Juridische verantwoording bij de Blauwdruk voor AI in de zorg

Deze bijlage maakt onderdeel uit van de Blauwdruk voor AI in de zorg: van idee tot prototype

Colofon

Auteur : Colette Cuijpers – Lector Recht en Digitale Technologie, Juridische Hogeschool Avans - Fontys

Contactgegevens
Voor vragen of suggesties over over deze juridische verantwoording bij de Blauwdruk voor AI in de zorg :
c.cuijpers@fontys.nl

Versie : Versie 1.0 – november 2025

Met dank aan
We danken alle betrokken partners voor hun waardevolle bijdrage, inzichten en feedback tijdens de totstandkoming van deze juridische verantwoording bij de Blauwdruk voor AI in de zorg. Hun praktijkervaring en betrokkenheid waren van grote waarde.

Inhoudsopgave

1. Inleiding

Deze juridische verantwoording is opgesteld tijdens het project *VVT en de Kansen van AI* en is bedoeld als hulpmiddel voor alle betrokken en toekomstige organisaties die met de blauwdruk werken. Het document biedt een overzicht van de juridische aspecten die relevant zijn wanneer meerdere partijen samenwerken aan de ontwikkeling van AI-toepassingen in de zorg.

Voordat een samenwerking daadwerkelijk van start kan gaan, of dit nu is met zorgpartijen onderling of met zorgpartijen en kennisinstellingen en/of commerciële partijen samen, moet er een overeenkomst getekend worden op basis waarvan wordt samen gewerkt. In deze overeenkomst worden basisafspraken gemaakt over de samenwerking. Wanneer er sprake is van een project waarbij een kennisinstelling betrokken is, wordt over het algemeen gesproken van een consortium agreement, de term samenwerkingsovereenkomst dekt ook de lading (een overeenkomst waarbij twee of meer partijen afspraken maken over een samen te realiseren doel). Een goede consortium- of samenwerkingsovereenkomst vormt het startpunt van de daadwerkelijke uitvoering van een project. Een project ontstaat vanuit een idee, waarvoor een projectplan is opgesteld en financiering is verkregen (meestal via een subsidieaanvraag). Met de overeenkomst gaan meerdere partijen een gezamenlijk commitment aan om samen een concreet doel te bereiken. In paragraaf 2 wordt daarom eerst opgelijst wat er in een consortium-/samenwerkingsovereenkomst geregeld moet worden.

In projecten die de ontwikkeling van een AI-toepassing betreffen is altijd sprake van het verwerken van gegevens. Om dit op een verantwoorde wijze binnen een consortium plaats te laten vinden is het noodzakelijk om, naast de consortium-/samenwerkingsovereenkomst (paragraaf 2), nadere afspraken te maken over het data management. In paragraaf 3 wordt nader ingegaan op het Data Management Plan (DMP). Een Data Management Plan bevat de afspraken tussen partijen over hoe gegevens verwerkt en bewaard worden. Het DMP bevat ook een aparte paragraaf over de verwerking van persoonsgegevens. Aangezien de verwerking van persoonsgegevens extra waarborgen vereist, wordt hier in paragraaf 4 meer uitgebreid bij stilgestaan. Tot slot worden in paragraaf 5 nog een paar belangijke juridische aandachtspunten aangestipt. In paragraaf 6 is als bijlage een samenvatting opgenomen in de vorm van handzame vragenlijsten.

2. Consortium agreement – Samenwerkingsovereenkomst

Zodra de partijen die samen willen gaan werken om een bepaald doel te bereiken het projectplan met succes hebben ingediend voor financiering, moet er een onderliggende overeenkomst getekend worden als juridische grondslag voor de samenwerking. Een dergelijke overeenkomst is van belang voor partijen om juridische zekerheid te hebben over de rechten en plichten die voor de partijen gelden met betrekking tot de betreffende samenwerking.

De consortium/samenwerkingsovereenkomst regelt het volgende:

- Wie zijn de betrokken partijen?
- Wat is het doel en de reikwijdte van de samenwerking?
- Wie heeft welke verantwoordelijkheden en taken?
- Hoe zijn de financiële verplichtingen belegd?
- Wie heeft welke intellectuele eigendomsrechten?
- Wat wordt er vastgelegd over vertrouwelijkheid en geheimhouding?
- Wie is er aansprakelijk voor wat met welke verplichting tot schadevergoeding?
- Hoe eindigt de overeenkomst?
- Wat te doen in geval van conflict – geschilbeslechtingsregeling?
- Welk recht en jurisdictie zijn van toepassing op de overeenkomst?

Wanneer sprake is van een samenwerking met een kennisinstelling, zal vanuit deze kennisinstelling naast de overkoepelende consortium agreement het waarschijnlijk verplicht zijn om een Data Management Plan (DMP) op te stellen. In een DMP wordt beschreven hoe onderzoeksdata worden verzameld, beheerd, opgeslagen, gedeeld en bewaard, zowel tijdens als na een onderzoeksproject. Naast een beschrijving van de verschillende partijen die binnen een project betrokken zijn bij de verwerking van gegevens en mogelijk het delen van gegevens, wordt in het DMP het project omschreven en de doeleinden voor en wijze waarop gegevens worden verwerkt.

3. Data Management Plan (DMP)

Een standaard DMP omvat de volgende onderdelen/bijlagen (voor sommige geldt: enkel indien van toepassing):

- Het project/onderzoek voorstel.
- De consortiumagreement/samenwerkingsovereenkomst.
- Beschrijving van de data die verwerkt gaan worden in het project/onderzoek.
- Beschrijving van de software en hardware die gebruikt gaat worden in het project/onderzoek.
- Data verwerkersovereenkomsten. In geval van de verwerking van persoonsgegevens moet het hier gaan om een verwerkersovereenkomst of gezamenlijke verwerkingsverantwoordelijke overeenkomst. Van een verwerkersovereenkomst is sprake waneer een partij puur in opdracht van de andere partij persoonsgegevens verwerkt. Indien partijen gezamenlijk het doel en/of de middelen van de verwerking van persoonsgegevens bepalen is sprake van gezamenlijke verwerkingsverantwoordelijkheid en dient een gezamenlijke verwerkingsverantwoordelijke overeenkomst opgesteld te worden. Het kan nodig zijn meerdere van dergelijke overeenkomsten te moeten sluiten, dit is afhankelijk van de doeleinden van verwerking en de verschillende partijen die deze verwerking gaan uitvoeren.
- Autorisatiematrix: wie heeft binnen het project/onderzoek toegang tot welke data. In geval van persoonsgegevens moet deze toegang beperkt zijn tot diegenen die noodzakelijkerwijs toegang nodig hebben tot de persoonsgegevens. Uitgangspunt is dat gegevens indien mogelijk geanonimiseerd worden, en dat wanneer herleidbaarheid noodzakelijk is alle gegegevens enkel gepseudonimiseerd verwerkt worden. Binnen het project moeten afspraken gemaakt worden over hoe geanonimiseerd en/of gespeudonimiseerd gaat worden en door wie bepaald wordt onder welke omstandigheden partijen toegang krijgen tot de sleutel om de gepseudonimiseerde data te kunnen herleiden tot zogenoemde natuurlijke personen. Hiervoor kan gebruik gemaakt worden van technieken als federated learning and secure multi-party computation.
- Bij de verwerking van persoonsgegevens moet mogelijk verplicht een Data Protection Impact Assessment (DPIA) opgesteld worden. Bij projecten in de zorgsector bestaat deze verplichting altijd, aangezien gewerkt wordt met gevoelige gegevens van een kwetsbare groep.
- Naar aanleiding van de DPIA moet een overzicht gemaakt worden van de technische en organisatorische maatregelen die genomen worden om de de risico's die gepaard gaan met de verwerking van persoonsgegevens te beperken, waaronder pseudonimisering. Indien de verwerking van persoonsgegevens niet noodzakelijk is moet altijd gewerkt worden met anonieme gegevens. Mogelijke alternatieven voor persoonsgegevens zijn synthetische data of data van overleden personen.
- Controlelijst voor onderzoeksethiek. Op basis van deze checklist kan worden vastgesteld of het project/onderzoek moet worden voorgelegd aan een ethische onderzoekscommissie. Bij projecten in de zorg zal deze verplichting altijd bestaan, aangezien gewerkt wordt met gevoelige gegevens van een kwetsbare groep.
- Paragraaf over het controleren van de toepasselijkheid van de Wet medisch-wetenschappelijk onderzoek met mensen (WMO). Onderzoek valt onder de WMO als er sprake is van medisch wetenschappelijk onderzoek én personen aan handelingen worden onderworpen of hen gedragsregels worden opgelegd.
- Paragraaf over intellectuele eigendom (zou reeds uitgewerkt moeten zijn in de consortiumagreement/samenwerkingsovereenkomst, waarnaar dan verwezen kan worden).

- Paragraaf over hoe en waar data opgeslagen worden tijdens het project/onderzoek en hoe data en onderzoeksresultaten tijdens en/of na het project bewaard en/of toegankelijk voor derden gemaakt zullen worden.

4. Verwerken van persoonsgegevens

4.1 Definities

Wanneer er persoonsgegevens worden verwerkt, dan moet voldaan worden aan de vereisten van de Algemene Verordening Gegevensbescherming (AVG). De AVG is enkel van toepassing op de verwerking van persoonsgegevens van natuurlijke personen. Dit zijn personen die nog in leven zijn. Het is van belang om op te merken dat zowel het begrip 'persoonsgegeven' als het begrip 'verwerken' ruim worden uitgelegd, door zowel de data protectie autoriteiten – in Nederland de Autoriteit Persoonsgegevens (AP) – als de bevoegde rechterlijke instanties. Er is sprake van persoonsgegevens als deze een geïdentificeerd of identificeerbare persoon betreffen. Het begrip 'betreffen' bevat drie elementen waardoor een gegeven gerelateerd kan worden aan een persoon: inhoud, doel en resultaat. Er is geen noodzaak tot cumulatie, een van de drie elementen is voldoende voor gegevens om onder de definitie 'persoonsgegeven' te vallen. Zo is er niet alleen sprake van persoonsgegevens als de informatie gaat 'over' de persoon (bijv. een naam). Ook informatie die op zich niet over een persoon gaat, kan een persoonsgegeven worden als het doel is om een persoon te beoordelen, op een bepaalde wijze te behandelen of de status van de persoon te beïnvloeden. Een voorbeeld: een locatiegegeven hoeft op zich geen persoonsgegeven te zijn, maar als bij een taxichauffeur locatiegegevens worden gebruikt om te beoordelen of hij de beste routes rijdt, dan kan dit wel een persoonsgegeven zijn. Als informatie niet over een (geïdentificeerd of identificeerbare) persoon gaat en ook het doel van de verwerking niet is om een persoon te beoordelen of beïnvloeden, moet er gekeken worden of de verwerking gevolgen kan hebben voor de rechten of belangen van een persoon, het 'resultaat'.[1] Om ook weer locatiegegevens als voorbeeld te gebruiken: hoewel de GPS in een auto niet bedoeld is om bijzondere gegevens over iemand te onthullen, kan veelvuldig bezoek aan een ziekenhuis of een bepaalde religieuze instelling toch als resultaat hebben dat deze gegevens wel degelijk iets blootgeven over de persoon. Indien in een dataset geen onderscheid gemaakt kan worden tussen wat wel en niet persoonsgegevens zijn, dan moet de gehele dataset worden aangemerkt als persoonsgegevens.[2]

4.2 Bijzondere categorieën van persoonsgegevens

Bij de verwerking van persoonsgegevens gelden een groot aantal eisen, zoals de eis dat het doel van de verwerking specifiek en nauwkeurig bepaald moet zijn, niet meer gegevens verzameld en verwerkt mogen worden dan noodzakelijk is om dit doel te bereiken, transparantieverplichtingen en beveiligingsverplichtingen (art. 5 AVG). Bovendien moet er sprake zijn van een rechtmatige grondslag om persoonsgegevens te mogen verwerken. Bij zogenaamde bijzondere categorieën van persoonsgegevens, ofwel gegevens die een extra groot risico vormen voor de privacy van

[1] De Artikel 29 Werkgroep, ook wel bekend als de Groep gegevensbescherming artikel 29 is opgericht op grond van artikel 29 van Richtlijn 95/46/EG, de voorloper van de AVG. De Groep is een onafhankelijk Europees adviesorgaan inzake uitleg van de Richtlijn 95/46/EG, welke uitleg ook geldt voor de AVG. De European Data Protection Board heeft met ingang van de AVG de Artikel 29 Werkgroep vervangen. Groep Gegevensbescherming Artikel 29, Advies 4/2007 over het begrip persoonsgegeven. 01248/07/NL WP 136, Goedgekeurd op 20 juni 2007, p. 10 en 11.

[2] Bart van der Sloot, Sascha van Schendel & César Augusto Fontanillo López (2022) De invloed van (technische) ontwikkelingen op het begrip persoonsgegevens in relatie tot de AVG, p. 1, beschikbaar via: https://repository.wodc.nl/bitstream/handle/20.500.12832/3229/3224-influence-of-technical-developments-on-concept-personal-data-samenvatting.pdf?sequence=2&isAllowed=y

betrokkenen (degenen op wie de data betrekking hebben) zoals gezondheidsgegevens, moet er sprake zijn van een rechtmatige grondslag onder zowel artikel 6 als artikel 9 van de AVG.[3]

Uit foto's en video's zijn vaak bijzondere persoonsgegevens af te leiden. Maar als alle foto's en video's verwerkt zouden moeten worden als ware het bijzondere persoonsgegevens, ontstaat een situatie die praktisch gezien onwerkbaar is. De AP heeft daarom bepaald dat foto's en camerabeelden niet als bijzondere persoonsgegevens beschouwd worden als: "het doeleinde van de verwerking niet gericht is op het verwerken van bijzondere persoonsgegevens dan wel op het onderscheid maken op grond van een bijzonder persoonsgegeven; het voor de verwerkingsverantwoordelijke redelijkerwijs niet voorzienbaar is dat de verwerking zal leiden tot het maken van onderscheid op grond van een bijzonder persoonsgegeven; en de verwerking van die bijzondere persoonsgegevens onvermijdelijk is bij die verwerking."[4]

4.3 Verantwoordelijke en verwerker

Hieronder wordt nader ingegaan op een aantal relevante concepten en artikelen van de AVG in het kader van onderzoeksprojecten waarin persoonsgegevens worden verwerkt. Om te kunnen bepalen voor wie welke rechten en plichten uit de AVG gelden, is een belangrijke stap in het proces van verwerking van persoonsgegevens het in kaart brengen van de betrokken stakeholders en het doel. Op basis van het doel van de dataverwerking kan immers bepaald worden welke gegevens hiervoor *noodzakelijk* zijn, een belangrijk juridisch criterium om de vereiste rechtsgrondslag vast te kunnen stellen (art. 6 en 9 AVG, zie hierover paragraaf 4.6). Daarnaast geeft de doelomschrijving een goede indicatie van de opdracht die de ene partij aan de andere partij geeft. Dit is belangrijk vanuit een oogpunt van verantwoordelijkheid en aansprakelijkheid – enkel hetgeen binnen de gegeven opdracht valt, dus hetgeen *noodzakelijk* is om het doel te bereiken – komt voor verantwoordelijkheid van de verwerkingsverantwoordelijke. Indien de partij die de opdracht krijgt om persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke te verwerken (de verwerker art. 4 (8) AVG) zelf besluit de gegevens voor een ander doel te verwerken, dan wordt deze partij voor deze verwerking de verwerkingsverantwoordelijke. Voor deze verwerking bepaalt die partij namelijk het doel en de middelen (art. 4 (7) AVG).

Zoals hierboven aangegeven moeten persoonsgegevens enkel verwerkt worden indien dit noodzakelijk is, zo niet, dan moeten de gegevens geanonimiseerd worden. Indien het wel noodzakelijk is om persoonsgegevens te verwerken, moeten de risio's voor betrokkenen zoveel mogelijk beperkt worden. Een van de te nemen maatregelen in dit kader is het pseudonimiseren van persoonsgegevens.

4.4 Anonieme en pseudonieme gegevens

Het kan niet vaak genoeg gezegd worden: uitgangspunt van de AVG is dat persoonsgegevens enkel verwerkt mogen worden voor zover dat noodzakelijk is. Wanneer de verwerking van persoonsgegevens niet noodzakelijk is om een bepaalt gerechtvaardigd doel van de verwerkingsverantwoordelijke te bereiken, dan kan de verwerking enkel plaatsvinden met toestemming van de betrokkene. De eerste vraag die dus gesteld moet worden in relatie tot de

[3] Bijzondere categorieën van gegevens zijn op grond van artikel 9 AVG: persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbe schouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

[4] Autoriteit Persoonsgegevens, 'Cameratoezicht Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens' p. 26.

verwerking van persoonsgegevens is of het wel noodzakelijk is om, in een bepaalde fase van het onderzoeksproject, te werken met persoonsgegevens. Wanneer het behalen van een bepaald doel ook mogelijk is met data die niet te herleiden zijn naar een natuurlijke persoon, zoals synthetische data of data van overleden personen indien voldaan is aan de vereisten uit de WGBO, dan mogen er geen persoonsgegevens verwerkt worden. Op grond van de WGBO geldt het medisch beroepsgeheim ook voor gegevens van overleden personen. Dit kan voor wetenschappelijk onderzoek doorbroken worden door een bij leven gegeven toestemming of wanneer het vragen van toestemming na overlijden onmogelijk of onevenredig is. De Gedragscode Gezondheidsonderzoek (beschikbaar via coreon.org) geeft uitleg hoe te voldoen aan de (U)AVG en de WGBO bij het verwerken van gezondheidsdata van overleden personen. Pseudonimiseren van gegevens is hierbij een van de vereisten. Een andere optie is om een dataset waarin persoonsgegevens voorkomen aan de bron te anonimiseren.

Er is sprake van anonieme gegevens wanneer deze gegevens niet terug herleid kunnen worden naar een identificeerbare natuurlijke persoon. Het verschil met pseudonimiseren wordt duidelijk op grond van de definitie uit artikel 4 (5) van de AVG: “het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld”. Bij pseudonieme data kan terug herleiden dus wel, door diegene die over de sleutel beschikt om de gegevens te herleiden.[5] Dit hoeft niet dezelfde persoon te zijn als degene die de pseudonieme gegevens verwerkt. Dus ook personen die gegevens verwerken die zij zelf niet kunnen herleiden tot een identificeerbare natuurlijke persoon, zijn gebonden aan de vereisten van de AVG als een ander die gegevens wel kan terug herleiden naar een persoon. Ook voor pseudonieme data geldt dus in principe dat verwerking van persoonsgegevens noodzakelijk moet zijn of er moet sprake zijn van toestemming. In dit kader speelt echter wel een interessante discussie momenteel: moeten we de vraag of sprake is van anonieme of pseudonieme data beantwoorden op basis van de relatieve of de absolute benadering?

4.5 Relatieve vs. Absolute benadering

De discussie over de kwalificatie van persoonsgegevens onder de AVG betreft de vraag of de “absolute” of “relatieve” benadering moet worden toegepast. De gangbare benadering is de absolute benadering. In deze benadering zijn persoonsgegevens alle gegevens die direct of indirect aan een individu kunnen worden gekoppeld, ongeacht wie er over de middelen voor heridentificatie beschikt.6 Onder deze benadering worden gegevens sneller als persoonsgegevens gekwalificeerd dan bij de relatieve benadering. Bij de relatieve benadering wordt namelijk gekeken naar de middelen die redelijkerwijs ter beschikking staan van degene die daadwerkelijke met de gegevens gaat werken, om deze gegevens te kunnen herleiden tot een natuurlijke persoon. In de concrete situatie waarbij een pseudonieme dataset van de ene partij (verstrekker) wordt overgedragen aan een andere partij (ontvanger) wordt dus het perspectief van de gegevensontvanger overwogen en de vraag gesteld of hij redelijkerwijs over de middelen kan beschikken voor heridentificatie. Als de gegevensontvanger geen aanvullende informatie heeft waarmee hij de betrokkenen kan identificeren en geen wettelijke middelen heeft om toegang te krijgen tot dergelijke informatie, kan de overgedragen informatie als geanonimiseerd worden beschouwd voor de ontvanger. Dit

[5] Zie overweging 26 van de AVG voor een uitleg over het verschil tussen anonimiseren en pseudonimiseren.
[6] Groep Gegevensbescherming Artikel 29, Advies 4/2007 over het begrip persoonsgegeven, 20 juni 2007, 01248/07/NL WP 136. Europees Comité voor Gegevensbescherming, Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679 en Europees Comité voor Gegevensbescherming, Richtsnoeren 01/2025 inzake pseudonimiseren.

betekent dat deze gegevens dus niet als persoonsgegevens aangemerkt hoeven te worden en de AVG niet van toepassing is voor de gegevensontvanger. Het feit dat degene die de gegevens heeft verstrekt de middelen heeft om de betrokkenen opnieuw te identificeren, betekent in de relatieve benadering niet automatisch dat de overgedragen informatie ook persoonsgegevens vormen voor de ontvanger.

Een eerste stap in de richting van een relatieve benadering kan gevonden worden in de zaak Breyer.[7] Hier is geoordeeld dat er geen sprake is van persoonsgegevens als identificatie van de betrokkene verboden is of praktisch gezien onmogelijk is. Dit biedt geen uitkomst in zaken waarbij zorgorganisaties pseudonieme data delen met andere zorgorganisaties en onderzoekers van kennisinstellingen. In deze situaties is herleidbaarheid immers niet wettelijk verboden of praktisch onmogelijk, de sleutel tot herleidbaarheid is gewoon aanwezig bij de verstrekkende zorgorganisatie. In twee meer recente Europese zaken wordt ook een contextuele, relatieve benadering gekozen bij het beoordelen van de vraag of gegevens kwalificeren als persoonsgegevens, waarbij het perspectief van de ontvanger en het risico op heridentificatie worden meegewogen.[8] Op 26 april 2023 heeft het Gerecht van de Europese Unie in de zaak *SRB vs. EDPS* geoordeeld dat gepseudonimiseerde gegevens die naar een ontvanger worden verzonden niet als persoonsgegevens worden beschouwd als de ontvanger van de gegevens niet over de middelen beschikt om de betrokkenen opnieuw te identificeren.[9] In deze zaak is hoger beroep ingesteld. Hier is het nog wachten op een uitspraak, maar Advocaat Generaal Spielman lijkt in zijn opinie van 6 februari 2025 in dit hoger beroep de relatieve benadering te ondersteunen.[10] Zijn betoog komt erop neer dat wanneer een ontvanger van gegevens niet over de juridische of technische middelen beschikt om de gegevens te herleiden tot natuurlijke personen, de gepseudonimiseerde gegevens mogelijk niet beschouwd moeten worden als persoonsgegevens voor de ontvanger. Dit perspectief suggereert dat identificeerbaarheid moet worden beoordeeld op basis van de specifieke context en de middelen waarover de ontvanger van de gegevens beschikt. Dit betekent ook dat gegevens voor de verstrekker wel, maar voor de ontvanger mogelijk geen persoonsgegevens zijn.

De opinie van de AG wordt in de literatuur zowel in positieve als in negatieve zin becommentarieerd.[11] Op 16 januari 2025 heeft het Europees Comité voor Gegevensbescherming richtlijnen gepubliceerd over pseudonimiseren. In overweging 22 van deze richtlijnen wordt uitdrukkelijk afstand genomen van de relatieve benadering: “Gepseudonimiseerde gegevens, die door het gebruik van aanvullende informatie aan een natuurlijke persoon kunnen worden toegeschreven, moeten worden beschouwd als informatie over een identificeerbare natuurlijke persoon en zijn daarom persoonsgegevens. Deze verklaring geldt ook als gepseudonimiseerde gegevens en aanvullende informatie niet in handen zijn van dezelfde persoon. Als gepseudonimiseerde gegevens en aanvullende informatie redelijkerwijs kunnen worden gecombineerd, door de verwerkingsverantwoordelijke of een andere persoon, dan zijn de gepseudonimiseerde gegevens persoonsgegevens. Zelfs als alle aanvullende informatie die de

[7] Conlusie van Advocaat-Generaal M. Campos Sánchez-Bordona, 12 mei 2016, Zaak C-582/14, Breyer, r.o. 68. Arrest van het Hsof 19 oktober 2016, Zaak C-582/14, Breyer, r.o. 44-46.
[8] ECLI:EU:C:2023:385 (Gesamtverband Autoteile-Handel e.V. v Scania CV AB) (C-319/22) ECLI:EU:T:2022:273 (T-384/2).
[9] Arrest van het Gerecht, 26 april 2023, zaak T-557/20, ECLI:EU:T:2023:219.
[10] Opinie van Advocaat Generaal Spielman, 6 February 2025, zaak C-413/23 P *European Data Protection Supervisor v Single Resolution Board,* ECLI:EU:C:2025:59, r.o. 51-51.
[11] Zie voor een erkenning van een praktische oplossing McCann FitzGerald, beschikbaar via: https://www.mccannfitzgerald.com/knowledge/data-privacy-and-cyber-risk/advocate-generals-opinion-signals-a-pragmatic-approach-to-pseudonymisation?utm_source=chatgpt.com. Voor een kritische noot zie Nirmalya Chaudhuri, Must “personal data” always be “relative”? 13 mei 2025, DOI10.21428/9885764c.edcc137b, beschikbaar via: https://www.europeanlawblog.eu/pub/4ubxito8/release/1.

pseudonimiserende verwerkingsverantwoordelijke bewaart, is verwijderd, worden de gepseudonimiseerde gegevens pas anoniem als aan de voorwaarden voor anonimiteit is voldaan." (Bijgeschaafde Google translate vertaling uit het Engelse document). Tot en met 14 maart 2025 bestond de mogelijkheid om in een publieke consultatie een zienswijze over deze richtlijnen naar voren te brengen. De richtlijnen zijn op het moment van schrijven nog niet definitief.[12]
Uit voorgaande kunnen we voor nu concluderen dat data die door zorginstellingen pseudoniem verstrekt worden aan andere partijen binnen een consortium aangemerkt moeten worden als persoonsgegevens. Het is immers niet wettelijke verboden of praktisch onmogelijk en redelijkerwijs te verwachten dat binnen de samenwerking pseudonieme data met aanvullende informatie tot een natuurlijke persoon herleid kunnen worden. Dit betekent dat de AVG van toepassing is en dat er sprake moet zijn van een rechtmatige verwerkingsgrondslag. Voor gezondheidsgegevens die kwallificeren als bijzondere categorie van persoonsgegevens, moet sprake zijn van een grondslag onder zowel artikel 6 als artikel 9 van de AVG.

4.6 Rechtmatige grondslag onder art. 6 en 9 AVG

Bij de verwerking van persoonsgegevens voor onderzoek ter verbetering van (de kwaliteit) van gezondheidszorg kunnen een aantal rechtsgrondslagen onder artikel 6 AVG in aanmerking komen. In de eerste plaats toestemming van de patiënten wiens gegevens verwerkt worden. Het kan echter lastig zijn om achteraf van een zeer grote groep patiënten alsnog toestemming te verkrijgen voor de verwerking van persoonsgegevens voor een bepaald onderzoek, als deze toestemming niet reeds verkregen is bij de oorspronkelijke verzameling van deze gegevens. Ook heeft toestemming als verwerkingsgrond de nodige nadelen, zo moet er een administratie gevoerd worden, ligt de bewijslast bij de verwerkingsverantoordelijke en kan toestemming altijd worden ingetrokken, waarna de gegevens niet meer verwerkt mogen worden. Andere rechtsgrondslagen waarop de verwerking mogelijk gebaseerd kan worden zijn: noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde wanneer deze belangen zwaarder wegen dan het privacybelang van betrokkenen, noodzakelijk voor de uitvoering van een overeenkomst, en noodzakelijk ter uitvoering van een wettelijke plicht.

4.6.1 Gerechtvaardigde belangen

Bij het baseren van de vewerking van persoonsgegevens op gerechtvaardigde belangen is het altijd maar de vraag of de belangen van de verwerkingsverantwoordelijke en/of derden zwaarder wegen dan de (privacy) belangen van patiënten. Dit is om die reden dan ook geen stabiele verwerkingsgrond, omdat deze afweging uiteindelijk door de AP of een rechter definitief gemaakt zal worden. In andere woorden, ookal kan de verwerkingsverantwoordelijke een zeer goede onderbouwing geven waarom zijn belang of het belang van derden zwaarder weegt, biedt dit nooit garanties dat de AP of een rechter deze redenering zullen volgen. In medische behandelrelaties wordt ook gewezen op de zorgovereenkomst als rechtsgrondslag voor de verwerking van persoonsgegevens.

4.6.2 Overeenkomst

Voor de verwerking van persoonsgegevens op basis van de zorgovereenkomst wordt inspiratie opgedaan bij het project GERDA.13 In dit project wordt een data-infrastructuur ontwikkeld om

[12] Voor zowel de tekst van de richtlijnen als de zienswijzen die zijn ontvangen in de publieke consultatie zie: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en

[13] Zie voor meer informatie over dit project: Werkgroep GERDA, Whitepaper Geïntegreerde Regionale Data-infrastructuur Achterhoek (GERDA). Een analyse naar de mogelijkheden voor een domeinoverstijgende data-

gezondheidsdata bij elkaar te brengen en te delen voor primair en secundair gebruik. Voor de verwerking van persoonsgegevens voor de deelnemende partijen wordt de (zorg)overeenkomst als rechtsgrondslag aangemerkt: “Partijen verlenen zorg en zijn
wettelijk verplicht dat goed te doen. Daarnaast hebben de organisaties processen ingericht om de kwaliteit van zorg te monitoren en te verbeteren. Deze datasamenwerking stelt de (zorg)organisaties in staat om -op basis van de resultaten- de zorg voor subgroepen zorgvragers en (daardoor) ook van individuen te verbeteren.”[14] Ook deze rechtsgrondslag is niet waterdicht, aangezien er hierbij vanuit gegaan moet worden dat de zorgovereenkomst elke verwerking van persoonsgegevens dekt die als doel heeft de kwaliteit van zorg te verbeteren. Of de bewoordingen van de gemiddelde zorgovereenkomst hier specifiek genoeg op gericht zijn, is een open vraag. Bovendien lijkt de overeenkomst geen rechtsgrond te bieden voor de verwerking van bijzondere categorieën persoonsgegevens onder artikel 9 AVG. Onder artikel 9(2) (h) wordt wel gesproken over een overeenkomst met een gezondheidswerker, maar enkel voor zover de verwerking van de bijzondere categorieën persoonsgegevens noodzakelijk is voor - zover relevant hier - medische diagnosen en het verstrekken van gezondheidszorg. In het Whitepaper van GERDA wordt niet expliciet ingegaan op artikel 9 AVG. Navraag heeft uitgewezen dat de redenering is dat bijzondere persoonsgegevens verwerkt mogen worden vanwege het verstrekken van gezondheidszorg hetgeen inherent is aan de zorgovereenkomst. Artikel 9 (2) (h) AVG wordt dus aangemerkt als rechtsgrondslag. In relatie tot ‘onderzoek voor beleidsvorming’ wordt in het Whitepaper gesteld dat voor het gebruik van (bijzondere) persoonsgegevens (iets) andere regels kunnen gelden dan voor ‘onderzoek ter verbetering van de zorg’.[15] Hierij wordt vervolgens verwezen naar de algemene branchevoorwaarden van ACTIZ, waarin staat dat expliciete toestemming aan cliënten gevraagd moet worden voor het gebruik van hun gegevens anders dan voor wetenschappelijk onderzoek ten behoeve van (verbetering van) de zorg. Zoals uit onderstaande zal blijken is het zeker niet evident dat voor wetenschappelijk onderzoek ten behoeve van verbetering van de zorg ook geen sprake moet zijn van toestemming, tenzij dit onmogelijk of onevenredig is.

4.6.3 Wettelijke plicht

Of de verwerking van persoonsgegevens gedekt is door een bestaande wettelijke plicht in Nederland roept een vergelijkbare vraag op als in relatie tot de zorgovereenkomst: kun je een algemeen geformuleerde zorgplicht voor het verlenen van kwalitatief goede zorg en/of het verbeteren van de zorg zo uitleggen dat hiermee dus de verwerking van persoonsgegevens ten behoeve van het verlenen van kwalitatief goede zorg of het vebeteren van zorg gedekt is? Hoewel het discutabel is dat de wettelijke plichten voor het bieden van goede zorg hiervoor al specifiek genoeg zijn, lijkt hier verandering in te komen door de “Wijziging van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) in verband met het regelen van regie op kwaliteitsregistraties in de zorg en grondslagen om ten behoeve van die kwaliteitsregistraties bijzondere persoonsgegevens te kunnen verwerken (Wet kwaliteitsregistraties zorg)”. In de Memorie van Toelichting wordt het doel van de wet als volgt omschreven: “Dit wetsvoorstel zorgt voor de benodigde wettelijke grondslagen voor het rechtmatig, goed en efficiënt functioneren van kwaliteitsregistraties. Onder een kwaliteitsregistratie wordt verstaan de verzameling, gegevensopslag en verdere verwerking van gegevens over een welomschreven cliëntenpopulatie, gedefinieerd aan de hand van de onderlinge overeenkomsten die de cliënten vertonen in hun aandoening, ziekte, zorgtype of complicatie, of combinaties daarvan met als doel om de kwaliteit van zorg aan die cliëntenpopulatie te meten en te verbeteren. Op basis van

infrastructuur, 5 juli 2022. Beschikbaar via: https://populationhealthdata.nl/wp-content/uploads/2022/08/Whitepaper_Overzicht_mogelijkheden_domein-overstijgende_data-infrastructuur_en_technisch_ontwerp_GERDA.pdf

[14] Projectgroep Gerda, Whitepaper Governance bij toepassing MPC, 25 april 2023. Beschikbaar via: https://populationhealthdata.nl/wp-content/uploads/2023/05/Whitepaper-inrichting-Governance-bij-toepassing-MPC.pdf

[15] Idem, p. 29.

de rapportages van deze kwaliteitsregistraties kunnen zorgverleners en zorgaanbieders leren van elkaar en zo de kwaliteit van zorg verbeteren. De kwaliteitsregistraties dienen daarmee een algemeen belang ter borging en verbetering van de kwaliteit van zorg."16 Naast dit wetsvoorstel kan tevens gewezen worden op het wetsvoorstel Evaluatie Wkkgz.17 Uit de Memorie van Toelichting bij dit wetsvoorstel blijkt dat onder goede zorg ook valt het delen van informatie, zowel van één patient in de keten maar ook het delen van informatie binnen een samenwerking ten behoeve van een groep patiënten met specifieke zorgbehoeften.18 Als beide wetsvoorstellen zijn aangenomen is het waarschijlijk dat hiermee een voldoende wettelijke basis gecreëerd is voor Nederland om persoonsgegevens te kunnen delen in onderzoeksprojecten waarbij (de verbetering van) kwaliteit van zorg het doel is.

4.6.4 Verenigbare verwerking

Naast de drie hierboven behandelde rechtgrondslagen, moet ook worden stilgestaan bij het concept 'verenigbare verwerking'. Als persoonsgegevens verwerkt worden voor een doel dat verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, mag dit onder bepaalde voorwaarden zonder dat een andere afzonderlijke rechtsgrond vereist is (artikel 6 (4) AVG). De verdere verwerking lift dan als het ware mee op de grondslag waarop de oorspronkelijke verzameling van persoonsgegevens rust. Verdere verwerking van persoonsgegevens met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden mag als een met de aanvankelijke doeleinden verenigbare rechtmatige verwerking worden beschouwd. Hoewel deze uitzondering een mogelijkheid biedt voor het verdere verwerken van persoonsgegevens voor wetenschappelijke doeleinden, is dit niet het geval voor het verder verwerken van bijzondere categorieën van persoonsgegevens. Aangezien er bij wetenschappelijk onderzoek in de medische sector vrijwel altijd sprake zal zijn van de verwerking van gezondheidsgegevens, is naast een rechtsgrondslag onder artikel 6, ook een rechtsgrondslag onder artikel 9 vereist.

4.6.5 Verdere vewerking voor wetenschappelijk onderzoek

Bij de verwerking van (bijzondere categorieën) persoonsgegevens op basis van toestemming voor wetenschappelijk onderzoek, moet gewezen worden op drie belangrijke aandachtspunten:

1. Ten eerste overweging 33 van de AVG waarin is bepaalt: "omdat het niet altijd mogelijk is om op het ogenblik waarop de persoonsgegevens worden verzameld het doel van de gegevensverwerking voor wetenschappelijke onderzoeksdoeleinden volledig te omschrijven, moeten betrokkenen worden toegestaan hun toestemming te geven voor bepaalde terreinen van het wetenschappelijk onderzoek waarbij erkende ethische normen voor wetenschappelijk onderzoek in acht worden genomen. Betrokkenen moeten de gelegenheid krijgen om hun toestemming alleen te geven voor bepaalde onderzoeksterreinen of onderdelen van onderzoeksprojecten, voor zover het voorgenomen doel zulks toelaat." Deze overweging laat dus specifiek voor wetenschappelijk onderzoek enige ruimte met betrekking tot het vereiste van artikel 5 (1) (b) AVG dat een doel 'welbepaald en uitdrukkelijk omschreven' moet zijn.
2. Een tweede aandachtspunt betreft de vraag wanneer de verwerking van persoonsgegevens niet langer geacht kan worden plaats te vinden in het kader van wetenschappelijk

[16] Tweede Kamer, vergaderjaar 2022–2023, 36 278, nr. 3, p. 1.
[17] Wijziging van de Wet kwaliteit, klachten en geschillen zorg naar aanleiding van de evaluatie van die wet (Evaluatiewet Wkkgz) (KetenID WGK013894) Alle documenten beschikbaar via de website van de openbare internetconsultatie die met betrekking tot dit wetsvoorstel heeft plaatsgevonden: https://www.internetconsultatie.nl/evaluatiewetwkkgz/b1#sectie-waarkuntuopreageren
[18] Zie onder 1.1 en 3.2 van de Memorie van Toelichting van de Evaluatiewet Wkkgz.

onderzoek. Wanneer sprake is van het valideren van het wetenschappelijke onderzoek in real-life situaties met daadwerkelijke gezondheidsinterventies, is de scope van het onderzoek waarschijnlijk de fase van wetenschappelijk onderzoek voorbij en moet of kan de verwerking mogelijk gestoeld worden op andere verwerkingsgrondslagen. Bij het vragen van toestemming voor wetenschappelijk onderzoek, kan het op voorhand wellicht verstandig zijn ook de fase van het onderzoek bij real-life validatie specifiek te beschrijven als zijnde onderdeel van het onderzoek en/of een fase die gedekt wordt door de toestemming.

3. Als derde aandachtspunt kan erop gewezen worden dat de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) slechts heel zelden de mogelijkheid biedt om bijzondere categorieën persoonsgegevens te verwerken voor wetenschappelijk onderzoek zonder dat toestemming noodzakelijk is. Artikel 24 van de UAVG bepaalt namelijk dat het verbod om deze gegevens te verwerken niet van toepassing is indien de verwerking noodzakelijk is met het oog op wetenschappelijk onderzoek, dit onderzoek een algemeen belang dient, het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Alleen wanneer het vragen van toestemming dus onmogelijk is of een onevenredige inspanning kost kan de verwerking van bijzondere categorieën van persoonsgegevens voor wetenschappelijk onderzoek plaatsvinden zonder toestemming.

4.6.6 Rechtsgrondslag voor bijzondere persoonsgegevens

Gezien de nadelen van toestemming is het verstandig om te kijken of de verwerking van bijzondere categorieën van persoonsgegevens op een andere rechtsgrondslag gebaseerd kan worden. In artikel 9 (2) (h) staat een uitzondering op het verwerkingsvergbod voor onder andere verwerkingen die noodzakelijk zijn “voor doeleinden van preventieve of arbeidsgeneeskunde (…), medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen (…)”. Deze uitzondering lijkt niet van toepassing op de fase van wetenschappelijk onderzoek, waarin nog sprake is van de ontwikkeling van een product of dienst ten behoeve van de medische sector en nog geen sprake is van daadwerkelijke diagnosen of gezondheidszorg. Mogelijk dat deze verwerkingsgrondslag na de fase van puur wetenschappelijk onderzoek, waarbij gevalideerd wordt in de praktijk met daadwerkelijke zorginterventies, wel relevant is. In artikel 9 (2) (i) staat een uitzondering wanneer de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim. Op grond van artikel 9 (3) mogen de gegevens bij deze rechtsgrondslag alleen worden verwerkt door of onder de verantwoordelijkheid van een beroepsbeoefenaar die gebonden is aan het beroepsgeheim. Op grond van artikel 9 (2) (j) kunnen bijzondere categorieen van persoonsgegevens woren verwerkt voor zover noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, lid 1, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de belangen van de betrokkene.
Zoals hieroven reeds beschreven, zal er op grond van artikel 24 UAVG in Nederland toch vrijwel altijd toestemming noodzakelijk zijn als gegevens op deze grond verwerkt worden.

4.7 Kernvereisten art. 5 AVG

Als de AVG van toepassing is en er een rechtmatige verwerkingsgrondslag is onder artikel 6 en indien van toepassing artikel 9 AVG, mogen persoonsgegevens enkel verwerkt worden als voldaan is aan alle vereisten die de AVG stelt. Niet naleving van de AVG kan leiden tot hoge boetes (art. 83 AVG). In deze juridische verantwoording gaan we niet alle rechten en plichten die voortvloeien uit de AVG met diepgang analyseren, maar volstaan we met kort te wijzen op de 8 kernbeginselen voor de verwerking van persoonsgegevens. Deze zijn neergelegd in artikel 5 van de AVG.
Het eerste vereiste betreft rechtmatigheid van de gegevensverwerking (art. 5 (1) (a)). Hiertoe is, zoals hierboven al beschreven, een verwerkingsgrondslag onder artikel 6 AVG voor persoonsgegevens en onder artikel 6 en 9 AVG voor bijzondere categorieën van persoonsgegevens noodzakelijk.

Vervolgens vereist art. 5 AVG voor de verwerking van persoonsgegevens dat deze verwerking voldoet aan de beginselen van: transparantie (a), doelbinding (b), minimale gegevensverwerking (c), juistheid (d), opslagbeperking (e), integriteit en vertrouwelijkheid (beveiliging) (f), en verantwoording (accountability) (g). Het vereiste van transparantie is nader uitgewerkt in in de artikelen 12-14 AVG, hierbij gaat het om verplichtingen om op eigen initiatief en op verzoek van betrokkenen informatie te verschaffen. Dit beginsel hangt nauw samen met de rechten die betrokkenen hebben met betrekking tot de data die naar hen te herleiden is. Deze rechten zijn vastgelegd in artikel 14 t/m 22 AVG. Verwerkingsverantwoordelijken zijn verplicht om het proces van gegevensverwerking organisatorische en technisch zo te regelen dat het eenvoudig is voor betrokkenen om gebruik te maken van deze rechten en dat tijdig opvolging gegeven wordt aan verzoeken van betrokkenen.

Onderdeel van transparantie is duidelijkheid bieden over het doel van de verwerking van persoonsgegevens, de wijze waarop gegevens worden opgeslagen, voor hoe lang en wie er toegang hebben tot de informatie, wat voor maatregelen er genomen zijn om de juistheid en integriteit en vertrouwelijkheid te borgen. Dit moet gebeuren via goede privacyverklaringen en voor het verkrijgen van toestemmingen moet gewerkt worden met duidelijke informatiebrieven en standaard toestemmingsformulieren waarmee vrij, specifiek, geïnformeerd en uitdrukkelijk toestemming kan worden verleend. Het kan nodig zijn om voor meerdere verwerkingen voor verschillende doeleinden apart toestemming te vragen, zodat patiënten wel overwogen en specifieke keuzes kunnen maken. Toestemming voor het gebruik van een medisch hulpmiddel betreft in principe enkel het gebruik van dat hulpmiddel, en omvat nog niet ook toestemming voor het mogen verwerken van de persoonsgegevens die dit hulpmiddel genereerd. Hiervoor moet apart toestemming worden gevraagd. Met het oog op de beveiliging van persoonsgegevens zijn ook de artikelen en de artikelen 32-34 AVG van belang, waarin de beveiligingsplicht en de meldplicht datalekken in zijn opgenomen. Artikel 32 wijst in het kader van beveiliging expliciet op pseudonimisering: “Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten: a) de pseudonimisering en versleuteling van persoonsgegevens (…).” Daarnaast zijn de artikelen 25 en 35 AVG van belang die hieronder in 4.8 besproken worden.

Tot slot is het beginsel van accountability van de AVG van belang. Op grond van dit beginsel moet niet alleen voldaan worden aan de vereisten van de AVG, maar moet de naleving hiervan ook aantoonbaar zijn. Alvorens persoonsgegevens verwerkt mogen worden, moet een aantal onderliggende documenten die aantonen dat de verwerking in overeenstemming met de AVG plaatsvindt gereed zijn. Het beginsel van accountability is daarom nauw verbonden met het beginsel

van transparantie. Op grond van de AVG moeten de volgende documenten in orde zijn: overzicht van genomen technische en organisatorische maatregelen naar aanleiding van de uitgevoerde DPIA (art. 24-25 AVG), Gezamenlijke verwerkingsverantwoordelijkenovereenkomst(en) en/of verwerkersovereenkomst(en) (art. 26 en 28 AVG), Register van de verwerkingsactiviteiten (art. 30 AVG), DPIA (art. 35 AVG). Als persoonsgegevens worden doorgegeven naar derde landen kunnen nog andere documenten vereist zijn zoals een contract of Bindende Bedrijfsvoorschriften (art. 46 en 47 AVG). Aangezien het niet aan te raden is gegevens buiten de EU te verwerken in het kader van onderzoeksprojecten met persoonsgegevens wordt hier niet verder op in te gaan. Advies is om altijd gebruik te maken van partijen en servers en clouds die zich binnen de EU bevinden.

4.8 DPIA, PbDD en PET

Een Data Protection Impact Assessment (in de AVG in artikel 35 bekend onder de naam 'gegevensbeschermingseffectbeoordeling') is een instrument om de risico's in te schatten van de verwerking van persoonsgegevens. Wanneer de verwerking van persoonsgegevens waarschijnlijk een hoog privacyrisico oplevert voor betrokkenen, dan is het uitvoeren van een DPIA verplicht alvorens over te gaan tot de verwerking van persoonsgegevens. Bij het werken met gezondheidsgegevens van patienten is het uitvoerin van een DPIA verplicht. Op basis van de geïnventariseerde risico's moeten vervolgens organisatorische en technische maatregelen worden genomen om deze risico's te beperken. Deze maatregelen moeten worden ingevoerd volgens de beginselen van 'Privacy by Design en Privacy by Default'. In artikel 25 van de AVG bekend als 'Gegevensbescherming door ontwerp en door standaardinstellingen'. Het idee achter deze beginselen is dat de kernbeginselen van de verwerking van persoonsgegevens zo goed mogelijk gewaarborgd worden in het design van een product of dienst en dat in de standaardinstelling zo min mogelijk persoonsgegevens worden verwerkt. De verwerkingsverantwoordelijke moet hiertoe zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen nemen, zoals pseudonimisering. Het doel is de nodige waarborgen in de verwerking in te bouwen ter naleving van de AVG en ter bescherming van de rechten van de betrokkenen en om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking.

Bij het vaststellen van technische en organisatorische maatregelen moet gekeken worden naar de mogelijkheid van het inzetten van zogenaamde Privacy Enhancing Technologies (PETs). Dit zijn technologieën die bijdragen aan het op een privacyvriendelijke manier verwerken van persoonsgegevens. Bekende voorbeelden in het zorgdomein zijn 'federated learning' en 'multi party computation'. Bij federated learning gaat het om een manier om algoritmes te trainen op lokale, gedecentraliseerde gegevens, terwijl het bij multi party computation gaat om een cryptografische techniek waarmee partijen gezamenlijke berekeningen uit kunnen voeren op gedeelde gegevens. [19]

[19] Op de website van de Interbestuurlijke Datastrategie (IBDS)is een overzicht en uitleg opgenomen van verschillende Privacy Preserving Technologie waaronder Federated Learning en Multi Party Computation: https://realisatieibds.nl/groups/view/c23ab74c-adb4-424e-917d-773a37968efe/kenniscentrum-van-de-ibds/wiki/view/a2d325d4-0047-4967-8200-c4a29e392060/privacy-enhancing-technologies-pet

5. Tot besluit

Tot slot wordt nog gewezen op twee belangrijke juridische aandachtspunten. In de eerste plaats dat het bij juridische compliance gaat om een doorlopende cyclus, en niet om een eenmalige check. Gedurende de gehele looptijd van het project moet er aandacht zijn of de regels van toepassing op de verwerking van gegevens nageleefd worden. Binnen een project zal er dus iemand verantwoordelijk moeten zijn voor het datamanagement en het toezicht hierop. Dit kan worden belegd bij een functionaris voor gegevensbescherming (art. 37 AVG). Wanneer er wijzigingen plaatsvinden, bijvoorbeeld in stakeholders, data of doeleinden voor verwerking, moet steeds opnieuw bekeken worden wat dit betekent voor juridische compliance en moeten waar nodig aanpassingen worden gedaan om de compliance te blijven borgen.

Een tweede belangrijk aandachtspunt betreft eigenaarschap van data. Hoewel het gangbaar is om te spreken over eigenaarschap van data, is vanuit juridisch oogpunt 'eigenaarschap' een lastig concept in relatie tot data.[20] Dit houdt verband met de definitie van eigendom in artikel 5:1 van het Nederlandse Burgerlijk Wetboek:

Eigendom is het meest omvattende recht dat een persoon op een zaak kan hebben.
Het staat de eigenaar met uitsluiting van een ieder vrij van de zaak gebruik te maken, mits dit gebruik niet strijdt met rechten van anderen en de op wettelijke voorschriften en regels van ongeschreven recht gegronde beperkingen daarbij in acht worden genomen.

Wat een zaak is wordt gedefinieerd in artikel 3:2 Burgerlijk Wetboek: "Zaken zijn de voor menselijke beheersing vatbare stoffelijke objecten". Data is als als zodanig geen "voor de menselijke beheersing stoffelijk object" en als je eigenaar bent van een fysieke houder (zoals een USB-stick) waarop data staan, dan betekent dit niet dat anderen geen rechten kunnen hebben op de data die op de houder staat, en is er dus geen sprake van "met uitsluiting van een ieder gebruik te kunnen maken van de zaak". Of dit kan, hangt ervan af of er op de data bijvoorbeeld gegevensbeschermingsrechten of auteursrechten van anderen rusten. Juridisch gezien gaat het daarom bij data om vragen als: "Wie kan er over de data beschikken en welke rechten van anderen rusten er mogelijk op die data?" Iemand die over data kan beschikken is daarom juridisch gezien geen *eigenaar*, maar mogelijk een van meerdere partijen die kunnen beschikken over of rechten hebben op deze data.

Hoewel juridisch gezien het concept eigendom van data dus niet correct is, wordt er toch vaak gesproken van data eigenaarschap. Het gaat er dan om vast te leggen welke partij, wat voor soort data ter beschikking stelt aan welke andere partij(en) voor welk doel, voor welke duur, en vooral ook wie er beschikkingsbevoegd zijn met betrekking tot eventuele binnen een project gegenereerde nieuwe data, in de zin wie welke rechten heeft op deze data. Hierbij dus de nadrukkelijke kanttekening dat er altijd ook nog andere partijen rechten op data kunnen hebben, en er dus geen sprake is van absolute eigendom(soverdracht), wanneer data door de ene partij beschikbaar worden gesteld aan een andere partij. Ongeacht of in de overeenkomst gesproken wordt van "data-eigenaar".

Zoals hierboven meerdere keren benadrukt: verwerk enkel persoonsgegevens indien noodzakelijk. Interessant om in dit kader te vermelden, is dat in veel fases van de ontwikkeling van een data model het niet noodzakelijk is om te werken met persoonsgegevens. Datasets kunnen geanonimiseerd worden aan de bron, eventueel met behulp van scripts geleverd door de data scientists aan de zorgorganisaties, of er kan gewerkt worden met synthetische data. Ook is voor niet alle vormen van validatie het werken met persoonsgegevens noodzakelijk. Wanneer validatie op het

[20] Zie hierover bijvoorbeeld: https://www.dirkzwager.nl/kennis/artikelen/eigendom-van-data/https://bg.legal/het-eigendom-van-data/

niveau van natuurlijke personen wel noodzakelijk is, kan bovendien overwogen worden om deze validatie plaats te laten vinden binnen de zorginstelling. Op deze wijze ontstaat er bij de overige betrokken partijen in het ontwikkelproces geen noodzaak om persoonsgegevens te verwerken. Alleen wanneer dit noodzakelijk is, omdat validatie binnen de zorginstelling bijvoorbeeld niet mogelijk of onredelijk bezwarend is, zou er noodzaak ontstaan tot het verwerken van persoonsgegevens door andere betrokken partijen, waarbij vanuit een oogpunt van veiligheid en privacybescherming deze gegevens enkel in pseudonieme vorm verwerkt mogen worden en er zoveel mogelijk gebruik gemaakt moet worden van Privacy Enhancing Technologies (PETs) om het risico voor betrokkenen zo klein mogelijk te houden. Bij validatie in real-life scenario's waarbij daadwerkelijk sprake is van zorginterventies moet bovendien goed nagedacht worden over de ethische inkadering hiervan.

6. Bijlage: Behulpzame vragenlijsten

Hieronder volgt een samenvatting in de vorm van een vragenlijst. Voorafgaand aan het werken met data moeten de volgende vragen beantwoord worden:

1. **Waarom worden er gegevens verwerkt?**
    - Wat is het doel/zijn de doelen om de gegevens te verwerken (delen)? Het doel is bepalend voor de vraag welke data noodzakelijk zijn om het doel/de doelen te bereiken.
2. **Waar komen de gegevens vandaan?**
    - Zijn de gegevens rechtmatig verkregen? (Bijvoorbeeld: scrapen van internet is niet altijd toegestaan en wil/mag je werken met een dataset die verkregen is via een hack en daarna online is gezet? Heeft degene van wie de data verkregen worden hiervoor toestemming (nodig) van de betrokkenen?)
    - Is de data betrouwbaar?
3. **Wie zijn er allemaal betrokken bij de verwerking van de gegevens?**
    - Wie hebben er allemaal toegang tot de data? Zijn er naast de partij die de data verstrekt nog andere partijen betrokken bij de verwerking (bijvoorbeeld: moeten alle betrokken onderzoekers toegang hebben tot de data of enkel diegenen die daadwerkelijk de data gaan verwerken? Wordt de data ergens door een externe partij gehost? Cloud provider?)
4. **Wat voor soort gegevens zitten er in de dataset?**
    - Juridisch is de categorie met de meeste impact **persoonsgegevens** omdat indien er sprake is van persoonsgegevens de Algemene Verordening Gegevensbescherming (AVG) van toepassing is.
    - Naast de AVG kan ook andere wetgeving relevant zijn zoals de WGBO, maar ook intellectuele eigendom: bedrijfsgeheimen, auteursrechten, portretrechten.
5. **Welke partijen hebben er rechten op de data in de dataset?**
    - Voor persoonsgegevens zijn dat bijvoorbeeld diegenen op wie de gegevens betrekking hebben, op foto's kan zowel degene die de foto gemaakt heeft als de persoon die op de foto staat rechten hebben. De een het portretrecht, de ander auteursrecht.
6. **Wie is er "eigenaar" van de dataset en wie wordt er "eigenaar" van de op basis van deze data te genereren nieuwe data?**
    - Juridisch spreken van "eigenaarschap van data" is problematisch, aangezien eigendom ziet op tastbare zaken en een absoluut recht is. Er wordt wel gesproken van data eigenaarschap, maar dat is dan enkel in deze zin: "Wie mag er op welke wijze over de data beschikken?"
7. **Wat zijn de risico's van de verwerking en hoe worden deze risico's gemitigeerd?**
    - Is er een inventarisatie gemaakt van de risico's die de verwerking van de data met zich meebrengt en zijn er technische en organisatorische maatregelen genomen om die risico's te mitigeren?
8. **Is het datamanagementplan (DMP) ingevuld (en met een data steward besproken)?**
    - Is er een datamanagementplan (DMP) ingevuld en, indien hiervan binnen de organisatie sprake is, is dit plan besproken met een data steward (persoon binnen kennisinstelling die aanspreekpunt is voor correcte omgang met data, vaak ook degene die op een daarvoor ingerichte Research Drive en/of Server een plek in kan richten specifiek bedoeld voor een bepaald project).
    - *Is er een verantwoordelijke binnen het project aangewezen die gedurende het project toezicht houdt op de naleving van het DMP en die zo nodig gedurende het project bijstuurt zodat de verwerking van data verantwoord en juridisch compliant is en blijft gedurende de looptijd van het project (en daarna indien data bewaard gaan worden)?*

Hieronder is een vragenlijst opgenomen die aanvullend is op de lijst hierboven. Deze tweede vragenlijst is relevant als er persoonsgegevens verwerkt worden en de AVG van toepassing is.

1. **Is de verwerking van persoonsgegevens noodzakelijk om het doel te bereiken?**
    - Ja, ga door naar punt 3.
    - Nee, verwerk deze gegevens dan niet! Ga door met punt 2.
2. **Kunnen de persoonsgegevens uit de dataset verwijderd worden? Of kunnen de data aan de bron geanonimiseerd worden?**
    - Verwijderen en/of anonimiseren zijn verwerkingen van persoonsgegevens, dus dit moet aan de bron/bij de verstrekker gebeuren.
    - Als de zorginstelling zelf niet weet hoe de data te anonimiseren, kan de kennisinstelling eventueel een script om de data te anonimiseren ter beschikking stellen aan de dataverstrekker.
3. **Als de persoonsgegevens niet aan de bron verwijderd kunnen worden en/of noodzakelijk zijn voor het onderzoek, dan worden persoonsgegevens verwerkt en is de AVG van toepassing. Wie zijn betrokkenen, (gezamenlijk) verwerkingsverantwoordelijke en verwerkers voor de verwerking van persoonsgegevens?**
    - Let op: indien er meer dan een doeleinde binnen het project is voor de verwerking van persoonsgegevens, dan moet per doeleinde worden vastgesteld wie (gezamenlijk) verwerkingsverantwoordelijke en, indien van toepassing, verwerker zijn. De omschrijving van de opdracht is hierbij bepalend.
    - Afhankelijk van de rollen die door de verschillende partijen in het project vervuld worden, moet een verwerkersovereenkomst en/of gezamenlijk verantwoordelijkenovereenkomst gesloten worden. Wanneer de kennisinstelling puur in opdracht van de zorgpartijen persoonsgegevens verwerkt zal sprake zijn van een verwerkersovereenkomst. Het zal echter vaker voorkomen dat in gezamenlijkheid met de zorgpartijen het doel en de middelen van de verwerking van de persoonsgegevens worden vastgesteld en er daarom een gezamenlijk verantwoordelijkenovereenkomst gesloten moet worden.
4. **Wat is de grondslag in de AVG op grond waarvan de (bijzondere categorieën) persoonsgegevens verwerkt mogen worden?**
    - Voor verwerking van persoonsgegevens in het kader van onderzoeksprojecten in de zorg kan voor een recthsgrond onder artikel 6 AVG het beste eerst gekeken worden naar de zorgovereenkomst of een wettelijke plicht. Als dat niet kan is mogelijk legitiem belang een optie:
    - de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is**.**
    - Indien bovenstaande rechtsgrondslagen geen uitkomst bieden zal toestemming van betrokkenen nodig zijn. Let hierbij op dat het gaat om specifieke, geïnformeerde, vrije en uitdrukkelijke toestemming voor de verwerking van persoonsgegevens ten behoeve van het doel/de doelen omschreven in het onderzoeksproject.
    - Voor een grondslag voor de verwerking van bijzondere categorieën van persoonsgegevens biedt mogelijk art. 9 (2) (h) verwerking noodzakelijk voor “medische diagnosen, het verstrekken van gezondheidszorg” of (i) “noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid” uitkomst. Indien niet noodzakelijk zal op basis van artikel 9 (2)(a) toestemming verkregen moeten worden voor de verwerking van de bijzondere categorieën van persoonsgegevens.

5. **Moet er een DPIA uitgevoerd worden?**
    - In principe moet er bij onderzoek met gezondheidsgegevens van patiënten uit zorginstellingen altijd een DPIA uitgevoerd worden. Er worden immers bijzondere persoonsgegevens verwerkt van een kwetsbare groep.
    - Ook wanneer het uitvoeren van een DPIA niet verplicht is, is het uitvoeren van een DPIA aan te raden vanuit een oogpunt van accountability.

6. **Wat voor technische en organisatorische maatregelen worden er binnen het onderzoek genomen om gegevensbeschermings- en privacyrisico's te verminderen?**
    - Pseudonimisering
    - Autorisatierollen
    - Federated learning
    - Multi Party Computation
    - Beleggen van rollen en verantwoordelijkheden bij specifieke personen binnen het project.