Bijlage 3: Vragenlijst

De vragenlijst helpt u om te beoordelen of u rekening heeft gehouden met diversen risico's. Ter ondersteuning van stap 4, 5 en 6 uit het DPIA Product. Op de volgende pagina is een tabel opgenomen met meer informatie over de herkomst van de vraag en een passende maatregel bij het ontdekte risico. Ook zijn de vragen daar ingedeeld op categorie. De volgende 26 vragen zijn van belang:

Vragenlijst

1. Is duidelijk wie verantwoordelijk is voor de verwerking van de gegevens?
2. Bestaat een grondslag voor de verwerking?
3. Worden er zo min mogelijk gegevens verzameld om het doel te bereiken?
4. Is het gebruik van de gegevens nodig voor het doel?
5. Worden de gegevens gebruikt voor andere bedrijfsprocessen of doelen dan waarvoor ze oorspronkelijk verzameld zijn?
6. Verwerkt u gegevens van kwetsbare groepen of personen?
7. Is de verwerking opgenomen in het verwerkingsregister?
8. Zijn er meerdere partijen betrokken bij de uitvoering van de verwerking?
9. Worden de gegevens verspreid buiten de organisatie?
10. Is het doorgeven van de gegevens aan partijen buiten de organisatie begrijpelijk voor het individu?
11. Worden gegevens uitgewisseld via een elektronisch uitwisselingssysteem?
12. Zijn er derden betrokken die als verwerker kwalificeren? Zo ja, is met die verwerker(s) een verwerkersovereenkomst afgesloten?
13. Meldt u de betrokkene dat de gegevens worden verzameld?
14. Kunnen de betrokkenen hun gegevens inzien/verbeteren/aanvullen/verwijderen of daarom vragen?
15. Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)?
16. Kan de manier waarop de gegevens worden verzameld worden opgevat als privacygevoelig?
17. Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig?
18. Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?
19. Worden de gegevens breed verspreid binnen de organisatie?
20. Is een bewaartermijn voor de gegevens vastgesteld?
21. Worden de gegevens na verstrijken van de bewaartermijn op zo'n manier vernietigd of verwijderd dat ze niet meer te benaderen en te gebruiken zijn?
22. Kunnen de gegevens na afloop van de bewaartermijn worden verwijderd (uit een bestand) of vernietigd (papier)?
23. Is sprake van intern geformuleerd beleid over het beveiligen van informatie?
24. Is duidelijk met welke maatregelen ervoor wordt gezorgd dat aan de gestelde eisen in het beveiligingsbeleid voldaan gaat worden?
25. Is een functionaris voor gegevensbescherming (FG) nodig en aangesteld?
26. Zijn maatregelen getroffen om datalekken op te nemen in een register en indien noodzakelijk te melden aan de Autoriteit persoonsgegevens en aan de getroffen personen van wie de gegevens zijn gelekt?

	Vraag	Extra informatie	Ja	Nee
		Beginselen		
1.	Is duidelijk wie verantwoordelijk is voor de verwerking van de gegevens?	Houd bij de beantwoording rekening met: - Of er iemand formeel verantwoordelijk is voor de verwerking van de gegevens. - Of er een interne contactpersoon is.		Als niet duidelijk is wie verantwoordelijk is en wie tot actie moet overgaan, kunnen risico's niet worden afgedekt. Wijs een verantwoordelijke aan.
2.	Bestaat een grondslag voor de verwerking?	De AVG noemt de volgende zes grondslagen: - Toestemming; - Noodzakelijk bij overeenkomst; - Wettelijk verplichting; - Vitale belangen; - Taak algemeen belang; - Noodzakelijk voor de gerechtvaardigde belangen van verantwoordelijke.		Zonder grondslag (reden om te verwerken) mag de verwerking niet plaatsvinden (art. 6 AVG). In de zorg zal het meestal gaan om de eerste drie grondslagen. De WGBO biedt veelal een (wettelijke) grondslag voor de verwerking. Toestemming is de restcategorie. Mocht u toch gebruik maken van toestemming zorg dat dit op correcte wijze gebeurt. Toestemming moet vrij, specifiek, geïnformeerd en een ondubbelzinnige wilsuiting zijn. Bovendien kan de toestemming altijd ingetrokken worden. Noteer voor elke verwerking de grondslag.
3.	Zijn alle gegevens nodig om het doel te bereiken (anders gezegd: worden er zo min mogelijk gegevens verzameld)? (Noodzaak)	Enkel de noodzakelijke gegevens mogen verzameld worden. Kijk bijvoorbeeld kritisch naar de wijze van rapporteren. Wordt er ook onnodige informatie genoteerd?		Hoe minder persoonsgegevens bewaard worden, des te minder er fout kan gaan. Bovendien loopt uw organisatie risico's als u te veel (onnodige) gegevens verzamelt (art. 5 AVG).
4.	Is het gebruik van de gegevens nodig voor het doel? (Doelbinding)	Houd bij de beantwoording rekening met: - Wat het verzameldoel is. - Waarvoor de gegevens worden gebruikt. - Welke gegevens worden verzameld. - Welke afdelingen/personen en andere partijen toegang hebben tot de gegevens.		Het gebruik van de gegevens moet in overeenstemming met het doel van de verwerking zijn (zie art. 5 AVG). Gegevens mogen niet zonder reden verzameld worden.
5.	Worden de gegevens gebruikt voor andere bedrijfsprocessen of doelen dan waarvoor ze oorspronkelijk verzameld zijn?	Denk bijvoorbeeld aan het toetsen van kwaliteit, nieuwsbrieven of doorgifte van gegevens aan derden zoals andere zorgaanbieders.	Beoordeel of het gebruik te rechtvaardigen is met het oorspronkelijke doel. Zo niet, dan is een eigen grondslag nodig. Meestal zal dat toestemming zijn.	
6.	Verwerkt u gegevens van kwetsbare groepen of personen?	Bijvoorbeeld patiënten, kinderen, verwarde personen of ouderen.	U loopt een verhoogd risico. U wordt geadviseerd maatregelen te treffen op een hoger beveiligingsniveau (art. 32 AVG). Gebruik hiervoor de NEN 7510, 7512, 7513. Ook moet extra kritisch gekeken worden of de verwerkingen mogen plaatsvinden (art. 9 AVG).	
7.	Is de verwerking opgenomen in het verwerkingsregister?	Alle verwerkingen moeten opgenomen worden in het verwerkingsregister.		Neem de verwerking op in het verwerkingsregister (art. 30 AVG).
		Samenwerking		
8.	Zijn er meerdere partijen betrokken bij de uitvoering van de verwerking?	Houd bij de beantwoording rekening met: - Andere zorgaanbieders; - Assistenten; - Ondersteunend personeel; - Zorgverzekeraars; - Gezamenlijke verwerkingsverantwoordelijke(n).	U loopt een verhoogd risico. Het risico bestaat dat niet alle partijen zorgvuldig met gegevens omgaan die tijdens het project worden verzameld. Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: - De beveiliging van gegevens; - Afhandeling van fouten; - Terugmelden van fouten; - Afstemming van beveiligingsbeleid; - Controle. Het is mogelijk dat u gezamenlijk verwerkingsverantwoordelijke bent. Indien dat het geval is moet u afspraken maken (art. 26 AVG)	

	Vraag	Extra informatie	Ja	Nee
9.	Worden de gegevens verspreid buiten de organisatie?	Houd bij de beantwoording rekening met: - Welke organisaties en personen toegang tot de gegevens hebben. - Hoe vaak (frequentie) de gegevens worden verstrekt. - Het medium dat gebruikt wordt voor verspreiding (bv. papier, CD-ROM, geheugenstick, e-mail, internet). - De maatregelen om ander gebruik te voorkomen. - De juiste grondslag voor het uitwisselen van gegevens.	U loopt een verhoogd risico. Hoe meer partijen betrokken zijn, hoe groter de kans op verlies van gegevens, onduidelijkheid in verantwoordelijkheden, het gebruik van de gegevens voor andere doelen en de kans op fouten. Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: - De beveiliging van gegevens en de afstemming daarvan tussen de partijen; - De gegevenskwaliteit; - Afhandeling van fouten; - Terugmelding van fouten; - Controle. Leg afspraken vast.	
10.	Is het doorgeven van de gegevens aan partijen buiten de organisatie begrijpelijk voor het individu?	Houd bij de beantwoording rekening met: - Wat individuen/patiënten verwachten - Of de betrokkene redelijkerwijs op de hoogte kan zijn van de verwerking van de gegevens. (privacyverklaring) - Of de betrokkenen toestemming geven om de gegevens te verzamelen. - Welke personen toegang hebben tot de gegevens. - Welke gegevens (data elementen) aan andere partijen worden verstrekt.		U loopt een verhoogd risico. Bij verstrekking van gegevens buiten de organisatie is het van belang dat de betrokkene hiervan op de hoogte is en dat maatregelen zijn getroffen om de gegevens te beschermen (art. 14 AVG).
11.	Worden gegevens uitgewisseld via een elektronisch uitwisselingssysteem?	Worden gegevens uitgewisseld via een elektronisch uitwisselingssysteem dan is de zorgaanbieder gehouden aan complexe regelgeving. Zo heeft de zorgaanbieder waarschijnlijk vooraf toestemming nodig van de patiënt.	U loopt een verhoogd risico. Indien gegevens uitgewisseld worden via een elektronisch uitwisselingssysteem moet u rekening houden met complexe wetgeving, waaronder het ''Besluit elektronische gegevensverwerking door zorgaanbieders'' en de ''Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg''.	
12.	Zijn er derden betrokken die als verwerker kwalificeren? Zo ja, is met die verwerker(s) een verwerkersovereenkomst afgesloten?	Zijn afspraken gemaakt: - Over de aansprakelijkheid; - Het informeren over datalekken; - Voldoen aan de verplichtingen.		Sluit een verwerkersovereenkomst af (art. 28 AVG).
	Rechten betrokkenen			
13.	Meldt u de betrokkene dat de gegevens worden verzameld?	Heeft u een privacyverklaring waarin duidelijk is opgenomen welke gegevens u waarom verzameld? In artikel 13 en 14 AVG staat welke onderwerpen opgenomen moeten worden in een privacyverklaring.		Stel een volledige privacyverklaring op en stel deze beschikbaar op uw website en op papier in de praktijk. De verklaring hoeft niet ondertekend te worden (art. 13 en 14 AVG).
14.	Kunnen de betrokkenen hun gegevens inzien/verbeteren/ aanvullen/verwijderen/beperken/ meenemen/bezwaar maken of daarom vragen.	De rechten van betrokkenen moeten gecommuniceerd worden met de betrokkenen. Technisch moet dit mogelijk zijn en er moet een duidelijke interne procedure zijn voor dergelijke verzoeken. De zorgaanbieder moet namelijk gehoor geven aan dergelijke verzoeken.		Betrokkenen hebben rechten. Hierbij is het van belang dat u zelf ook een helder overzicht heeft van de gegevens die worden verwerkt en waar deze zich binnen de organisatie bevinden (art. 15, 16, 17, 18, 19, 20, 21, 22, 23 AVG en art. 455, 456 WGBO).
	Beveiliging			
15.	Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)?	Pseudonimiseren is een beveiligingsmaatregel waarbij persoonsgegevens worden verwerkt zonder dat daarbij duidelijk wordt over welke personen de gegevens gaan. Bij pseudonimiseren van persoonsgegevens kunnen gegevens alleen nog herleidbaar zijn tot een specifiek persoon als er gebruik wordt gemaakt van aanvullende gegevens.	Door de gegevens te pseudonimiseren kunt u het nemen van verdere maatregelen ter bescherming van de privacy van de betrokkenen minimaliseren (art. 6, 25, 32 AVG).	

	Vraag	Extra informatie	Ja	Nee
		Geanonimiseerde gegevens zijn gegevens die helemaal geen betrekking meer hebben op individuen. Er mogen bij anonimisering dus géén aanvullende gegevens beschikbaar zijn waarmee iemand alsnog een koppeling kan maken met een specifiek persoon.	Door het gebruik van geanonimiseerde gegevens valt u niet meer onder het regime van de AVG. U verwerkt immers geen persoonsgegevens meer. U wordt geadviseerd periodiek na te gaan of de gegevens niet indirect herleidbaar zijn.	
16.	Kan de manier waarop de gegevens worden verzameld worden opgevat als privacygevoelig?	Bijvoorbeeld omdat intieme of gevoelige informatie wordt gevraagd in een publiek gebied waar anderen dit kunnen horen, of omdat gebruik gemaakt wordt van (camera)observatie of tracking door cookies of GPS?	U wordt geadviseerd na te gaan of de gegevens op een andere manier kunnen worden verzameld. Tevens moet u ervoor zorgen dat betrokkenen zich hiervan bewust zijn evenals de mensen die de gegevens verwerken. U moet de betrokkenen over deze verwerking goed informeren.	
17.	Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig?	Houd bij de beantwoording rekening met: - Of de gegevens worden gecontroleerd, op welke wijze en op welke aspecten de controle plaatsvindt. - Of de gegevens kunnen worden gecorrigeerd. - Welke personen toegang hebben tot de gegevens voor correctie, verwijderen et cetera van de gegevens. - Welke afdelingen toegang hebben tot de gegevens. - Hoe vaak de gegevens worden geüpdatet. - Wat de gevolgen zijn van het gebruiken van onjuiste gegevens. - Of maatregelen getroffen worden om ander gebruik dan het beoogde te voorkomen. - Of kwaliteitswaarborgen worden verstrekt bij verstrekking van de gegevens. - Wat er gebeurt als (delen van) de gegevens niet aan de andere partijen worden verstrekt.		Het is van belang dat de verwerkte gegevens juist zijn om ervoor te zorgen dat geen verkeerde conclusies worden getroffen of verkeerde acties worden ondernomen (art. 5 AVG). Zeker in de zorg moeten de gegevens actueel, juist en volledig zijn.
18.	Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?	Het gebruik van verschillende bronnen kan een aantal gevolgen hebben, houd rekening met: - Het incompleet zijn van dossiers of niet up-to-date zijn van dossiers; - Dubbelingen en zelfs tegenstrijdigheden; - De doelbinding.	U loopt een verhoogd risico dat de gegevens gebruikt worden of in de toekomst gebruikt gaan worden voor andere doeleinden dan waar zij oorspronkelijk voor zijn verzameld (function creep). U wordt geadviseerd maatregelen te treffen om deze zogenaamde function creep te voorkomen of onmogelijk te maken, bijvoorbeeld door het hanteren van strikte bewaartermijnen.	
19.	Worden de gegevens breed verspreid binnen de organisatie?	Houd bij de beantwoording rekening met: - Welke afdelingen toegang hebben tot de gegevens. - Welke personen toegang hebben tot de gegevens. - De doelen en het gebruik van de gegevens.	Het verspreiden van gegevens binnen de organisatie verhoogt het risico dat de gegevens voor zaken gebruikt worden waar ze niet voor bedoeld zijn of in handen komen van mensen die hier niet voor geautoriseerd zijn. Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: - De beveiliging van gegevens; - Afhandeling van fouten; - Terugmelding van fouten; - Afstemming van begeleidingsbeleid; - Controle.	
20.	Is een bewaartermijn voor de gegevens vastgesteld?	Houd hierbij rekening met het doel waarvoor de gegevens zijn verzameld en vervolgens worden verwerkt, bedrijfsrichtlijnen en wettelijk vastgestelde bewaartermijnen zoals bijvoorbeeld in de WGBO en belastingwetgeving.		U dient gegevens slechts zo lang te bewaren als nodig is voor het voldoen aan de doelstellingen. Dit zal in de zorg meestal een termijn van 15 jaar zijn (art. 5 AVG en art. 455 WGBO).

	Vraag	Extra informatie	Ja	Nee
21.	Kunnen de gegevens na afloop van de bewaartermijn worden verwijderd (uit een bestand) of vernietigd (papier)?	Het is niet voldoende om gegevens aan te merken als 'verlopen'; na het aflopen van de bewaartermijn dienen deze daadwerkelijk verwijderd te worden. Houd bij de beantwoording van de vraag rekening met: □ Of het mogelijk is (delen van) de gegevens te vernietigen of te verwijderen. □ Indien de gegevens worden vernietigd of verwijderd, of dit ongedaan kan worden gemaakt. □ Of de gegevens anoniem kunnen worden gemaakt om ze te bewaren.		U loopt een verhoogd risico. Indien gegevens oneindig bewaard worden wordt het risico dat deze gebruikt worden door ongeautoriseerde personen hoger. Eveneens brengt het kosten met zich mee om de gegevens te bewaren (en te onderhouden).
22.	Worden de gegevens na verstrijken van de bewaartermijn op zo'n manier vernietigd of verwijderd dat ze niet meer te benaderen en te gebruiken zijn?	Houd bij de beantwoording rekening met: □ Of regelgeving of beleid bestaat voor de vernietiging van gegevens (bijvoorbeeld de Archiefwet). □ Waar (welke locatie) de gegevens worden bewaard. □ Op welk medium (papier, CD, harde schijf) de gegevens worden bewaard. □ Of deze locatie/dit medium is afgeschermd voor gebruik (bijvoorbeeld het archief). □ Welke andere redenen bestaan om de gegevens te bewaren zoals bedrijfs- historische, wettelijke, juridische redenen.		Het zo kort mogelijk bewaren van gegevens heeft een aantal voordelen. • De benodigde opslag en rekencapaciteit van uw computersystemen is lager, waardoor prestaties, hersteltijden en service niveaus kunnen worden verhoogd. • U zult minder gegevens hoeven te onderhouden en updaten en de kans op fouten wordt verkleind. U wordt geadviseerd per gegevensdrager te bepalen op welke wijze de gegevens hierop vernietigd worden.
23.	Is sprake van intern geformuleerd beleid over het beveiligen van informatie?	Houd bij de beantwoording rekening met: □ Of iemand verantwoordelijk is voor dit beleid. □ Of wordt aangesloten bij algemene beveiligingsstandaarden (NEN 7510). □ Of rekening wordt gehouden met het bijzondere of gevoelige karakter van gegevens. □ Of het beveiligingsbeleid wordt getoetst.		Beveiligingsbeleid is noodzakelijk voor het maken van keuzes en het effectief en efficiënt nemen van maatregelen die de gegevens beveiligen. Voor zorgaanbieders met een zorginformatiesysteem is het verplicht om te voldoen aan de NEN 7510 en NEN 7512.
24.	Is duidelijk met welke maatregelen ervoor wordt gezorgd dat aan de gestelde eisen in het beveiligingsbeleid voldaan gaat worden?	Denk hierbij aan welke maatregelen getroffen worden om te voldoen aan het beschreven beleid (een informatiebeveiligingsplan).		U wordt geadviseerd een informatiebeveiligingsplan op te stellen met daarin maatregelen die voor een passende bescherming van de gegevens zorgen.
25.	Is een functionaris voor gegevensbescherming (FG) nodig en aangesteld?	Zo niet beoordeel of de nieuwe verwerking dit noodzakelijk maakt.		Een FG is onder andere nodig indien grootschalig bijzondere persoonsgegevens worden verwerkt. In de zorg is dat doorgaans het geval als van meer dan 10.000 betrokken (patiënten/cliënten) gegevens verzameld worden (art. 37 AVG).
		Datalekken		
26.	Zijn maatregelen getroffen om datalekken op te nemen in een register en indien noodzakelijk te melden aan de Autoriteit persoonsgegevens en aan de getroffen personen van wie de gegevens zijn gelekt?	In de AVG is een meldplicht opgenomen voor datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken onder bepaalde voorwaarden moeten melden aan de Autoriteit persoonsgegevens en in bepaalde gevallen ook aan de betrokkene. De betrokkene is degene van wie persoonsgegevens zijn gelekt. Elk datalek moet opgenomen worden in een intern datalekken register.		Maatregelen zijn noodzakelijk om gestructureerd en adequaat invulling te geven aan de wettelijke meldplicht van datalekken. Medewerkers moeten bekend zijn met de plicht. Iemand moet verantwoordelijk zijn en een intern meldprotocol is raadzaam. U wordt geadviseerd alsnog maatregelen te treffen (art. 33 en 34).