *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming* (’s-Gravenhage 2018), 48.

[3] Eerste Kamer der Staten-Generaal, *Uitvoeringswet*, art. 44.

[4] Europese Unie, *Algemene verordening gegevensbescherming* (2016), art. 9 lid 2, www.privacy-regulation.eu/nl/artikel-9-verwerking-van-bijzondere-categorieen-van-persoonsgegevens-EU-AVG.htm.

[5] Schermer, Hagenauw & Falot, *Handleiding*, 75-77.

[6] Schermer, Hagenauw & Falot, *Handleiding*, 473.

hoeft hier geen toestemming voor worden gevraagd aan het individu.[7] Ook in deze gevallen is er geen informatieplicht om iedereen gelijk afzonderlijk te informeren. Zorg in deze gevallen er wel voor dat informatie over de verwerking van persoonsgegevens openbaar kan worden gemaakt wanneer onderzochte personen hierom vragen.[8] Hierdoor kunnen zij alsnog verwittigd worden waarom hun persoonsgegevens worden onderzocht. Doe dit door hen binnen een maand per e-mail te beantwoorden.[9]

Grondslag 3. Gerechtvaardigd belang:

Daarnaast mag je als onderzoeker alleen persoonsgegevens verwerken die essentieel en noodzakelijk zijn voor je onderzoek. Dit waarborg je door aan beide volgende voorwaarden te voldoen:

- Verwerking van persoonsgegevens kan pas plaatsvinden als de grondslag gerechtvaardigd belang goed verantwoord kan worden. Persoonsgegevens mogen namelijk alleen worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden die noodzakelijk zijn voor de behartiging van het gerechtvaardigde belang van de verwerkingsverantwoordelijke of een derde. “Verwerkingen voor wetenschappelijk en historisch onderzoek, statistische doeleinden en archivering in het algemeen belang worden altijd verenigbaar geacht met het oorspronkelijke verzameldoel.”[10] Dit wil zeggen dat je binnen wetenschappelijk onderzoek alleen persoonsgegevens mag verzamelen en verwerken die strikt aansluiten op breed opgezette onderzoeksthema’s en gebieden die je vooraf aan je onderzoek hebt gedefinieerd en tijdens je onderzoek strikt blijft hanteren.
- Tevens verwerk je door middel van gegevensminimalisatie alleen de soort(en) persoonsgegevens die van essentieel belang zijn voor je onderzoek. Dit wil zeggen dat je alle persoonsgegevens die niet van essentieel belang zijn voor je onderzoek en argumentatie achterwege laat tijdens de verzamelfase en zeker tijdens het delen en opslaan van je onderzoeksproductie (artikelen, boeken, databestanden etc.) door middel van het omitteren, pseudonimiseren of anonimiseren van overbodige persoonsgegevens.[11]

2. Soorten persoonsgegevens

Wanneer voldaan is aan de bovenstaande grondslagen voor de verwerking van persoonsgegevens mag je als onderzoeker voor wetenschappelijke en statistische doeleinden persoonsgegevens verwerken. Persoonsgegevens zijn alle gegevens (= geschreven tekst, beeld

---

7 Eerste Kamer der Staten-Generaal, *Uitvoeringswet*, art. 24, onderdeel c.

8 Schermer, Hagenauw & Falot, *Handleiding*, 75-77.

9 Schermer, Hagenauw & Falot, *Handleiding*, 473.

10 Schermer, Hagenauw & Falot, *Handleiding*, 48.

11 Europese Commissie & Europees Parlement, ‘Regulation on the protection of the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)’, *Official journal of the European Union* (2016), L 119/29, art. 156; Schermer, Hagenauw, Falot, *Handleiding*, 48.

en/of geluid) die betrekking hebben op een geïdentificeerde (= informatie die direct over iemand gaat) of identificeerbare (= informatie die naar iemand te herleiden is) natuurlijke persoon (≠ organisatie (= rechtspersoon) of overledene).

Een eerste categorie behelst 'algemene' persoonsgegevens, waarbij je onder andere aan de volgende subcategorieën kan denken:

- Naam.
- Leeftijd en geboortedatum.
- Sekse.
- Nationaliteit.
- Adresgegevens.
- Contactgegevens (e-mailadres, telefoonnummer etc.).
- Locatiegegevens.
- Online identificatoren (bijvoorbeeld IP-adressen).[12]
- Uiterlijke kenmerken (lengte, postuur, haarkleur etc.).
- Sociale en economische kernmerken (beroep, inkomen, opleiding etc.).

Daarnaast is wetenschappelijk onderzoek uitgezonderd van het verbod op het verwerken van bijzondere persoonsgegevens wanneer voldaan is aan de bovengenoemde grondslagen. Onder bijzondere persoonsgegevens wordt het volgende verstaan:

- Persoonsgegevens over ras of etniciteit (huidskleur, traditionele klederdracht, opvattingen over multiculturalisme etc.).
- Persoonsgegevens waaruit politieke, filosofische of maatschappelijke opvattingen blijken (lidmaatschap politieke partij, politieke meningsuiting, aanstelling bij een NGO, deelname in demonstraties etc.).
- Persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken (kerkgang, religieuze klederdracht, levensbeschouwelijke meningsuitingen etc.).
- Persoonsgegevens waaruit een relatie met een vakvereniging blijkt (contributiegegevens lidmaatschap vakvereniging, deelname vakbondsdemonstraties etc.).
- Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid (seksueel getinte klederdracht, bedpartners, seksueel getinte meningsuitingen etc.).
- Gegevens over gezondheid (ziektes, handicaps, uithoudingsvermogen etc.).
- Genetische gegevens (DNA etc.).
- Biometrische gegevens met het oog op de unieke identificatie van een persoon (vingerafdrukken, armlengte, oogkleur etc.).[13]
- Strafrechtelijke gegevens (strafblad, verkeersboetes, duur hechtenis etc.).

---

[12] Schermer, Hagenauw & Falot, *Handleiding*, 24-25.

[13] Europese Unie, *Algemene*, art. 9 lid 1, www.privacy-regulation.eu/nl/artikel-9-verwerking-van-bijzondere-categorieen-van-persoonsgegevens-EU-AVG.htm.

Hogeschool van Amsterdam

Deel 2. Handreiking gebruik onderzoeksdata

Voor de verwerking van onderzoeksdata moet rekening worden gehouden met een aantal zaken. In dit deel van het dataprotocol vind je nadere informatie en regels over het beheren van onderzoeksdata, zoals verantwoordelijkheden, het opstellen van een Data Management Plan, versiebeheer en het maken van *back-ups*, het beveiligen van onderzoeksdata, de veilige omgang met privégevoelige persoonsgegevens, het verantwoordelijk publiceren van onderzoeksdata, het correct archiveren van onderzoeksdata, en richtlijnen omtrent intellectueel eigendom. Hierbij is uitgegaan van de algemeen geldende gedragscode praktijkgericht onderzoek voor het HBO.

Verantwoordelijkheid

Wie is verantwoordelijk voor de verantwoorde omgang met onderzoeksgegevens?

1. De primaire verantwoordelijkheid over de data ligt bij degenen die de data creëren en betrokken zijn bij de (dagelijkse) omgang met data: onderzoekers, studenten/promovendi en hun begeleiders.
2. Het is de gezamenlijke verantwoordelijkheid van studenten/promovendi en hun begeleiders om het beheer en gebruik van data goed te regelen en te documenteren. Begeleiders van studenten en promovendi hebben de verantwoordelijkheid om studenten en promovendi op de hoogte te stellen van geldende gedragscodes, richtlijnen en afspraken die binnen het onderzoeksproject zijn gemaakt over *datamanagement* (bijvoorbeeld in een DMP).
3. Studenten dienen zich aan deze richtlijnen en afspraken te houden bij het uitvoeren van het onderzoek.
4. De coördinerende onderzoekers van elk onderzoek schrijven het DMP en voeren het protocol uit. De lector bewaakt dit proces en stelt archiveringstermijnen vast.
5. De *principal investigator* (lector) is verantwoordelijk voor de correcte procedures voor *datamanagement*-protocol voor elk onderzoek binnen de kenniskring van zijn of haar lectoraat. De lector is daarmee verantwoordelijk voor een systematische en verantwoorde omgang met onderzoeksdata binnen zijn/haar lectoraat. Hij/zij is verantwoordelijk voor gemaakte afspraken met onderzoekers, studenten en externe partijen, voor geactualiseerde DMPs per project en voor een ethisch juiste omgang met (gegevens van) deelnemers/proefpersonen.
6. Ook als een andere partij penvoerder is of het een uitvoerende opdracht betreft, is de lector er verantwoordelijk voor dat het databeheer zorgvuldig gebeurt.
7. De decaan is bekend met elk onderzoeksproject en is eindverantwoordelijk. De decaan is eindverantwoordelijk voor toezicht op de correcte naleving van het dataprotocol.
8. Als de HvA penvoerder of opdrachtgever is, is de HvA formeel eindverantwoordelijke voor alle zaken die met dat onderzoek te maken hebben.

9. Een lector maakt onderzoekers, studenten en medewerkers in zijn/haar kenniskring of lectoraat attent op bovenstaande gedragscodes.
10. Bij het Kenniscentrum FDMCI is een datasteward werkzaam. Deze functionaris is expert op het gebied van *research datamanagement* en kan onderzoekers op dit gebied adviseren. De functionaris heeft een signalerende rol naar hoofd bedrijfsvoering onderzoek of de decaan.

Data Management Plan (DMP)

Wat is een DMP? Waarom moet je vooraf aan een onderzoeksproject een DMP invullen? Hoe geef je een DMP vorm?

Wanneer onderzoekers aan een onderzoek beginnen, worden zij per fase geacht aan te geven hoe met de data moet worden omgegaan, en welke (ICT-)voorzieningen nodig zijn om data te beheren. Een Data Management Plan kan hier gestalte aan geven. Het wordt gemaakt wanneer de subsidiegever hierom vraagt. Een DMP is een digitaal document waarin de onderzoeker aangeeft welke data hij/zij tijdens een onderzoeksproject gaat verzamelen; hoe de onderzoeker de data tijdens het project bewerkt en toegankelijk maakt; en wat er na afloop van het project met de data gebeurt. Voor het opstellen van een DMP binnen het Kenniscentrum FDMCI is een sjabloon beschikbaar (zie hiervoor de AZ-lijst van het kenniscentrum). Een DMP maakt het RDM-proces concreet en uitvoerbaar, doordat de onderzoeker voorbereid is op het beschrijven, opslaan, delen en publiceren van data. Wanneer een subsidiegever niet om een DMP vraagt, wordt er een DMP gemaakt wanneer uit het intakegesprek van het project of uit een lichte RDM-toets blijkt dat dit nodig is.

Inhoud DMP
In het DMP komen aan de orde:

1. Context
   Projectgegevens
2. Datacollectie
   Eigenschappen van de datacollectie; eigenaars van copyright en intellectueel eigendom
3. Datamanagement, documentatie en beheer
   Over de opslaglocatie; wijze van documentatie en versiebeheer; gebruik van metadata naar bv. Dublin Core metadata-standaard; eigenschappen van niet-digitale data
4. Dataveiligheid
   Risicoanalyse; licenties
5. Data-archivering en behouden
   Bewaartermijn; metadata; en verantwoordelijkheid na einde-project
6. Data publicatie en toegang
   Publiceren/delen van data; licentie eigenschappen
7. Rollen, verantwoordelijkheden en bron

Controle en evaluatie van DMP

Beheer DMP
Gedurende de looptijd van het onderzoeksproject moet regelmatig gecontroleerd worden of het DMP nog actueel is, dan wel moet worden bijgesteld. De onderzoeker is verantwoordelijk voor het opstellen en controleren van het DMP; de lector is verantwoordelijk voor het toezicht op de uitvoering door onderzoekers binnen het lectoraat. De datasteward kan advies uitbrengen op deze taken.

Alle datamanagementplannen worden door de datasteward opgeslagen bij de projectendesk van het kenniscentrum, gekoppeld aan de betreffende onderzoeksprojecten, zodat vindbaarheid gegarandeerd is. De datasteward archiveert de DMP's van alle lectoraten bij het kenniscentrum; de lectoren kunnen voor hun eigen lectoraat een archief bijhouden.

Eigenaar van de folder bij het Kenniscentrum is de datasteward, deze bewaakt de kwaliteit van het DMP en een adequaat gebruik van de folders. Lectoren en betrokken onderzoekers, programmamanagers hebben toegang tot de DMP's van het eigen lectoraat; en de datasteward heeft toegang tot alle datamanagementplannen.

Back-ups en versiebeheer

Bij gebruik van andere opslagplekken buiten SURFdrive om worden onderzoekers geacht om zelf verantwoordelijkheid te dragen voor het maken van reservekopieën van hun data. Op deze manier voorkom je dat je je onderzoeksdata niet meer kan inzien wegens verlies of het sneuvelen van een opslagplek.

Bij het creëren van reservekopieën en versiebeheer moeten onderzoekers de volgende punten overwegen:

1. Aantal back-ups: hoeveel opslagplekken ga je gebruiken om reservekopieën te maken? Maak gebruik van minstens één *back up*-mogelijkheid, zodat je je onderzoeksdata ook op een andere locatie kan beheren, verwerken en opslaan.
2. Soort: welke opslagplekken en reservekopieën ga je gebruiken voor het opslaan van data?
3. Frequentie: hoe vaak worden de bestanden bijgewerkt/aangepast?
4. Identificatie: hoe worden de inhoud, datum aanmaak/aanpassing van bestanden beschreven?
5. Controle: zijn de bestanden nog compleet en toegankelijk?
6. Creëren: worden reservekopieën handmatig aangemaakt of via software/ICT Services?

Beveiliging van data

De onderzoekers zijn verantwoordelijk voor de fysieke en virtuele beveiliging van de data.

Denk bij fysieke beveiliging aan de beveiliging van computerapparatuur, laptop en andere opslagmedia, bijvoorbeeld door het bewaren van deze producten in kluizen en het op slot doen van je kantoor wanneer je even weggaat en er verder niemand is in de ruimte.

Virtuele beveiliging is ten alle tijden verplicht door de volgende maatregelen te nemen (tenzij aangegeven als 'eventueel'):

- Het gebruik van een *firewall* op de computer of laptop.
- Het installeren van een antivirussoftware op de computer of laptop. Op dit moment wordt voor zowel Apple- en Windows-producten Avast aangeraden, de best gerecenseerde gratis antivirussoftware van Duitse makelij (het uitwisselen van virus- en systeemgegevens valt hierdoor onder EU-wetgeving).
- Het regelmatig *updaten* van *software* en besturingssystemen.
- Het versleutelen van wachtwoorden voor je netwerk, pc, bestand, etc.
- Het versleutelen van bestanden, (harde) schijf, *usb-sticks*, etc.
- (Eventueel) het installeren van *open-source privacy*-extensies voor webbrowser(s). Hiermee voorkom je voor een groot deel dat derden (o.a. Google en Facebook) je internetactiviteiten kunnen volgen en onderscheppen. Denk bijvoorbeeld aan *open-source* extensies zoals:
    - Adblock Plus: blokkeert advertenties en daarmee het uitwisselen van je browseractiviteiten met derden die achter deze advertenties zitten. Ook kunnen bijvoorbeeld *adware*, *malware*, *scam*-websites, en *mining* door derden geblokkeerd worden door optionele filterabonnementen toe te voegen. Link: adblockplus.org.
    - HTTPS Everywhere: versleutelt je browseractiviteiten tijdens het surfen op websites door bij elke verbinding met een website een https-verbinding te forceren. Link: www.eff.org/https-everywhere.
    - Ghostery: blokkeert *scripts* en *trackers* van derden die 'verscholen' zitten op websites, zoals advertenties en Facebook-iconen. Hierdoor kunnen derden je browseractiviteiten niet volgen. Link: www.ghostery.com.
    - Disconnect: blokkeert net als Ghostery *scripts* en *trackers* van derden op diverse manieren, maar heeft daarnaast ook een optie om *content* (video's, afbeeldingen etc.) van derden op websites optioneel te blokkeren. Ghostery en Disconnect overlappen elkaar aldus, maar niet volledig. Link: disconnect.me.

  Let op: zorg ervoor dat je tijdens het installeren van deze *privacy*-extensies altijd aangeeft dat de aanbieders zelf je browsergegevens niet mogen ontvangen en verwerken om bijvoorbeeld 'hun diensten te verbeteren'. Let er daarnaast op dat je deze extensies activeert voor privésessies.

Andere verplichte specifieke maatregelen zijn als volgt:

1. Onderzoekers en studenten dienen zich ten minste te houden aan de HvA ICT-gedragsregels en de door RDM-support voorgestelde maatregelen. Een overzicht hiervan zijn binnenkort *online* beschikbaar.
2. Onderzoekers nemen gepaste beveiligingsmaatregelen om dataverlies en datalekken te voorkomen. Gepast houdt in dit geval in: hoe gevoeliger/vertrouwelijker de (persoons)gegevens, hoe strenger de beveiligingsmaatregelen die genomen moeten worden.
3. De projectleider maakt regelmatig ten minste twee reservekopieën op een andere locatie (fysiek of digitaal) dan waar de originele gegevens staan.
4. Als *datasets* met persoonsgegevens of andere vertrouwelijke gegevens verstuurd moeten worden, dan gebeurt dit alleen versleuteld en via de HvA-mail, SURF Filesender (grote bestanden) of via een geforceerde https/sftp versleuteling in de webbrowser.
5. Er wordt zo min mogelijk gebruik gemaakt van *usb-sticks* en externe harde schijven. Indien deze toch gebruikt worden (bijv. voor *back-ups*) dan moeten deze dragers of de folders en bestanden die erop staan versleuteld worden. *Usb-sticks* en externe harde schijven worden in een gesloten kast bewaard.

De beveiliging van privégevoelige persoonsgegevens

Bij dataverzameling van personen moet hun *privacy* gegarandeerd worden. Het recht op informationele *privacy* komt er kort gezegd op neer dat ieder persoon zoveel mogelijk zelf invloed heeft op wie wat over hem of haar weet. Om de beveiliging van privégevoelige persoonsgegevens te waarborgen moet het volgende geregeld worden:

1. Onderzoekers implementeren de ‘Gedragscode praktijkgericht onderzoek voor het hbo’, daarbij specifiek lettend op de 5 regels van die gedragscode.
2. Onderzoekers houden zich aan de ‘Algemene verordening gegevensbescherming’ (AVG).
2. Er worden passende beveiligingsmaatregelen voor dataverzameling, -opslag en –archivering getroffen (zie hiervoor de bovenstaande paragraaf ‘Beveiliging van data’). In het algemeen geldt: hoe gevoeliger de informatie, hoe strenger de veiligheidseisen.
3. Bij het verzamelen en opslaan van persoonsgegevens dient gebruik gemaakt te worden van Nederlandse en Europese diensten. Clouddiensten als Dropbox zijn Amerikaanse bedrijven onder Amerikaanse wetgeving en voldoen daarmee niet zondermeer aan de Nederlandse en Europese wetgeving voor bescherming van persoonsgegevens.
4. Als persoonsgegevens door een andere partij worden verwerkt, zoals bij een *cloud*-leverancier (server, Qualtrics, SURFdrive, Research Manager) dan is een bewerkersovereenkomst wettelijk verplicht. Raadpleeg daarvoor een juridisch adviseur van IXA.
5. Verzamel niet meer persoonsgegevens dan noodzakelijk voor het onderzoek door dataminimalisatie toe te passen.

6. Wees terughoudend met het verzamelen van bijzondere persoonsgegevens. Onder bijzondere persoonsgegevens wordt onder andere verstaan gegevens over ras, gezondheid, godsdienst, politieke gezindheid en strafrechtelijke gegevens.
7. Direct identificeerbare en/of contactgegevens worden zo snel mogelijk verwijderd uit het onderzoeksbestand en opgeslagen in een apart sleutelbestand. Dit sleutelbestand is administratief gelinkt met het onderzoeksbestand en staat op een andere locatie (met andere toegangsvereisten).
8. Eenzelfde scheiding dient gemaakt te worden indien gegevens in een database worden opgeslagen.
9. Indien over langere tijd een systematische database met direct identificeerbare persoonsgegevens beheerd wordt, dient de lector of projectleider te verifiëren of de database geregistreerd dient te worden bij het College Bescherming Persoonsgegevens (via de functionaris gegevensbescherming van de HvA.
10. Een sleutelbestand dient vernietigd te worden wanneer het niet meer nodig is voor het doel van het onderzoeksproject. Zodoende blijft alleen een bestand over met anonieme of gepseudonimiseerde persoonsgegevens.
11. Het is in de meeste gevallen wettelijk verplicht deelnemers om toestemming te vragen (middels een *informed consent*, oftewel een instemmingsverklaring) voor het verwerken van persoonsgegevens en om hen te wijzen op hun rechten en plichten.
12. Bij het openstellen van data na afloop van een onderzoek zit je al snel met het niet kunnen waarborgen van de *privacy*. Geanonimiseerde of gepseudonimiseerde gegevens kunnen zonder problemen opengesteld worden hoewel enige voorzichtigheid geboden is bij hergebruik of het combineren van die gegevens met een ander databestand. Voor databestanden die persoonsgegevens bevatten moet nagedacht worden over openstellen. In veel gevallen zal dat laatste, het volledig openstellen van data, niet mogelijk zijn, maar gedeeltelijk openstellen wel (bijv. alleen de metadata).

Het verantwoordelijk publiceren van data

Data publiceren vergroot de impact van een onderzoek binnen en buiten het eigen vakgebied. Het kan leiden tot nieuwe (interdisciplinaire) samenwerking, vergemakkelijkt meta-analyses en reduceert het nodeloos dupliceren van onderzoek. Onderzoeksdata en *datasets* worden gepubliceerd met als doel:

- verificatie mogelijk maken van de conclusies die binnen het onderzoek worden getrokken door collega-onderzoekers;
- het hergebruik van data mogelijk maken door anderen voor onderzoek of onderwijs;
- voldoen aan de verplichtingen (van openbaarheid van data) volgens de richtlijnen van de subsidiegever, je instituut, je financier, of het tijdschrift waarin je publiceert.

Het wel of niet openbaar mogen maken van data is afhankelijk van:

- wetgeving;
- juridisch eigendom en auteursrecht;
- in hoeverre informatie reeds openbaar is gemaakt door de instanties of onderzochte personen zelf;
- het vooraf laten tekenen van *informed consents* (instemmingsverklaringen) door onderzochte personen of hun ouders/voogden;
- consortiumafspraken;
- het *open acces*-beleid van de HvA.

Wanneer onderzoeksdata en *datasets* gepubliceerd worden dan moet dit op een veilige en verantwoordelijke manier worden gedaan. Vooraf aan het onderzoek worden de details hierover in het DMP vastgelegd. De beheerder van het DMP, de verantwoordelijke onderzoeker, ziet ook toe op gebruik en hergebruik van openbaar gemaakte datasets, of van datasets die via een dataverzoek worden opgevraagd. De lector is eindverantwoordelijk.

Als onderzoeksdata en *datasets* aan de voorwaarden van zorgvuldigheid, eigenaarschap en openbaarheid voldoen dan kan data gepubliceerd worden via:

- Uva/HvA figshare, automatisch gekoppeld aan Pure.
- Pure, automatisch gekoppeld aan UvA/HvA figshare.
- Eigen website
- Website van een tijdschrift
- *Data journal* (een periodiek waarin beschrijvingen van *datasets* in een *data paper* worden gepubliceerd, de *papers* zijn *peer reviewed*; de dataset zelf wordt in een *repository* gedeponeerd)

HvA hecht eraan dat data uit afgerond onderzoek zo openbaar toegankelijk zijn als mogelijk en beschikbaar zijn voor hergebruik in nieuw onderzoek. Hiervoor kunnen onderzoekers zorgen door hun data na afronding van een onderzoeksproject onder te brengen in een data-archief dat de mogelijkheid biedt de data te publiceren en aan de data een persistent identifier (een unieke code die wordt gebruikt om naar de dataset te verwijzen/linken), zoals een DOI, toe te kennen (zie ook de paragraaf over archivering).

Datasets die gevoelige gegevens bevatten –persoonsgegevens, bedrijfsinformatie, informatie die bij openbaarheid schade kan veroorzaken –zullen niet open beschikbaar gesteld kunnen worden. Deze data moeten echter wel bruikbaar zijn voor nieuw onderzoek. Bij veel data-archieven is het mogelijk om van deze data een beschrijving te publiceren en de data zelf alleen op aanvraag ter beschikking te stellen.

Archiveren en openstellen van data

Tijdens het onderzoek is veel geïnvesteerd in het verkrijgen van onderzoeksdata. Na het onderzoeksproject kunnen de onderzoeksdata voor de toekomst bruikbaar blijven, voor het onderzoek zelf, maar ook voor anderen. Onderzoeksdata dienen dus goed te worden gearchiveerd in een data-archief. Voorwaarde voor correcte archivering is dat de data niet persoonsafhankelijk zijn en daardoor verdwijnen als bijvoorbeeld de onderzoeker uit dienst treedt.

De doelen van het opslaan van data in een data-archief zijn:

1. data duurzaam opslaan
2. data vindbaar publiceren

Gepubliceerde datasets moeten een 'persistent identifier' (bijv. DOI) krijgen. Bij de volgende repository's bestaat de mogelijkheid om zo'n 'persistent identifier' toe te kennen:

a. Een internationale data repository
b. Een nationale data repository zoals 4TU.ResearchData of DANS EASY
c. Uva/HvA figshare (uvaauas.figshare.com), automatisch gekoppeld aan Pure.

Het kenniscentrum stimuleert het delen van data met de wetenschappelijke gemeenschap (openstellen) op basis van het principe dat data zo 'open mogelijk' moeten worden gedeeld, daarbij lettend op ethische en vertrouwelijke beperkingen. In volgorde van openheid:

a. Onderzoeksdata en metadata zijn bij het deponeren meteen open.
b. Metadata zijn bij het deponeren meteen open; onderzoeksdata worden open na een embargoperiode.
c. Metadata zijn bij het deponeren meteen open; onderzoeksdata zijn alleen op aanvraag beschikbaar.
d. Zowel metadata als onderzoeksdata zijn niet open en alleen op aanvraag beschikbaar. Data worden bij voorkeur met een geschikte licentie gepubliceerd. Welke licentie en wat geschikt is, dient met de datasteward en RDM-support bepaald te worden.

In het CvB document Richtlijnen voor Research Data Management is de bewaartermijn van 10 jaar uit de Gedragscode praktijkgericht onderzoek voor het hbo overgenomen. De lector bewaakt de bewaartermijn. Onderzoekers die niet meer aan het onderzoeksinstituut of kenniscentrum verbonden zijn worden niet geïnformeerd over verlenging van de bewaartermijn van door hen verzamelde data.

Vernietiging van data vindt plaats als:
1. De data vallen niet onder één van de twee bovengenoemde redenen om de data te bewaren en de kosten voor lange termijnopslag zijn (te) hoog.
2. Vernietiging van de data verplicht is, bijvoorbeeld in het geval van persoonsgegevens.

Vernietiging geschiedt als volgt:

- Bij harde schijf en usb-sticks: formatteren en overschrijven met behulp van software. De voorkeur gaat uit naar het programma MiniTool (www.minitool.com).
- Bij Cd's en Dvd's: fysiek vernietigen.
- Bij papieren data: digitaliseren en de papieren versies vernietigen.

In de centrale RDM-richtlijnen worden promovendi apart genoemd (richtlijn 17): zij dienen de bij hun proefschrift behorende data te deponeren in een vakspecifiek, nationaal of institutioneel data-archief.

Op de uitvoering van het dataprotocol door de promovendus wordt toegezien door de promotor en de lector van het programma waarbinnen het promotieonderzoek plaatsvindt. Daarbij worden de keuzes in de uitvoering van het protocol (zoals bewaartermijnen) uitgevoerd conform de universiteitnormen waar de promotie plaatsvindt en volgens de normen van de uitvoering van het protocol van het kenniscentrum van de faculteit DMCI. Dit kan betekenen dat het protocol tweemaal wordt uitgevoerd, volgens verschillende normen.

Intellectueel eigendom

Van wie zijn de data? Wie is de producent van de databank[14] *? Mogelijkheden: van de onderzoeker, de student, de faculteit, een externe partij, de financier, de school, de deelnemer, etc.*

1. Uitgangspunt voor afspraken rondom intellectueel eigendom is de HvA Regeling Intellectueel Eigendom. Tenzij elders schriftelijk is vastgelegd (bijvoorbeeld in een overeenkomst) hoe met intellectueel eigendom om te gaan, gelden de bepalingen in deze regeling. De regeling houdt kort gezegd in:
    a. De HvA is eigenaar van tijdens een project verzamelde data; niet de onderzoeker(s) zelf.
    b. Bij studenten ligt het net iets complexer en hangt het af van of het primair onderwijs of onderzoek betreft. Raadpleeg hiervoor de regeling.
    c. Data zijn niet van proefpersonen maar ze hebben wel zeggenschap over gebruik en beschikbaarstelling ervan. Zij moeten in veel gevallen daarvoor toestemming geven middels een *informed consent*.
2. NWO (en dus ook SIA/RAAK) en ZonMw beschouwen zichzelf ook als producent van de databanken die voortkomen uit onderzoeken waarvoor een overeenkomst met hen is

[14] 'Producent van de databank' is een juridische term zoals wordt gebruikt in de Databankenwet. In die wet gaat het verder over 'originele creatie' en 'substantiële investering'.

aangegaan. Zij zijn daarmee mede-eigenaar van de data (zie desbetreffende subsidiebepalingen).

3. Bij samenwerking in een consortium of met externe partijen moeten duidelijke afspraken worden gemaakt over o.a. intellectueel eigendom en deze afspraken moeten worden vastgelegd in een consortiumovereenkomst. Onderzoekers dienen voor de start van het project contact op te nemen met een juridisch adviseur van IXA. De lector ziet erop toe dat het voor elke partij duidelijk is hoe de vork in de steel zit alvorens wordt gestart met de uitvoering van het project.
4. Ook wanneer een overeenkomst van een andere partij getekend dient te worden is het raadzaam contact op te nemen met een juridisch adviseur van IXA.