

Kennisbank – toelichting onderwerpen DPIA

Bij elk onderwerp in een DPIA wordt gekeken welke mitigerende maatregelen genomen kunnen worden om mogelijke risico's te kunnen verwijderen of minimaliseren.

1. Het soort persoonsgegevens dat wordt verzameld

Bij dit onderwerp worden de gegevens omschreven die binnen het onderzoek worden gebruikt en welke categorie persoonsgegevens dit zijn. De AVG maakt onderscheid tussen 'gewone' persoonsgegevens en 'bijzondere' persoonsgegevens. Bijzondere persoonsgegevens zijn gevoelige gegevens zoals iemands ras of etnische afkomst, politieke opvatting of religieuze of filosofische overtuiging. Deze zijn door de wetgever extra beschermd. Gegevens over de gezondheid zijn ook bijzondere persoonsgegevens.

2. Grondslagen voor verwerking

De grondslag is de reden op grond waarvan je (volgens de AVG) de gegevens mag verwerken. Vaak is dit de toestemming van de deelnemer, maar er zijn ook andere grondslagen zoals een algemeen of een gerechtvaardigd belang. Alle grondslagen voor standaard persoonsgegevens staan in artikel 6 van de AVG. In artikel 9 van de AVG worden de grondslagen benoemd voor het verwerken bijzondere persoonsgegevens, zoals gegevens over gezondheid (artikel 9 noemt deze 'grondslagen' uitzonderingen op het verbod om bijzondere persoonsgegevens te verwerken, maar in deze toelichting worden deze voor de leesbaarheid ook grondslagen genoemd). De belangrijkste gronden voor gezondheidsonderzoek worden in de onderstaande tabel genoemd.

Grondslagen 'standaard' persoonsgegevens Artikel 6 AVG	Grondslagen (uitzonderingsgronden) verwerking bijzondere persoonsgegevens Artikel 9 AVG
1-a Toestemming	2-a Toestemming
1-e Algemeen belang	2-j Wetenschappelijk onderzoek
1-f Gerechtvaardigd belang	

Voor veel medisch wetenschappelijk mensgebonden onderzoek (WMO en niet WMO-plichtig onderzoek) is toestemming de aangewezen grondslag. Bij WMO-plichtig onderzoek is toestemming altijd verplicht. Ook voor niet WMO-plichtig onderzoek waarbij bij deelnemers gegevens worden verzameld, wordt altijd toestemming gevraagd.

Voor niet WMO-plichtig onderzoek waarbij gegevens die in de zorg zijn verkregen worden hergebruikt voor wetenschappelijk onderzoek, is soms een uitzondering op het vragen van toestemming mogelijk. Wanneer toestemming redelijkerwijs niet mogelijk is, is de grondslag in artikel 6 het algemeen of een gerechtvaardigd belang. De grondslag in artikel 9 is dan in de meeste gevallen wetenschappelijk onderzoek. Om op deze grondslag een beroep te mogen doen moet aan een aantal voorwaarden wordt voldaan. Een aantal van deze voorwaarden heeft als doel de risico's die ontstaan omdat geen toestemming wordt gevraagd, te minimaliseren.

Deze voorwaarden staan beschreven in de Nederlandse uitvoeringswet van de AVG, de UAVG (art. 24), en de Wet op de Geneeskundige Behandelingsovereenkomst, de WGBO (art 7), en de gedragscode gezondheidsonderzoek (hoofdstuk 5). De gedragscode gezondheidsonderzoek stelt daarbij dat, als het vragen van een toestemming voor een specifiek onderzoek niet mogelijk is, eerst onderzocht moet

worden of een algemene toestemming kan worden gevraagd. Als dat ook niet mogelijk is, kan het vragen van toestemming achterwege gelaten worden.

In onderstaande tabel staan deze voorwaarden opgesomd:

Voorwaarden beroepen op grondslag 'wetenschappelijk onderzoek'
Het vragen van toestemming blijkt onmogelijk of zou onevenredige inspanning kosten <i>Voorbeelden waarbij het vragen van toestemming niet mogelijk is of onevenredige inspanning zou vergen (verdere toelichting specifiek voor het onderzoek is vereist):</i> ➤ <i>het gaat om dusdanig grote aantallen patiënten dat redelijkerwijs niet kan worden verwacht dat benodigde grote inspanningen worden gedaan om iedere patiënt te bereiken</i> ➤ <i>een groot deel van de patiënten is overleden</i> ➤ <i>het gaat om jaren geleden verzamelde persoonsgegevens van wie de adressen niet meer te achterhalen zijn</i> ➤ <i>bij het vragen van toestemming kan selectieve respons ontstaan</i> ➤ <i>het vragen van toestemming is te zeer belastend voor de betrokken proefpersoon</i> <i>* Zie de gedragscode gezondheidsonderzoek (paragraaf 5.4) voor meer informatie</i> <i>Welke reden kan niet worden aangedragen?</i> ➤ <i>toestemming vragen zorgt voor te hoge kosten (<u>tenzij de kosten onredelijk hoog worden</u>)</i> ➤ <i>toestemming vragen zal het onderzoek vertragen (<u>tenzij de vertraging onredelijk is</u>)</i>
Onderstaande factoren zijn niet van toepassing op het onderzoek (gedragscode hfst. 4.4) ➤ Onderzoek en toepassingen met een aanmerkelijk risico op individuele bevindingen ➤ Het gaat om onderzoek met gegevens die intrinsiek herleidbaar worden geacht, bijvoorbeeld bij 'whole genome sequencing', en waarbij deze gegevens breder worden gedeeld dan binnen de onderzoeksinstelling waar de sequencing plaatsvond ➤ Zuiver commercieel onderzoek waarbij resultaten uitsluitend aan een private, op winst gerichte partij beschikbaar komen; ➤ Het amplificeren van lichaamsmateriaal tot onsterfelijke (stam)cellen en cellijnen; ➤ Het amplificeren van lichaamsmateriaal tot geslachtscellen en embryoachtige structuren; ➤ Mens-dier-combinaties waarbij sprake is van een substantiële vermenging van genetisch materiaal van menselijke en dierlijke oorsprong (bijvoorbeeld cybriden en chimeraen). → Indien bovenstaande factoren wél van toepassing zijn, dient ALTIJD toestemming te worden gevraagd.
De verwerking is noodzakelijk voor het uitvoeren van wetenschappelijk onderzoek
De betrokkene heeft geen schriftelijk bezwaar gemaakt tegen het verzamelen van de gegevens én dit is gecontroleerd door de behandelaar.
De betrokkenen hebben toegang tot informatie over de verwerking van persoonsgegevens zonder dat er toestemming wordt gevraagd (bv. website-instelling, folders etc.).
Het onderzoek dient het algemeen belang (bevordering of bescherming volksgezondheid).
Het wetenschappelijk onderzoek kan niet worden uitgevoerd zonder de verzamelde gegevens. Hierbij is gegarandeerd dat de enkel de minimaal noodzakelijke gegevens worden verzameld. Dit betekent dat bv (indien mogelijk) enkel Geboortjaar i.p.v. datum, leeftijd range i.p.v. leeftijd, regio i.p.v. woonplaats wordt verzameld.
Speciale maatregelen zijn genomen om te verzekeren dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad (herleiding dient redelijkerwijs te worden voorkomen door minimaal pseudonimisering toe te passen)
De verzamelde gegevens worden niet gedeeld buiten de Europese Economische Ruimte (EER) zonder dat er een passend beschermingsniveau kan worden gegarandeerd (bespreek dit met een jurist). Indien wel gedeeld wordt zonder passend beschermingsniveau, is expliciete toestemming vereist.
Er wordt een notitie gemaakt van het gebruik van de persoonsgegevens in het medisch dossier van de betrokkene (indien aanwezig).

Een voorbeeld van een onderzoek waarop deze voorwaarden van toepassing zouden kunnen zijn, is een niet WMO-plichtig retrospectief onderzoek waarbij gegevens vanuit het EPD worden gebruikt.

De wijze waarop naleving van deze voorwaarden wordt getoetst, is aan de instelling of organisatie.

3. Verantwoordelijkheid voor de persoonsgegevens

De instelling die het onderzoeksprotocol heeft opgesteld is verantwoordelijk voor de verwerking van de verzamelde persoonsgegevens. Wie dit is wordt beschreven in de DPIA. Het is ook mogelijk dat meerdere instellingen samen verantwoordelijk zijn als ze gezamenlijk het protocol schrijven en/of uitvoeren. De gezamenlijke verwerkingsverantwoordelijken moeten de verdeling van taken en maatregelen die getroffen worden ter bescherming van de verwerking persoonsgegevens vastleggen in een passend contract.

4. Doel van het verwerken van persoonsgegevens

Hierbij wordt omschreven waarom het onderzoek wordt uitgevoerd. De omschrijving omvat alles wat met de gegevens zou worden gedaan. Het doel kan bijvoorbeeld wetenschappelijk onderzoek of het ontwikkelen van beleid zijn. In een DPIA kan een verkort of gestandaardiseerd doel worden opgenomen, waar nodig met extra verwijzing. Als je de gegevens wil gebruiken voor een ander doel dan waarvoor ze oorspronkelijk zijn verzameld dan moet je in de DPIA zorgvuldig beschrijven waarom dit doel verenigbaar is met het oorspronkelijke doel.

5. De noodzaak van de persoonsgegevens voor het onderzoek

Uit een DPIA moet naar voren komen, dat de persoonsgegevens die verwerkt worden, ook echt nodig zijn om de onderzoeksvraag te beantwoorden. Gegevens die niet nodig zijn om het doel te bereiken, zoals dat in de DPIA is omschreven, mogen ook niet verwerkt worden.

6. Betrokken partijen bij het verwerken van de persoonsgegevens

De rol van alle partijen die zijn betrokken bij het verwerken van de persoonsgegevens moet duidelijk worden in de DPIA. Alle rollen dienen te worden vastgelegd, evenals de wijze waarop gegevens worden gedeeld en de wijze van gegevensbescherming. Afspraken tussen onderlinge partijen worden vastgelegd in een passend contract.

Elke partij die bij de verwerking van persoonsgegevens betrokken is, is ofwel verwerkingsverantwoordelijke ofwel verwerker. De verwerkingsverantwoordelijke is onder punt 3 al beschreven. Een verwerker verwerkt persoonsgegevens niet voor zichzelf, maar in opdracht van een verwerkingsverantwoordelijke. Indien een dienstverlener bij het onderzoek is betrokken, zoals een leverancier van een applicatie of software, is deze dienstverlener vaak een verwerker.

Indien een verwerker betrokken is, zal een verwerkersovereenkomst met deze partij worden gesloten. Als de gegevens met een andere partij worden gedeeld die geen verwerker is, zowel tijdens als na afloop van het onderzoek, dient een data-uitwisselingsovereenkomst of data sharing agreement (DSA), te worden afgesloten tussen partijen. Als meerdere partijen verwerkingsverantwoordelijke zijn dient een onderlinge regeling te worden opgesteld.

Naast de risico's die voortkomen uit het daadwerkelijke delen van de persoonsgegevens en/of de gezamenlijke verantwoordelijkheid voor de gegevens, is het ook van belang dat de deelnemers goed worden geïnformeerd over de verschillende partijen die hun persoonsgegevens verwerken.

Een voorbeeld waarbij verschillende rollen van toepassing zijn, zijn de opzet en de uitvoering van de studie. Wie heeft bijvoorbeeld het onderzoekprotocol opgesteld? Dit kan één partij zijn, of meerdere. Bovendien kan er een dienstverlener betrokken zijn, zoals een leverancier van een applicatie of software. Ook kunnen gegevens worden gedeeld met een externe partij zoals bv. een laboratorium of ander ziekenhuis, om bepaalde gegevens te laten analyseren.

Een laatste voorbeeld heeft betrekking op het delen van persoonsgegevens na afloop van het onderzoek. Ook hier dienen duidelijke afspraken over te worden vastgelegd.

7. Updaten van de persoonsgegevens tijdens het onderzoek

Om te zorgen dat gedurende het onderzoek van de juiste gegevens wordt uitgegaan zal in de DPIA worden beschreven of de onderzoeker toegang heeft tot de actuele persoonsgegevens (bv. contactgegevens) van de deelnemers. Ook is van belang dat wordt nagegaan of deze up-to-date blijven gedurende het onderzoek. Zo kan een deelnemer bijvoorbeeld een nieuw adres krijgen door een verhuizing.

8. Bewaartermijn van de persoonsgegevens

In de DPIA wordt opgenomen hoe lang de gegevens zullen worden bewaard. Voor wetenschappelijk onderzoek met mensen (WMO-plichtig onderzoek) dat onder de CTR of MDR valt, zijn wettelijke termijnen vastgesteld. Voor overig WMO-plichtig onderzoek adviseert de CCMO een termijn van 15 jaar, mits onderbouwd in het protocol. Zie de [website van de CCMO](#).

Als het niet mogelijk is om een specifieke bewaartermijn vast te stellen worden de criteria opgenomen die worden gebruikt voor de invulling van die termijn. Daarbij kan ook worden opgenomen hoe wordt geborgd dat de bewaartermijn wordt nagekomen en/of periodiek wordt getoetst of bewaren nog steeds noodzakelijk is. Uw organisatie of instelling heeft hier mogelijk een beleid of proces voor opgesteld ter ondersteuning.

Bij het vaststellen van de bewaartermijn moet rekening worden gehouden met mogelijk hergebruik. Deze moet lang genoeg zijn om dit hergebruik te faciliteren. Wanneer de gegevens na afloop van een onderzoek worden gedeeld met externe partijen, dient te worden nagedacht over de termijn dat de gegevens beschikbaar worden gesteld (bijvoorbeeld 5 jaar na afloop van het onderzoek). Dit, zodat de initiële bewaartermijn waarover de deelnemers zijn geïnformeerd, niet wordt overschreden.

9. Opslag en beveiliging van de persoonsgegevens

Opslag en gebruik van de persoonsgegevens moet veilig gebeuren. De beveiligingsmaatregelen worden in de DPIA beschreven. Hierbij kan vaak worden aangesloten bij het informatiebeveiligingsbeleid van de organisatie die verwerkingsverantwoordelijke is voor de gegevens.

Van belang is te kijken of op basis van het soort persoonsgegevens (bv. gegevens over seksualiteit) of de kwetsbaarheid van de deelnemers (bv. wanneer voor die deelnemer het privacy risico bij een datalek groot is), specifieke of aanvullende maatregelen kunnen worden genomen.

Een aantal maatregelen kunnen door de onderzoeker zelf genomen worden, in aansluiting op het informatiebeveiligingsbeleid van de instelling. Dit gaat bijvoorbeeld over het pseudonimiseren van persoonsgegevens voor iedere verwerking, beheer van mappentoeegang o.b.v. het instellingsbeleid en

clean desk policy. De instelling bepaalt of deze apart aan de onderzoeker worden voorgelegd per onderzoek of wordt verwezen naar het instellingsbrede beleid.

Risico's kunnen bijvoorbeeld ontstaan wanneer een onderzoeker persoonsgegevens op een andere dan door de organisatie voorgeschreven locatie wil opslaan of verzenden. Een extra toetsing is op dit moment aangewezen om de veiligheid van de gegevens te garanderen.

10. Procedure bij een datalek

Vaak is er een beleid aanwezig bij de instelling of organisatie voor de melding van datalekken. Deze procedure dient duidelijk te zijn en vindbaar voor de onderzoekers.

11. Informeren van deelnemers over het verzamelen en gebruiken van de persoonsgegevens

In de DPIA wordt opgenomen hoe de deelnemers aan het onderzoek worden geïnformeerd over het verzamelen en gebruiken van persoonsgegevens en wie hiervoor verantwoordelijk is (zie hoofdstuk 3 van de gedragscode gezondheidsonderzoek). Indien er toestemming wordt gevraagd van de betrokkene wordt deze informatie opgenomen in het informed consentformulier. Is dit niet aanwezig, dan dient de deelnemer op andere wijze informatie te worden aangeboden (vaak instellingsbreed).

Wanneer de dataset na afloop van het onderzoek zal worden gedeeld met een derde partij, dient de deelnemer ook hierover geïnformeerd te worden en, indien mogelijk, toestemming voor te geven.

12. Uitoefenen van rechten uit de AVG, bijvoorbeeld op gegevenswissing, door de deelnemers

Deelnemers hebben op grond van de AVG een aantal rechten met betrekking tot de gegevens die over hen verzameld en gebruikt worden voor het onderzoek. De deelnemer heeft een recht op inzage, op rectificatie, op overdraagbaarheid, op wissing van de gegevens en op bezwaar tegen het verwerken van de gegevens (hoofdstuk 6 gedragscode). Soms zijn er beperkingen op het uitoefenen van deze rechten door deelnemers, bijvoorbeeld omdat de gegevens van een deelnemer niet zomaar terug te vinden zijn in de gegevensset of omdat de gegevens al gebruikt zijn voor een wetenschappelijke publicatie. In de DPIA wordt opgenomen hoe de deelnemers hun rechten kunnen uitoefenen, of hier beperkingen voor bestaan, en hoe deelnemers hierover worden geïnformeerd.

Dit zal veelal gebeuren middels een informed consent waarin contactgegevens voor de deelnemer worden opgenomen. In de informatie die openbaar wordt gemaakt voor bv. patiënten van een ziekenhuis (in geval van retrospectief onderzoek) zal ook naar voren moeten komen hoe deelnemers hierover worden geïnformeerd.