Landelijk Coördinatiepunt Research Data Management

Risicomanagement voor onderzoeksdata over mensen

EEN GENERIEKE MATRIX ALS HULPMIDDEL VOOR DATASTEWARDS EN ONDERZOEKS-ONDERSTEUNERS VOOR HET BEOORDELEN VAN PRIVACYRISICO'S MET ONDERZOEKSDATA EN HET VASTSTELLEN VAN DE JUISTE METHODES VOOR RISICOMANAGEMENT

'Hoe waarschijnlijk is het dat her-identificatie van een persoon aan de hand van de onderzoeksdata mogelijk is?'

'Wat zijn geschikte maatregelen om de data en de mensen achter de data te beschermen?'

Wat?

Deze matrix is generiek. Het is een hulpmiddel voor datastewards en onderzoeksondersteuners om onderzoekers te helpen de juiste maatregelen te nemen voor veilig gebruik én bescherming van data over mensen in wetenschappelijk onderzoek. Het is een template dat je kunt aanpassen aan de context van je eigen instelling, faculteit en/of afdeling door rekening te houden met het bij jou geldende beleid, de richtlijnen, de infrastructuur en de technische oplossingen. Zo kun je op een effectievere manier de juiste technische en organisatorische maatregelen nemen om de data te beschermen, gebaseerd op de context van het onderzoek en op de aan de data verbonden risico's.

Waarom?

Data over mensen die worden gebruikt in wetenschappelijk onderzoek zijn zelden anoniem. Het is belangrijk dat de onderzoekers zich hiervan bewust zijn in een vroeg stadium van hun datamanagementplanning. Wanneer blijkt dat de data niet anoniem zijn, is de AVG namelijk van toepassing. Dit betekent onder meer dat de correcte technische en organisatorische maatregelen genomen moeten worden om deze data te beschermen.

Hoe?

De matrix is gebaseerd op het *Five Safes Framework*.[1] Dit framework bestaat uit vijf dimensies (projecten, mensen, data, instellingen en output) op basis waarvan passende maatregelen kunnen worden genomen voor gegevensbescherming. Over het algemeen zouden dergelijke maatregelen alle vijf dimensies moeten afdekken. Als bepaalde maatregelen in de ene dimensie niet mogelijk zijn vanwege de specifieke onderzoeksvraag, kunnen in een andere dimensie van het *Five Safes Framework* 'zwaardere' maatregelen genomen worden.

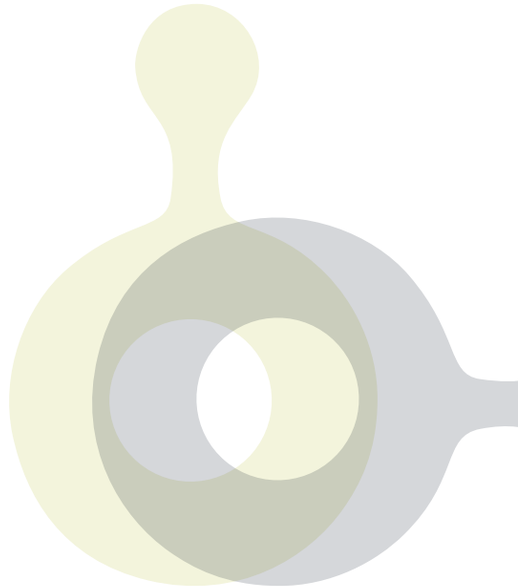
Eén maatregel ter bescherming van onderzoeksdata is pseudonimisering. Het niveau van de-identificatie kan bij gepseudonimiseerde data verschillen, maar bedenk altijd: zelfs als data gepseudonimiseerd zijn, zijn ze nog steeds **niet** anoniem.

Onderstaande matrix biedt een richtlijn voor maatregelen om data te beschermen op verschillende de-identificatieniveau 's van gepseudonimiseerde data, waarbij met alle dimensies van het *Five Safes Framework* rekening wordt gehouden.

Samengevat: deze matrix helpt je in je rol van onderzoekssupporter om
disciplinespecifiek advies te geven voor passende maatregelen in lijn met
de eisen van de AVG en in overeenstemming met de praktische aanpak
van andere onderzoeksinstellingen in Nederland.

De matrix biedt de volgende informatie:

I. 5 risiconiveaus om te bepalen hoe waarschijnlijk of hoe makkelijk een individu kan worden geïdentificeerd op basis van de data
II. Een generiek voorbeeld voor elk van deze niveau's
III. Een veld dat ingevuld kan worden met disciplinespecifieke voorbeelden
IV. 5 dimensies van het *Five Safes Framework* om te overwegen bij ieder risiconiveau.



Tenslotte

Twijfel je, of heb je vragen over anonimisering, pseudonimisering of beschermingsmaatregelen voor onderzoeksdata? Neem contact op met de privacyspecialist van je eigen instelling.

LCRDM taakgroep Anonimisering
(Versie: december 2019)

1] Meer informatie over
The Five Saves Matrix (Engels):
– https://en.wikipedia.org/wiki/Five_safes;
– https://www2.uwe.ac.uk/faculties/BBS/Documents/1601.pdf
– http://blog.ukdataservice.ac.uk/access-to-sensitive-data-for-research-the-5-safes/
– http://archive.stats.govt.nz/browse_for_stats/snapshots-of-nz/integrated-data-infrastructure/keep-data-safe.aspx

De volgende richtlijnen worden aanbevolen als kader voor de gegevensbeschermingsmaatregelen van elke kennisinstelling.
Voeg indien van toepassing extra informatie toe bij de verschillende onderdelen

ONDERDEEL I: Wat zijn de risiconiveaus voor her-identificatie van onderzoeksgegevens over mensen?

Identificatierisiconiveau	**PS0** Niet gepseudonimiseerd	**PS1** Gepseudonimiseerd op niveau 1	**PS2** Gepseudonimiseerd op niveau 2	**PS3** Gepseudonimiseerd op niveau 3	**'ANON'** Geanonimiseerd
Hoe hoog is het risico van her-identificatie?					
Definitie voor elk risiconiveau	*Direct identificerende* persoonlijke gegevens*	*Directe identificatiegegevens* zijn niet aanwezig maar:* *1. deelnemers worden geïdentificeerd via pseudoniem/ID nummer met een koppeling naar een koppelingstabel of sleutelbestand** dat de direct identificerende informatie bevat* ***EN*** *2. de pseudoniem of ID nummer is van belang of niet willekeurig, bijv. geboortedatum + postcode* ***EN/OF*** *3. de verzamelde gegevens kunnen gemakkelijk worden gebruikt om iemand te her-identificeren*	*Directe identificatiegegevens* zijn niet aanwezig maar:* *1. deelnemers worden geïdentificeerd via een betekenisloos pseudoniem/willekeurig ID nummer met een koppeling naar een koppelingstabel of sleutelbestand** dat de direct identificerende informatie bevat* ***EN/OF*** *2. uit de verzamelde gegevens kan een uniek profiel voor een persoon worden gegenereerd* ***EN/OF*** *3. met enige redelijke tijd en moeite is het*	*Directe identificatiegegevens* zijn niet aanwezig maar:* *1. deelnemers worden geïdentificeerd via een betekenisloos pseudoniem/willekeurig ID nummer met een koppeling naar een koppelingstabel of sleutelbestand** dat de direct identificerende informatie bevat* ***EN*** *2. uit de verzamelde gegevens is het niet mogelijk een uniek profiel te genereren voor een persoon* ***EN*** *3. het zou niet mogelijk zijn om een persoon te her-identificeren op*	*Gegevens anoniem verzameld:* *1. Geen directe of indirecte identificatiegegevens* aanwezig.* ***EN*** *2. Er is geen koppelingstabel/sleutelbestand aanwezig** (d.w.z. er is geen manier om de anonieme gegevens aan een andere dataset te koppelen)* ***EN*** *3. Er worden onvoldoende gegevens verzameld om een profiel te genereren dat uniek is voor een persoon* ***EN*** *4. Het is niet mogelijk om deelnemers te her-identificeren op*

* Direct identificerende/directe identificatiegegevens: gegevens kunnen direct en gemakkelijk aan een persoon worden toegewezen via kenmerken en variabelen die uniek zijn voor die persoon, zoals naam, adres, e-mail, BSN etc. Houd er rekening mee dat direct identificerende variabelen afhankelijk kunnen zijn van de context of de persoon in kwestie (bijvoorbeeld Jan Janssen versus Mark Rutte). Het is dus mogelijk dat u de context moet laten meewegen in de beslissing of een variabele direct identificeert.
→Indirecte identificerende/indirecte identificatiegegevens: gegevens die moeten worden gecombineerd met andere informatie om een persoon te identificeren, zoals een willekeurige ID code die verwijst naar direct identificerende informatie of door middel van een combinatie van variabelen die een unieke persoon onderscheidt (bijvoorbeeld een man in een borstkankerregister die kan worden geïdentificeerd door een combinatie van geslacht en borstkankerstatus).

** Koppelingstabel/sleutelbestand: een dataset met direct identificerende informatie die via een willekeurige ID code is gekoppeld aan onderzoeksgegevens.

Er kunnen identificatiegegevens in de dataset voorkomen waarmee personen via een ander bestand kunnen worden geïdentificeerd. Op deze manier maakt u onbedoeld een sleutelbestand. Als de dataset bijvoorbeeld technische sleutels (record ID's) uit een bronbestand bevat of als de dataset cijfers/ID's voor laboratoriummonsters/metingen of document ID's of bestandsnamen bevat.

mogelijk om een persoon te her-identificeren op basis van kenmerken in de gegevens

NB: Dit niveau is zelfs van toepassing als er geen willekeurige ID nummers met een koppeling naar een koppelingstabel/sleutelbestand worden gebruikt, maar het nog steeds mogelijk is om unieke profielen van individuen te genereren op basis van de verzamelde gegevens en/of het mogelijk zou zijn om een individu te her-identificeren op basis van de kenmerken in de verzamelde gegevens

basis van kenmerken in de gegevens

NB: Op dit niveau van pseudonimisering zijn de gegevens bijna anoniem, maar is de AVG nog steeds van toepassing. Er kunnen situaties zijn waarin de gegevens op een vergelijkbare manier kunnen worden behandeld als op het 'ANON' niveau zolang de koppelingstabellen en sleutelbestanden extreem veilig worden bewaard, en ALLEEN na instemming van privacy/beveiligingsspecialist binnen de eigen instelling.

basis van de kenmerken in de gegevens

De volgende richtlijnen worden aanbevolen als kader voor de gegevensbeschermingsmaatregelen van elke kennisinstelling.
Voeg indien van toepassing extra informatie toe bij de verschillende onderdelen

ONDERDEEL II: Generiek voorbeeld van onderzoeksgegevens op elk identificatierisiconiveau

PS0 Niet gepseudonimiseerd	**PS1** Gepseudonimiseerd op niveau 1	**PS2** Gepseudonimiseerd op niveau 2	**PS3** Gepseudonimiseerd op niveau 3	**'ANON'** Geanonimiseerd
NAAM: Rutger Hauer PATIËNTNUMMER: 90210 E-MAIL: blade.runner@batman.nl POSTCODE: 8911 AA WOONPLAATS: Leeuwarden GEBOORTEDATUM: 27-4-1967 SALARIS: 7,861 BEROEP: rechter AUTO: DeLorean KENTEKEN: SN-09-HN	PATIËNTNUMMER: 90210 POSTCODE: 8911 WOONPLAATS: Leeuwarden GEBOORTEDATUM: 27-4-1967 SALARIS: 7,861 BEROEP: rechter AUTO: DeLorean KENTEKEN: SN-09-HN	DEELNEMERSNUMMER: 47110009 REGIO: Friesland GEBOORTEJAAR: 1967 SALARIS: 7,500-10,000 BEROEP: jurist AUTO: DeLorean	DEELNEMERSNUMMER: 47110009 LAND: Nederland LEEFTIJD: 51-60 SALARIS: 5,000-15,000 BEROEP: jurist AUTO: Sportwagen	LAND: Nederland LEEFTIJD: 51-60 SALARIS: 5,000-15,000 BEROEP: jurist AUTO: Sportwagen

ONDERDEEL III:
Discipline specifieke voorbeelden van onderzoeksgegevens in te vullen door de gebruikers van de matrix

Gebruikers kunnen hier aanvullende discipline specifieke voorbeelden toevoegen	*Gebruikers kunnen hier aanvullende discipline specifieke voorbeelden toevoegen*	*Gebruikers kunnen hier aanvullende discipline specifieke voorbeelden toevoegen*	*Gebruikers kunnen hier aanvullende discipline specifieke voorbeelden toevoegen*	*Gebruikers kunnen hier aanvullende discipline specifieke voorbeelden toevoegen*

ONDERDEEL IV:

Vijf dimensies (projecten, mensen, data, instellingen, output) op basis waarvan passende maatregelen kunnen worden genomen voor gegevensbescherming

	PS0 Niet gepseudonimiseerd	**PS1** Gepseudonimiseerd op niveau 1	**PS2** Gepseudonimiseerd op niveau 2	**PS3** Gepseudonimiseerd op niveau 3	**'ANON'** Geanonimiseerd
Safe projects *Hoe kan ervoor worden gezorgd dat gebruik van de gegevens passend, wettelijk en ethisch is?*	Onderzoekers moeten: – Een DPIA, DMP en ethische aanvraag voltooien ***voorafgaand aan het verzamelen van gegevens*** – Controleren of expliciete toestemming vereist is en of het proces voor het verkrijgen van toestemming is gevolgd – Ervoor zorgen dat contracten tussen betrokken partijen, die door de AVG vereist zijn, aanwezig zijn ***voorafgaand aan het verzamelen van gegevens*** – Controleren of andere contracten vereist zijn, gelet op intellectueel eigendom en bedrijfsheimen	Onderzoekers moeten: – Een DPIA, DMP en ethische aanvraag voltooien ***voorafgaand aan het verzamelen van gegevens*** – Controleren of expliciete toestemming vereist is en of het proces voor het verkrijgen van toestemming is gevolgd – Ervoor zorgen dat contracten tussen betrokken partijen, die door de AVG vereist zijn, aanwezig zijn ***voorafgaand aan het verzamelen van gegevens*** – Controleren of andere contracten vereist zijn, gelet op intellectueel eigendom en bedrijfsheimen	Onderzoekers moeten: – Een DPIA, DMP en ethische aanvraag voltooien ***voorafgaand aan het verzamelen van gegevens*** – Controleren of expliciete toestemming vereist is en of het proces voor het verkrijgen van toestemming is gevolgd – Ervoor zorgen dat contracten tussen betrokken partijen, die door de AVG vereist zijn, aanwezig zijn ***voorafgaand aan het verzamelen van gegevens*** – Controleren of andere contracten vereist zijn, gelet op intellectueel eigendom en bedrijfsheimen	Onderzoekers moeten: – Een pre-DPIA (om te bepalen of een DPIA noodzakelijk is), DMP en ethische aanvraag voltooien ***voorafgaand aan het verzamelen van gegevens*** – Controleren of expliciete toestemming vereist is en of het proces voor het verkrijgen van toestemming is gevolgd – Ervoor zorgen dat contracten tussen betrokken partijen, die door de AVG vereist zijn, aanwezig zijn ***voorafgaand aan het verzamelen van gegevens*** – Controleren of andere contracten vereist zijn, gelet op intellectueel eigendom en bedrijfsheimen	Onderzoekers moeten: – Waar nodig een DMP en ethische aanvraag voltooien, ***voorafgaand aan het verzamelen van gegevens*** – Contact opnemen met experts om bevestigd te krijgen dat de gegevens echt anoniem zijn. Kies experts die geschikt zijn voor uw discipline en die het soort gegevens op de juiste manier kunnen beoordelen – Controleren of andere contracten vereist zijn, gelet op intellectueel eigendom en bedrijfsheimen

	PS0	PS1	PS2	PS3	‘ANON’
Safe people *Kunnen gebruikers worden vertrouwd om de gegevens op de juiste manier te gebruiken?*	– Wetenschappelijk personeel is contractueel verplicht om de gegevens vertrouwelijk te houden en om standaardprocedures te volgen voor het veilig verzamelen van gegevens – Wetenschappelijk personeel zou relevante privacy training moeten hebben gehad – Studenten/stagiaires moeten geheimhoudingsverklaringen tekenen en moeten institutionele regels volgen voor hoe en waar gegevens worden opgeslagen na het verzamelen ervan – Toegangsrechten moeten worden beperkt tot enkele personen die echt toegang nodig hebben tot de gegevens – Documentatie van wie toegang heeft en wat de toegangsrechten zijn, moet regelmatig worden onderhouden en bijgewerkt; tijdelijke toegang moet tijdig worden ingetrokken	– Wetenschappelijk personeel is contractueel verplicht om de gegevens vertrouwelijk te houden en om standaardprocedures te volgen voor het veilig verzamelen van gegevens – Wetenschappelijk personeel zou relevante privacy training moeten hebben gehad – Studenten/stagiaires moeten geheimhoudingsverklaringen tekenen en moeten institutionele regels volgen voor hoe en waar gegevens worden opgeslagen na het verzamelen ervan – Documentatie van wie toegang heeft en wat de toegangsrechten zijn, moet regelmatig worden onderhouden en bijgewerkt; tijdelijke toegang moet tijdig worden ingetrokken – Er moeten contracten worden gesloten met externe partijen die toegang hebben tot de gegevens (zoals ver-	– Wetenschappelijk personeel is contractueel verplicht om de gegevens vertrouwelijk te houden en om standaardprocedures te volgen voor het veilig verzamelen van gegevens – Wetenschappelijk personeel zou relevante privacy training moeten hebben gehad – Studenten/stagiaires moeten geheimhoudingsverklaringen tekenen en moeten institutionele regels volgen voor hoe en waar gegevens worden opgeslagen na het verzamelen ervan – Documentatie van wie toegang heeft en wat de toegangsrechten zijn, moet regelmatig worden onderhouden en bijgewerkt; tijdelijke toegang moet tijdig worden ingetrokken – Er moeten contracten worden gesloten met externe partijen die toegang hebben tot de gegevens (zoals ver-	– Wetenschappelijk personeel is contractueel verplicht om de gegevens vertrouwelijk te houden en om standaardprocedures te volgen voor het veilig verzamelen van gegevens – Wetenschappelijk personeel zou relevante privacy training moeten hebben gehad – Studenten/stagiaires moeten geheimhoudingsverklaringen tekenen en moeten institutionele regels volgen voor hoe en waar gegevens worden opgeslagen na het verzamelen ervan – Documentatie van wie toegang heeft en wat de toegangsrechten zijn, moet regelmatig worden onderhouden en bijgewerkt; tijdelijke toegang moet tijdig worden ingetrokken – Er moeten contracten worden gesloten met externe partijen die toegang hebben tot de gegevens (zoals ver-	– Toegangs-, lees- en schrijfrechten van alle interne leden van het onderzoeksteam moet worden gedocumenteerd en regelmatig worden bijgehouden – Onderzoekers moeten bepalen of er contracten moeten worden afgesloten met externe partners of met studenten, gelet op intellectueel eigendom en bedrijfsgeheimen. Indien bovenstaande niet van toepassing is, kan de data vrijelijk worden gedeeld en/of openlijk worden gepubliceerd – Als gegevens in de toekomst kunnen worden gebruikt om te her-identificeren als gevolg van verbeterde technologische methoden, is elke derde partij die de gegevens gebruikt vanaf dat moment zelfstandig verantwoordelijk voor het behandelen van de data als persoonsgegevens (het is dus niet de verantwoordelijkheid

	– Er moeten contracten worden gesloten met externe partijen	werkers of meewerkende partijen)	werkers of meewerkende partijen)	werkers of meewerkende partijen)	van de oorspronkelijke gegevensverzamelaar om secundaire gebruikers te informeren of te controleren
	PSO	**PS1**	**PS2**	**PS3**	**'ANON'**
Safe data *Hoe kan het risico van openbaarmaking binnen de gegevens zelf geminimaliseerd worden?*	Onderzoekers moeten: – Bepalen of onderzoeksdoelen kunnen worden bereikt zonder direct identificerende gegevens – Direct identificerende informatie moeten worden gescheiden van indirect identificerende informatie, bijvoorbeeld in een afzonderlijke koppelingstabel/sleutelbestand. – In sommige gevallen kan het passend zijn om de direct identificerende informatie te verhullen, bijvoorbeeld via hashing	Onderzoekers moeten: – Bepalen of onderzoeksdoelen kunnen worden bereikt zonder direct identificerende gegevens – Bepalen of onderzoeksdoelen kunnen worden bereikt zonder specifieke variabelen die zorgen voor her-identificatie, en deze vervangen door een alternatieve variabele te gebruiken die minder identificeert (bijvoorbeeld geboortejaar in plaats van geboortedatum) – Alert zijn op tekstvelden die identificerende informatie weergeven – Unieke datapunten/ extreme waarden generaliseren of verwijderen – Onnodige identificerende informatie verwijderen	Onderzoekers moeten: – Bepalen of onderzoeksdoelen kunnen worden bereikt zonder direct identificerende gegevens – Bepalen of onderzoeksdoelen kunnen worden bereikt zonder specifieke variabelen die zorgen voor her-identificatie, en deze vervangen door een alternatieve variabele te gebruiken die minder identificeert (bijvoorbeeld geboortejaar in plaats van geboortedatum) – Alert zijn op tekstvelden die identificerende informatie weergeven – Unieke datapunten/ extreme waarden generaliseren of verwijderen – Onnodige identificerende informatie verwijderen	Onderzoekers moeten: – Bepalen of onderzoeksdoelen kunnen worden bereikt zonder het gebruik van koppelingstabel/sleutelbestand	Onderzoekers moeten: – Contact opnemen met experts om bevestigd te krijgen dat de gegevens echt anoniem zijn. Kies experts die geschikt zijn voor uw discipline en die het soort gegevens op de juiste manier kunnen beoordelen

		– Gegevens opnieuw coderen naar een minder herkenbare vorm – Betekenisloze pseudoniemen/willekeurige ID nummers gebruiken waar mogelijk	– Gegevens opnieuw coderen naar een minder herkenbare vorm		
	PS0	**PS1**	**PS2**	**PS3**	**'ANON'**
Safe settings *Hoe wordt ongeautoriseerde toegang voorkomen?*	– Instellingen moeten op facultair niveau discipline specifieke standaardprocedures voor veilige gegevensverzameling en opslag ontwikkelen – Onderzoeksteam moet protocollen voor gegevensverzameling en opslag opstellen die door alle teamleden moeten worden gevolgd om privacy risico's tijdens de gegevensverzameling te minimaliseren – Gegevens moeten lokaal worden opgeslagen, alleen gedeeld met externe partijen onder strikte voorwaarden, met veilige methoden voor het delen van gegevens en met contracten tussen partijen	– Instellingen moeten op facultair niveau discipline specifieke standaardprocedures voor veilige gegevensverzameling en opslag ontwikkelen – Onderzoeksteam moet protocollen voor gegevensverzameling en opslag opstellen die door alle teamleden moeten worden gevolgd om privacy risico's tijdens de gegevensverzameling te minimaliseren – Gegevens moeten lokaal worden opgeslagen, alleen gedeeld met externe partijen onder strikte voorwaarden, met veilige methoden voor het delen van gegevens en met contracten tussen partijen	– Instellingen moeten op facultair niveau discipline specifieke standaardprocedures voor veilige gegevensverzameling en opslag ontwikkelen – Gegevens moeten lokaal worden opgeslagen, alleen gedeeld met externe partijen onder strikte voorwaarden, met veilige methoden voor het delen van gegevens en met contracten tussen partijen – Het beveiligingsniveau wat moet worden gehanteerd bij het verzamelen en opslaan van gegevens is afhankelijk van de gevoeligheid van de verzamelde gegevens en de kwetsbaarheid van de deelnemers.	– Gegevens moeten lokaal worden opgeslagen, maar mogen met externe partners worden gedeeld zolang er veilige methoden voor het delen van gegevens worden gebruikt en zolang er contracten tussen partijen zijn opgesteld – Het beveiligingsniveau wat moet worden gehanteerd bij het verzamelen en opslaan van gegevens is afhankelijk van de gevoeligheid van de verzamelde gegevens en de kwetsbaarheid van de deelnemers. Beveiligingsvereisten zijn over het algemeen lag voor dit soort gegevens. Toch moet een passend beveiligingsniveau worden afgestemd met	– Methoden voor gegevensverzameling en opslag moeten voldoen aan goede normen voor gegevensbeheer, maar privacy kwesties zijn niet van toepassing – Beveiligingskwesties kunnen van toepassing zijn als het gaat om bedrijfsgeheimen of intellectueel eigendomsrechten. Dit moet worden beoordeeld door een beveiligingsspecialist. – Gegevens kunnen openlijk worden gearchiveerd en gepubliceerd zonder datatoegangsbeperkingen zolang er geen bedrijfsgeheimen of intellectueel eigendomsrechten op de gegevens van toepassing zijn.

	– Het hoogste beveiligingsniveau moet worden gehanteerd bij het verzamelen en opslaan van gegevens. Bij kwetsbare groepen en bij gevoelige gegevens, kunnen aanvullende beveiligingsmaatregelen nodig zijn die verder gaan dan de standaardopties (bijvoorbeeld aanvullende versleuteling of het gebruik van computers die niet zijn aangesloten op het internet (air-gapped computers))	– Over het algemeen moet het hoogste beveiligingsniveau worden gehanteerd bij het verzamelen en opslaan van gegevens. Vooral als het gaat om gegevens van kwetsbare personen of wanneer de aard van de gegevens zeer gevoelig is en potentieel schadelijk is voor de personen. In sommige gevallen kan een gematigd beveiligingsniveau geschikt zijn, als de kwetsbaarheid van de deelnemers of het risico op schade laag is. Dit moet worden afgestemd met een privacy/beveiligingsspecialist. – Gegevens die in een opslag/repository van derden worden gepubliceerd moeten alleen op verzoek toegankelijk zijn	Beveiliging varieert van gemiddeld to het hoogste niveau. Een passend beveiligingsniveau moet worden afgestemd met behulp van een privacy/beveiligingsspecialist. – Gegevens die in een opslag/repository van derden worden gepubliceerd moeten alleen op verzoek toegankelijk zijn en gegevens mogen alleen worden gedeeld met externe partijen als beveiligde methoden worden gebruikt en als relevante contracten tussen partijen zijn opgesteld	behulp van een privacy/beveiligingsspecialist, gebaseerd op de aard van de gegevens – Gegevens mogen alleen openlijk worden gepubliceerd zonder datatoegangsbeperkingen als de koppelingstabel/sleutelbestand is verwijderd. Zo niet, dan mogen de gegevens alleen op verzoek toegankelijk zijn en mogen gegevens alleen worden gedeeld met externe partijen als beveiligde methoden worden gebruikt en als relevante contracten tussen partijen zijn opgesteld	– Voor archivering moet een vertrouwde en discipline specifieke opslag/repository worden gebruikt. – Gepubliceerde gegevens moeten een licentie hebben zodat andere gebruikers weten wat ze met de gegevens mogen doen
	PS0	**PS1**	**PS2**	**PS3**	**'ANON'**
Safe output *Bestaat er een risico op openbaarmaking in de statistische resultaten (bijv. tabellen, diagrammen)?*	– Doorloop output data op risico's op openbaarmaking – Bepaal of de resultaten van het onderzoek gevolgen kunnen hebben voor de samenleving of voor personen	– Doorloop output data op risico's op openbaarmaking – Bepaal of de resultaten van het onderzoek gevolgen kunnen hebben voor de samenleving of voor personen	– Doorloop output data op risico's op openbaarmaking – Bepaal of de resultaten van het onderzoek gevolgen kunnen hebben voor de samenleving of voor personen	– Doorloop output data op risico's op openbaarmaking – Bepaal of de resultaten van het onderzoek gevolgen kunnen hebben voor de samenleving of voor personen met	– Bepaal of de resultaten van het onderzoek gevolgen kunnen hebben voor de samenleving of voor personen met vergelijkbare kenmerken als de deelnemers aan het

met vergelijkbare kenmerken als de deelnemers aan het onderzoek. Bespreek ethische zorgen en gevolgen van onderzoeksresultaten met de ethische commissie – Secundaire gebruikers zijn zelf verantwoordelijk voor het doorlopen van output voor her-identificatie – Bij beoordeling van verzoeken om toegang te verlenen tot gegevens, moet rekening worden gehouden met de gevolgen voor de deelnemers aan het onderzoek	met vergelijkbare kenmerken als de deelnemers aan het onderzoek. Bespreek ethische zorgen en gevolgen van onderzoeksresultaten met de ethische commissie – Secundaire gebruikers zijn zelf verantwoordelijk voor het doorlopen van output voor her-identificatie – Bij beoordeling van verzoeken om toegang te verlenen tot gegevens, moet rekening worden gehouden met de gevolgen voor de deelnemers aan het onderzoek	met vergelijkbare kenmerken als de deelnemers aan het onderzoek. Bespreek ethische zorgen en gevolgen van onderzoeksresultaten met de ethische commissie – Secundaire gebruikers zijn zelf verantwoordelijk voor het doorlopen van output voor her-identificatie – Bij beoordeling van verzoeken om toegang te verlenen tot gegevens, moet rekening worden gehouden met de gevolgen voor de deelnemers aan het onderzoek	vergelijkbare kenmerken als de deelnemers aan het onderzoek. Bespreek ethische zorgen en gevolgen van onderzoeksresultaten met de ethische commissie – De koppelingstabel/sleutelbestand en andere ID variabelen moeten niet worden verstrekt aan secundaire gebruikers, om het risico van her-identificatie op basis van de output te voorkomen – Indien van toepassing, moet er bij de beoordeling van verzoeken om toegang te verlenen tot gegevens, rekening worden gehouden met de gevolgen voor de deelnemers aan het onderzoek – Voorafgaand aan de openlijke publicatie van gegevens moet rekening worden gehouden met mogelijke onvoorziene gevolgen die de anonieme/geanonimiseerde gegevens kunnen hebben op personen. Deze kwesties kunnen worden besproken met privacy/beveiligingsspecialisten.	onderzoek. Bespreek ethische zorgen en gevolgen van onderzoeksresultaten met de ethische commissie – Voorafgaand aan de openlijke publicatie van gegevens moet rekening worden gehouden met mogelijke onvoorziene gevolgen die de anonieme/geanonimiseerde gegevens kunnen hebben op personen. Deze kwesties kunnen worden besproken met privacy/beveiligingsspecialisten.

COLOFON

Risicomanagement voor onderzoeksdata over mensen. *Een generieke matrix als hulpmiddel voor datastewards en onderzoeksondersteuners voor het beoordelen van privacyrisico's met onderzoeksdata en het vaststellen van de juiste methodes voor risicomanagement*

PUBLICATIEDATUM | december 2019
DOI | 10.5281/Zenodo.3584333

LCRDM Taakgroep Anonimisering
Jessica Hrudey (Vrije Universiteit),
Jan Lucas van der Ploeg (Universitair Medisch Centrum Groningen - UMCG),
Joan Schrijvers (Wageningen University & Research),
Arnold Verhoeven (Universiteit Maastricht),
Henk van den Hoogen (Universiteit Maastricht/liaison LCRDM adviesgroep),
Marjolein Sijbers-Klaver (Universitair Medisch Centrum Utrecht – UMCU),
Santosh Ilamparuthi (TU Delft),
Toine Kuiper (TU Eindhoven),
Erik Tjong Kim Sang (eScience Center),
Niek van Ulzen (Hogeschool van Amsterdam),
Yvonne Drost (Rijksdienst Cultureel Erfgoed),
Ingeborg Verheul (LCRDM)

ONTWERP | Nina Noordzij, Collage, Grou

LCRDM wordt mogelijk gemaakt door