Shared Service Center
Data Governance

Handreiking Toetsing naar aanleiding van wetswijziging Wkkgz

Voor registratiehouders van kwaliteitsregistraties

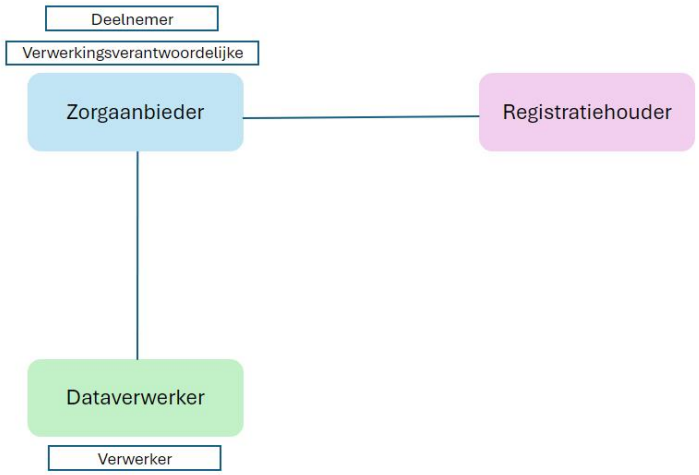
SSC-DG – versie 1.1
20-6-2024

Inhoudsopgave

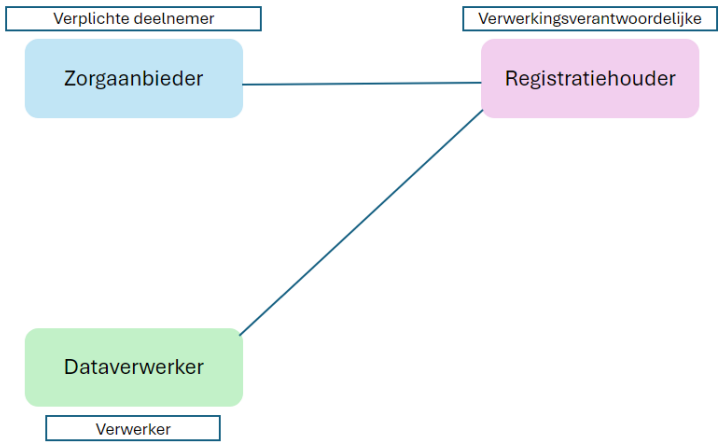
1 Introductie

Wettelijke eisen aan registratiehouders veranderen na wijziging Wkkgz

Zodra de wetswijziging Wet kwaliteit, klachten en geschillen zorg (Wkkgz) in werking treedt, veranderen de rollen en verantwoordelijkheden bij het ontvangen en verwerken van gegevens voor kwaliteitsregistraties (zie figuur 1a en 1b voor het verschil in rollen vóór en na de inwerkingtreding). Registratiehouders en dataverwerkers krijgen hierdoor te maken met andere wettelijke eisen.



Figuur 1a: Rollen vóór de inwerkingtreding van de wet[1]



Figuur 1b: Rollen na de inwerkingtreding van de wet[2] (voor registraties opgenomen in het register)

[1] Het huidige kwaliteitsregistratielandschap vertoont veel verschillen in governancestructuren. De getoonde afbeelding is de meest voorkomende variant op dit moment.
[2] De nieuwe Wkkgz regelt dat de registratiehouder verwerkingsverantwoordelijke is voor de kwaliteitsregistratie en dat de zorgaanbieder een aanleverplicht heeft. Het is voor een registratiehouder niet verplicht om gebruik te maken van een dataverwerker. Het zou dus kunnen dat de registratiehouder ook als verwerker optreedt.

Om in het register voor kwaliteitsregistraties van Zorginstituut Nederland opgenomen te kunnen worden, moeten registratiehouders aantonen dat zij en hun dataverwerker(s) aan de nieuwe wettelijke eisen van de Wkkgz voldoen.

Voordat registratiehouders een aanvraag kunnen indienen bij Zorginstituut Nederland, worden zij getoetst door de IGC en DGC aan de hand van toetsingscriteria. Daar waar de wettelijke eisen veranderen ten opzichte van de huidige situatie, wijzigen ook de toetsingscriteria in lijn met deze veranderingen. Het gaat hierbij om de **DGC-criteria 6 (6.1), 8 (8.1 t/m 8.4) en 9 (9.1 t/m 9.4)**.

Scenario's toetsing DGC na wetswijziging

Omdat de eerder genoemde toetsingscriteria van de DGC in lijn met de wetswijziging aangepast worden, en Zorginstituut Nederland kwaliteitsregistraties op basis van de nieuwe wettelijke eisen opneemt in het register, zullen de kwaliteitsregistraties op deze nieuwe criteria moeten worden getoetst. Daarvoor zijn verschillende scenario's mogelijk:

- Registratiehouders die na de invoering van de wetswijziging een aanvraag tot toetsing doen, dienen direct (gedurende de reguliere toetsing) te laten zien dat zij aan de nieuwe eisen voldoen.
- Voor kwaliteitsregistraties waarbij de wet tijdens de toetsing wijzigt, zullen de benodigde aanvullende bewijsstukken tijdens de reguliere toetsing worden opgevraagd bij de registratiehouder.
- Registratiehouders die al een advies van de DGC hebben ontvangen voordat de wet in werking treedt, moeten aanvullend worden getoetst op de gewijzigde criteria. Zij hoeven dus niet het volledige toetsingsproces opnieuw te doorlopen, maar worden alleen getoetst op de wijzigingen. Hoofdstuk 6 gaat hier uitgebreider op in.

Voorbereiding op de wijzigingen en de toetsing

Het SSC-DG heeft deze handreiking opgesteld zodat registratiehouders en hun dataverwerker(s) zich kunnen voorbereiden op de wijzigingen in de toetsingscriteria als gevolg van de inwerkingtreding van de gewijzigde Wkkgz en de (aanvullende) toetsing door de DGC. Dit document is een uitgebreide aanvulling op het document Toetsingscriteria DGC, waarin de wijzigingen na ingang van de Wkkgz ook staan beschreven.

Leeswijzer

In hoofdstuk 2, 3 en 4 wordt voor de DGC-criteria 6 (6.1), 8 (8.1 t/m 8.4) en 9 (9.2 t/m 9.4) beschreven welke wijzigingen er zijn en welke voorbereidingen registratiehouders en dataverwerkers kunnen treffen. Hoofdstuk 5 beschrijft per criterium wat er wordt getoetst door de DGC. Registratiehouders die al een advies van de DGC hebben ontvangen, vinden in hoofdstuk 6 meer informatie over de aanvullende toetsing.

FAQ interpretatie wetswijziging Wkkgz

Op deze FAQ-pagina vindt u de antwoorden op enkele vragen die het veld heeft gesteld over de interpretatie van de Wkkgz na wetswijziging, onder andere op het gebied van pseudonimisatie. De antwoorden zijn in samenwerking met VWS geformuleerd.

2 Wijzigingen criterium 6 Pseudonimisatie

Het uitgangspunt van de criteria van de IGC en DGC is dat deze toetsbaar moeten zijn voor de elementen waar registratiehouders en dataverwerkers invloed op hebben en/of verantwoordelijk voor zijn. In de gewijzigde Wkkgz ligt de verantwoordelijkheid voor de pseudonimisatie van direct identificeerbare gegevens bij de zorgaanbieders. Registratiehouders en dataverwerkers moeten kunnen aantonen dat zij werken op basis van gepseudonimiseerde gegevens.

Met Zorginstituut Nederland en het ministerie van VWS wordt momenteel nog afgestemd wat er bij registratiehouders en dataverwerkers vastgesteld moet worden ten aanzien van de wettelijk vereiste inrichting op dit onderwerp. Zodra hier duidelijkheid over bestaat, wordt de vernieuwde inhoud van criterium 6 gepubliceerd. Daarna wordt dit hoofdstuk aangepast.

NB: Meer informatie over pseudonimiseren en een diepgaande interpretatie van de wet- en regelgeving over dit onderwerp vindt u op de projectpagina Pseudonimiseren en in de handreiking Pseudonimisatie.

2.1 Criterium 6.1 Gebruik pseudoniemen en toegepaste methode

Wat wijzigt er?
Artikel 11o lid 2 van de gewijzigde Wkkgz bepaalt dat *de registratiehouder, of een onder diens verantwoordelijkheid werkzame verwerker, slechts persoonsgegevens mag verwerken als daarop pseudonimisering is toegepast en vervolgens ten aanzien van deze verwerkingen onafgebroken is gecontinueerd.*

Uitgevraagde persoonsgegevens dienen door de zorgaanbieder gepseudonimiseerd aangeleverd te worden aan de registratiehouders, voor de kwaliteitsregistraties waarvoor een wettelijke aanleverplicht bestaat op basis van opname in het register van Zorginstituut Nederland. Voor registratiehouders en dataverwerkers heeft deze wijziging mogelijk impact op de verwerking van de aangeleverde (en bestaande) data, bestaande koppelingen tussen datastromen en validaties.

Voortschrijdend inzicht leidt tot aanpassingen van de te toetsen elementen in criterium 6.1. Deze aanpassingen zullen zo spoedig mogelijk gepubliceerd worden en na vaststelling ook in dit hoofdstuk beschreven worden.

Wat kunt u doen?
Het is op dit moment nog niet duidelijk waarop exact getoetst gaat worden. Desalniettemin kan de registratiehouder, in samenwerking met haar dataverwerker, ervoor zorgen dat er gepseudonimiseerde databestanden verwerkt kunnen worden en dat de organisatie-inrichting voldoet aan de wet- en regelgeving over de verwerking van gepseudonimiseerde gegevens.

Organisatorische vereisten:
- De registratiehouder heeft beleid waarin staat dat activiteiten in het kader van re-identificatie van de gepseudonimiseerde gegevens door medewerkers zijn verboden.
- De registratiehouder heeft beleid waarin de procedures zijn vastgelegd die bij datalekken gevolgd moeten worden, bijvoorbeeld wanneer er bestanden zijn ontvangen met daarin toch (identificeerbare) persoonsgegevens.

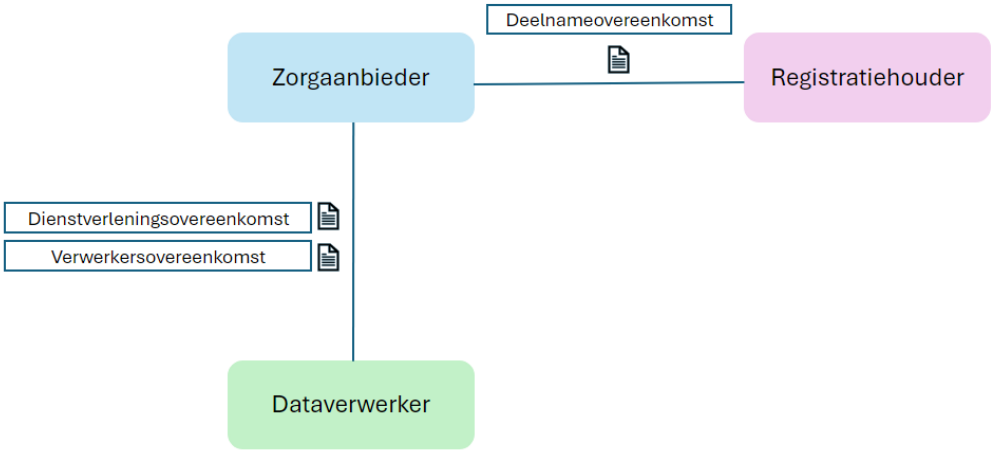
- In de databestanden (data dictionairy) staat duidelijk aangegeven welke direct identificerende persoonsgegevens uitgevraagd worden en welke direct identificerende persoonsgegevens gepseudonimiseerd aangeleverd moeten worden.
- De uitvraag van de (identificerende) persoonsgegevens heeft een onderbouwing, risico-afweging en gepaste (beveiligings)maatregelen in de DPIA.

Aanvullend benoemen we graag enkele aandachtspunten voor de dagelijkse processen bij de registratiehouder en dataverwerker:

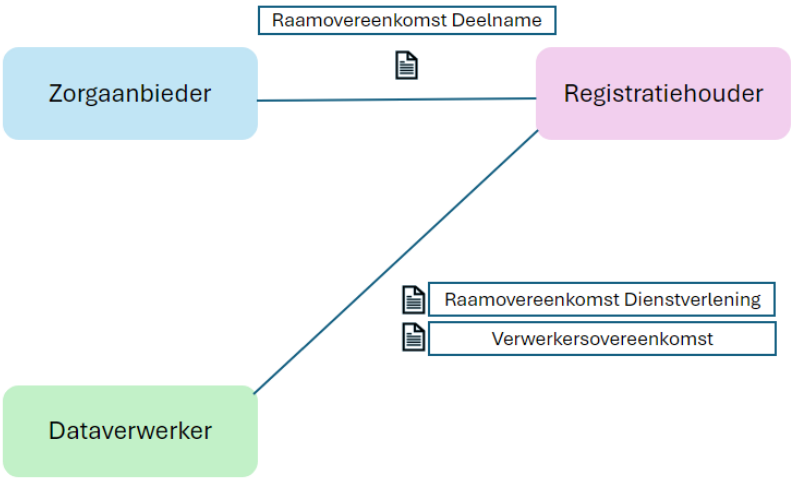
- Zorg ervoor dat de databestanden en -processen ingericht zijn ten behoeve van werken met pseudoniemen.
- Valideer aangeleverde bestanden op het voldoen aan de wettelijke eisen voor pseudonimiseren en relateer een negatieve uitkomst van een validatie aan het beleid voor datalekken.
- Zorg ervoor dat geen trendbreuk optreedt in de koppelbaarheid van data-records verzameld voor en na ingang van de Wkkgz-wijziging.

3 Wijzigingen criterium 8 Overeenkomsten

Criterium 8 van de DGC ziet toe op de benodigde afspraken die tussen zorgaanbieders, registratiehouders en dataverwerkers moeten worden gemaakt. Zoals in hoofdstuk 1 staat beschreven, veranderen de rollen en verantwoordelijkheden van partijen na de Wkkgz-wetswijziging. Deze verschuiving betekent ook dat de overeenkomsten tussen deze partijen aangepast moeten worden. Figuur 2a toont de overeenkomsten vóór inwerkingtreding van de wet en figuur 2b toont de overeenkomsten na inwerkingtreding van de wet.



Figuur 2a: Overeenkomsten vóór inwerkingtreding van de wet[3]



Figuur 2b: Overeenkomsten na inwerkingtreding van de wet

[3] Momenteel bestaan er veel verschillende governancestructuren voor kwaliteitsregistraties. Dat betekent dat er op dit moment ook veel verschillende overeenkomststructuren voor kwaliteitsregistraties bestaan. Figuur 2a toont een structuur die nu veel wordt gebruikt.

3.1 Standaardovereenkomsten

Samen met zorgaanbieders (NFU en NVZ), registratiehouders (SKR) en dataverwerkers (SDV) heeft de DGC drie standaardovereenkomsten opgesteld (zie ook figuur 2b):

- **Raamovereenkomst voor deelname**. Deze overeenkomst wordt gesloten tussen de zorgaanbieder en de registratiehouder en regelt de (verplichte) deelname aan de kwaliteitsregistratie. Deze overeenkomst kent vier bijlagen: de primaire dienstenbeschrijving, de gegevensuitwisselingsovereenkomst, de nadere deelnameovereenkomst(en) en (optioneel) een overeenkomst indien zorgaanbieder secundaire diensten wenst af te nemen bij de registratiehouder.
- **Raamovereenkomst voor dienstverlening**. Deze overeenkomst wordt gesloten tussen de registratiehouder en dataverwerker en regelt het generieke afsprakenkader voor de afgenomen diensten. Deze overeenkomst vormt één geheel met de bijbehorende verwerkersovereenkomst, inclusief alle bijlagen (zoals de nadere overeenkomst(en) en een Service Level Agreement).
- **Verwerkersovereenkomst**. Deze overeenkomst wordt gesloten tussen de registratiehouder en dataverwerker en regelt afspraken met betrekking tot de verwerking van persoonsgegevens. Het vormt één geheel met de raamovereenkomst voor dienstverlening.

De standaardovereenkomsten voldoen aan de eisen uit de toekomstige Wkkgz en bijbehorende ministeriële regeling. Door het gebruik van deze standaarden zullen de administratieve lasten bij de partijen afnemen. De DGC gaat ervan uit dat partijen gebruikmaken van deze standaardovereenkomsten en dit tijdens de toetsing kunnen laten zien. Omdat het over standaardovereenkomsten gaat, zijn deze in beginsel onveranderlijk en wordt bij voorkeur de gehele tekst van de overeenkomst gehandhaafd. Toch kunnen partijen, mits zij het hierover eens worden en dit noodzakelijk is, bepaalde onderdelen wijzigen door middel van een aparte bijlage (zie hiervoor de handleiding behorend bij de overeenkomst).

Beheer

In opdracht van de DGC beheert het SSC-DG deze standaardovereenkomsten. Het SSC-DG coördineert eventuele wijzigingen voor aanpassingen en/of verbeteringen van de overeenkomsten. Partijen kunnen bij het SSC-DG met hun vragen en/of opmerkingen over de overeenkomsten terecht. Voor het gebruik van de standaardovereenkomsten zijn handleidingen opgesteld. Hierin staan de artikelen, gebruiksinstructies en definities toegelicht, wordt aangegeven welke aanpassingen wel en niet toegestaan zijn en staat een schematisch uitgewerkt werkproces. De standaardovereenkomsten en handleidingen zijn beschikbaar op de website van het SSC-DG.

Naamgeving in document toetsingscriteria

Let op! In het huidige DGC-criteriadocument (v1.2) hebben de standaardovereenkomsten een andere naam:

- Raamovereenkomst voor deelname wordt in DGC-criteriadocument (v1.2) nog Dienstverleningsovereenkomst genoemd.
- Raamovereenkomst voor dienstverlening wordt in DGC-criteriadocument (v1.2) nog Hoofdovereenkomst genoemd.

De DGC heeft de naamgeving aangepast op advies van de werkgroep voor standaardovereenkomsten. De strekking van de overeenkomsten is niet veranderd. De namen in het criteriadocument worden nog aangepast.

3.2 Toetsingscriteria

De DGC stelt minimumeisen aan de overeenkomsten die voor kwaliteitsregistraties worden gebruikt. In het DGC-criteriadocument staan deze eisen beschreven voor zowel de huidige situatie als de situatie na de Wkkgz-wijziging. Hieronder vindt u een toelichting gegeven van de veranderingen per criterium en leest u wat er van betrokken partijen wordt verwacht.

3.2.1 Criterium 8.1 Deelnameovereenkomst én criterium 8.4 Raamovereenkomst voor deelname

Wanneer een zorgaanbieder wil deelnemen aan een kwaliteitsregistratie, wordt doorgaans een deelnameovereenkomst[4] gesloten met de registratiehouder. Hierin leggen partijen afspraken vast over (onder andere) de doeleinden en financiering van de kwaliteitsregistratie en de wijze van data-aanlevering en -terugkoppeling.

Wat wijzigt er?

Op dit moment is deelname aan een kwaliteitsregistratie voor zorgaanbieders nog optioneel. Na de Wkkgz-wijziging is deelname aan een kwaliteitsregistratie voor zorgaanbieders verplicht als de kwaliteitsregistratie is opgenomen in het register voor kwaliteitsregistraties en de zorgaanbieder op grond van de Wkkgz gegevens voor de kwaliteitsregistratie moet verstrekken.

Criterium 8.1 (vrijwillige) Deelnameovereenkomst vervalt en wordt vervangen door criterium 8.4 Raamovereenkomst voor (verplichte) deelname. De strekking van de deelnameovereenkomst verandert niet, maar de rechten en verplichtingen van partijen veranderen door inwerkingtreding van de gewijzigde Wkkgz wel. Dit komt dus (onder andere) doordat registratiehouders verwerkingsverantwoordelijk worden voor de kwaliteitsregistraties en doordat zorgaanbieders een aanleverplicht krijgen.

Wat kunt u doen?

Van registratiehouders wordt verwacht dat zij een Raamovereenkomst voor deelname afsluiten met alle zorgaanbieders die binnen de gewijzigde Wkkgz verplicht zijn gegevens te verstrekken voor de betreffende kwaliteitsregistratie(s). Geadviseerd wordt dat registratiehouders reeds vóór opname in het register voor kwaliteitsregistraties beginnen met het afsluiten van de raamovereenkomsten voor deelname. Hierin is bepaald dat (na ondertekening van partijen) de overeenkomst ingaat op het moment dat de kwaliteitsregistratie wordt ingeschreven in het register voor kwaliteitsregistraties.

3.2.2 Criterium 8.2 Verwerkersovereenkomst

Wanneer een dataverwerker (bepaalde delen van) de gegevensverwerking uitvoert voor de verwerkingsverantwoordelijke, is een verwerkersovereenkomst verplicht (volgens artikel 28 lid 3 AVG). Hierin leggen partijen hun wederzijdse rechten en verplichtingen vast met betrekking tot de verwerking van persoonsgegevens. Criterium 8.2 toetst deze verwerkersovereenkomst. Momenteel wordt de verwerkersovereenkomst meestal afgesloten tussen de zorgaanbieders (huidige verwerkersverantwoordelijke) en de verwerker(s).

[4] Door de verschillende governance- en overeenkomststructuren kunnen de onderwerpen uit de deelnameovereenkomst ook in (een) andere overeenkomst(en) zijn geregeld. Hier wordt bij de toetsing rekening mee gehouden.

Wat wijzigt er?
Na de Wkkgz-wetswijziging is de registratiehouder verwerkingsverantwoordelijk voor een in het register voor kwaliteitsregistraties opgenomen kwaliteitsregistratie. De verwerkersovereenkomst moet dan worden afgesloten tussen registratiehouder en dataverwerker.

Wat kunt u doen?
Van registratiehouders wordt verwacht dat zij (indien zij gebruikmaken van een dataverwerker) een verwerkersovereenkomst met hun dataverwerker(s) hebben afgesloten vóór opname in het register voor kwaliteitsregistraties. Partijen worden geacht gebruik te maken van de standaardovereenkomst Verwerkersovereenkomst. Hierin is bepaald dat (na ondertekening van partijen) de verwerkersovereenkomst ingaat op het moment dat de kwaliteitsregistratie wordt ingeschreven in het register voor kwaliteitsregistraties.

3.2.3 Criterium 8.3 Raamovereenkomst voor dienstverlening

Wanneer een dataverwerker (bepaalde delen van) de gegevensverwerking uitvoert voor de verwerkingsverantwoordelijke, sluiten partijen naast de verwerkersovereenkomst vaak ook een dienstverleningsovereenkomst af. De dienstverlenings- en verwerkersovereenkomst vormen samen vaak één overeenkomst. Waar de verwerkersovereenkomst toeziet op verwerkingen van persoonsgegevens, ziet de dienstverleningsovereenkomst toe op méér dan dat. Het ‘dienstverleningsgedeelte’ regelt de algemene rechten en verplichtingen van partijen zoals bijvoorbeeld de te leveren diensten, de vergoeding en betaling en het intellectueel eigendom.

Momenteel wordt de dienstverleningsovereenkomst niet getoetst omdat deze overeenkomst niet wettelijk verplicht is en door de DGC niet noodzakelijk wordt geacht voor een registratiehouder. De overeenkomst zal nu namelijk (meestal) gesloten zijn tussen zorgaanbieder en verwerker.

Wat wijzigt er?
Na de Wkkgz-wetswijziging is de registratiehouder verwerkingsverantwoordelijk voor een in het register voor kwaliteitsregistraties opgenomen kwaliteitsregistratie. Dit betekent dat de registratiehouder afspraken maakt met de dataverwerker over de te leveren diensten voor de kwaliteitsregistratie. Criterium 8.3 ziet op de toetsing van de Raamovereenkomst voor dienstverlening.

Wat kunt u doen?
Registratiehouders worden geacht (indien zij gebruikmaken van een dataverwerker) de raamovereenkomst voor dienstverlening met hun verwerker(s) te hebben afgesloten vóór opname in het register voor kwaliteitsregistraties. Partijen worden geacht gebruik te maken van de standaardovereenkomst Raamovereenkomst voor dienstverlening. Hierin is bepaald dat (na ondertekening van partijen) de raamovereenkomst voor dienstverlening ingaat op het moment dat de kwaliteitsregistratie wordt ingeschreven in het register voor kwaliteitsregistraties.

4 Wijzigingen criterium 9 Compliance

Na de inwerkingtreding van de gewijzigde Wkkgz wordt de registratiehouder van de kwaliteitsregistratie verwerkingsverantwoordelijke voor een in het register opgenomen kwaliteitsregistratie. Omdat er ten behoeve van kwaliteitsregistraties persoonsgegevens worden verwerkt, is de AVG ook van toepassing op de registratiehouder. Deze verandering heeft invloed op criterium 9 (9.1 t/m 9.4).

4.1 Criterium 9.1 Beveiliging van de dataverwerking

Wat wijzigt er?
Op basis van artikel 32 lid 1 van de AVG dienen de verwerkingsverantwoordelijke en verwerker passende technische en organisatorische maatregelen te treffen.

> **Artikel 32 lid 1 AVG (Beveiliging van de verwerking) stelt:**
> *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 bevatten...*

Doordat een registratiehouder onder de gewijzigde Wkkgz verwerkingsverantwoordelijke wordt, wordt artikel 32 lid 1 van de AVG ook van toepassing op die registratiehouder. Dit betekent dat de registratiehouder moet aantonen dat het beveiligingsniveau van de verwerking die onder haar verantwoordelijkheid uitgevoerd wordt, voldoet aan de eisen van artikel 32 lid 1 AVG.

Voor de verwerker heeft deze wetswijziging met betrekking tot het voldoen aan artikel 32 lid 1 AVG nauwelijks tot geen impact. Van verwerkers werd (door de verwerkingsverantwoordelijke zorgaanbieders) al een aantoonbaar beveiligingsniveau geëist, veelal door het kunnen overleggen van een informatiebeveiligingsbeleid en externe toetsing en certificering van de informatiebeveiligingsnormen NEN7510 en/of ISO27001.

Wat kunt u doen?
Om te bepalen wat ‘passende technische en organisatorische maatregelen’ voor een registratiehouder zijn, dient een DPIA uitgevoerd te worden (zie criterium 9.2). Een DPIA is een instrument om vooraf de privacyrisico’s van een gegevensverwerking in kaart te brengen, zodat technische en organisatorische maatregelen getroffen kunnen worden om deze risico’s te verkleinen. De DPIA brengt ook in kaart welke risico’s wáár (bij registratiehouder en/of verwerker) gelopen worden en wie (registratiehouder en/of verwerker) welke technische en organisatorisch maatregelen moet treffen om een op die risico’s afgestemd beveiligingsniveau te waarborgen.

Deze risico-gebaseerde aanpak zal ertoe leiden dat de registratiehouder die alleen doel- en middelen bepaalt en uitsluitend geanonimiseerde gegevens ontvangt nauwelijks of geen extra technische en/of organisatorische maatregelen hoeft te treffen om aan de toetsingscriteria te kunnen voldoen, terwijl de registratiehouder die zelf wél persoonsgegevens verwerkt (analyseert) mogelijk aanvullende technische en/of organisatorische maatregelen moet treffen om aan de toetsing te voldoen. De benodigde maatregelen zullen uit de DPIA naar voren komen. Ter voorbereiding op de

nieuwe wetgeving kunt u deze maatregelen treffen en documenteren (en gebruiken als bewijsstukken voor de toetsing).

4.2 Criterium 9.2 Er is een DPIA uitgevoerd

Wat wijzigt er?
Tot aan de inwerkingtreding van de gewijzigde Wkkgz is de deelnemende zorgorganisatie verwerkingsverantwoordelijke en dus ook verantwoordelijk voor het uitvoeren van een DPIA. Tot aan de inwerkingtreding betreft het toetsingscriterium daarom uitsluitend dat deel van de DPIA dat uitgevoerd wordt bij de verwerker.

Omdat na de inwerkingtreding van de gewijzigde Wkkgz de registratiehouder verwerkingsverantwoordelijke wordt, moet de registratiehouder, op basis van artikel 35 lid 1 AVG, een gegevensbeschermingseffectbeoordeling (ofwel DPIA) uit gaan voeren.

Voor de verwerker heeft deze wetswijziging met betrekking tot het voldoen aan artikel 35 lid 1 AVG nauwelijks tot geen impact. Van verwerkers werd namelijk al een DPIA geëist, maar de verwerker levert deze na ingang van de wetswijziging aan de registratiehouder (in plaats van aan de zorgaanbieder).

> **Artikel 35 lid 1 AVG (Gegevensbeschermingseffectbeoordeling) stelt:**
> *Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.*
>
> **Bij ministeriële regeling (in concept) is deze voorwaarde nader uitgewerkt (artikel 7ad):**
> *Een kwaliteitsregistratie moet op grond van artikel 11o, eerste lid, onderdeel g, van de Wkkgz een DPIA opstellen. Indien dit ingevolge de Algemene verordening gegevensbescherming verplicht is, moet de AP over deze DPIA worden geraadpleegd. Met deze regeling wordt daarnaast voor alle kwaliteitsregistraties een onafhankelijk oordeel over de DPIA verplicht gesteld. Op deze manier wordt voorkomen dat het Zorginstituut inhoudelijk moet toetsen of de registratiehouder zich conformeert aan de AVG. De onafhankelijke toets mag bij het indienen van de aanvraag niet ouder zijn dan 1 jaar.*

Hiermee ontstaat voor de registratiehouder de verplichting om een DPIA uit te voeren. Die verplichting betreft de totale verwerking; dus ook het deel van de verwerking dat bij de verwerker plaatsvindt, valt onder de verantwoordelijkheid van de registratiehouder.

De impact van deze verantwoordelijkheid op de extra inspanningen die de registratiehouder nog moet doen om aan deze eis te voldoen, is afhankelijk van de mate van gegevensverwerking die de registratiehouder zelf uitvoert:

- Wanneer de registratiehouder de volledige verwerking uitbesteedt aan haar verwerker, is de impact van deze eis klein. De DPIA van de verwerker omvat dan al het overgrote deel van de omschrijvingen van de met de verwerking gepaard gaande privacyrisico's en de genomen maatregelen om die risico's te mitigeren. De registratiehouder kan dan met beperkte aanvullingen/aanpassingen de door de verwerker opgestelde DPIA aanvullen.

- Wanneer een registratiehouder na de inwerkingtreding van de gewijzigde Wkkgz besluit om bijvoorbeeld (een deel van de) analyses zelf uit te gaan voeren op gepseudonimiseerde data, dan moeten ook de privacyrisico's (zoals de informatiebeveiliging bij de registratiehouder) in kaart worden gebracht en de mitigerende maatregelen worden geïmplementeerd.

Ook wanneer de registratiehouder de volledige verwerkingen uitbesteedt aan de verwerker, heeft de registratiehouder de verantwoordelijkheid voor de DPIA en dient zij samen met de DPIA van de verwerker tot één DPIA te komen die het gehele gegevensverwerkingsproces omvat. Onderdelen die typisch de verantwoordelijkheid zijn van de verwerkingsverantwoordelijke zijn bijvoorbeeld de beschrijving van de gegevensverwerking en de rechtmatigheidsbeoordeling[5].

Wat kunt u doen?

1. Stel een DPIA op

Al voor de inwerkingtreding van de gewijzigde Wkkgz kunnen registratiehouders samen met hun verwerkers nadenken over hoe de gegevensverwerking er straks uit komt te zien. De DGC heeft in samenwerking met de SKR, SDV, NFU en NVZ en in afstemming met Zorginstituut Nederland de wettelijke vereisten aan een DPIA vertaald naar een gestandaardiseerd DPIA-format. Dit format is beschikbaar op website van het SSC-DG. Met behulp van dit format en advies van de functionaris gegevensbescherming kan de DPIA vervolgens gecompleteerd worden en kan aan de geïdentificeerde mitigerende maatregelen worden gewerkt.

Voorbeeld: Als de registratiehouder zelf analyses gaat uitvoeren op een eigen dataplatform, dan dienen de daarmee gepaard gaande risico's en de op die risico's afgestemde maatregelen beschreven en geïmplementeerd te worden. De beschrijvingen van de ingevoerde maatregelen zijn bewijsstukken in de toetsing (zie ook paragraaf 4.1).

De vereisten aan de DPIA staan beschreven in criterium 9.2 van de DGC.

2. Richt een continu herzieningsproces in

De DGC raadt registratiehouders tevens aan om een proces in te richten om de DPIA regelmatig te herzien, zodat zij blijvend voldoen aan de wet- en regelgeving. De DGC toetst dit proces (nog) niet, maar beschrijft hieronder de wettelijke eisen die aan het onderhoud van de DPIA worden gesteld.

Artikel 35 lid 1 AVG bepaalt dat de verwerkingsverantwoordelijk de DPIA vóór de verwerking dient uit te voeren. Een DPIA uitvoeren is geen eenmalige opdracht, maar een continu proces. De verwerkingsverantwoordelijke zal altijd moeten (blijven) monitoren of de gegevensverwerking wijzigt en of de DPIA daarom bijgesteld moet worden.

Veranderingen die aanleiding kunnen geven om een toetsing op de DPIA uit te voeren zijn:

- *Veranderingen in gegevensverwerking*
  Bijvoorbeeld als een nieuwe technologie wordt gebruikt of als persoonsgegevens voor een ander doel worden gebruikt. In deze situaties verandert de gegevensverwerking feitelijk in een nieuwe gegevensverwerking.
- *Veranderingen in de risico's van de verwerking*
  Risico's kunnen bijvoorbeeld veranderen omdat een onderdeel van het verwerkingsproces

[5] Zie bijvoorbeeld het NOREA DPIA Raamwerk.

wijzigt. De technologische ontwikkelingen gaan snel, waardoor nieuwe kwetsbaarheden kunnen ontstaan.

- *Veranderingen in de context van de verwerking*
  Het kan nodig zijn de DPIA opnieuw uit te voeren omdat de organisatiecontext of maatschappelijke context verandert. Bijvoorbeeld omdat de gevolgen van bepaalde geautomatiseerde beslissingen belangrijker zijn geworden of omdat nieuwe categorieën betrokkenen kwetsbaar worden voor discriminatie.

De AP adviseert om sowieso periodiek een DPIA uit te voeren, ook als de gegevensverwerking zelf niet is veranderd; zij noemt als voorbeeld een frequentie van ééns in de drie jaar. Ook de AVG-Helpdesk voor Zorg, Welzijn en Sport adviseert om de DPIA ten minste elke drie jaar te evalueren.

Inbreuken op de verplichtingen van de verwerkingsverantwoordelijke overeenkomstig de DPIA (artikel 35 AVG) worden onderworpen aan een administratieve geldboete (artikel 83 lid 4 onder a AVG). De uitvoering van en het aantoonbaar herzien van de DPIA is dus niet vrijblijvend.

4.3 Criterium 9.3 FG

Wat wijzigt er?
Artikel 37 lid 1 AVG benoemt de gevallen waarin de verwerkingsverantwoordelijke en de verwerker een functionaris gegevensverwerking (FG) moeten aanwijzen. Daarbij wordt na de wetswijziging met name onderdeel c van toepassing voor registratiehouders en ook onderdeel van de toetsing:

> **Artikel 37 lid 1 AVG (Aanwijzing van de functionaris voor gegevensbescherming)**
> *De verwerkingsverantwoordelijke en de verwerker wijzen een functionaris voor gegevensbescherming aan in elk geval waarin:*
> *c) de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens uit hoofde van artikel 9.*

Voor de verwerker heeft deze wetswijziging geen consequenties. De verwerker was op basis van artikel 37 lid 1 van de AVG al verplicht om een FG aan te wijzen.

Wat kunt u doen?
Stel een gekwalificeerde FG aan. De eisen die aan een gekwalificeerde functionaris gesteld worden staan beschreven in criterium 9.3.

4.4 Criterium 9.4 Verwerkingsregister

Wat wijzigt er?
Op basis van artikel 30 lid 1 van de AVG dient de registratiehouder na inwerkingtreding van de wetswijziging een verwerkingsregister bij te houden van de verwerkingsactiviteiten die onder haar verantwoordelijkheid plaatsvinden:

> **Artikel 30 lid 1 van de AVG (Register van verwerkingsactiviteiten) stelt:**
> *Elke verwerkingsverantwoordelijke en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden.*

Voor de verwerker heeft deze wetswijziging weinig[6] consequenties. De verwerker was namelijk al op basis van artikel 30 lid 2 van de AVG verplicht om een verwerkingsregister bij te houden:

> **Artikel 30 lid 2 van de AVG (Register van verwerkingsactiviteiten) stelt:**
> *De verwerker, en, in voorkomend geval, de vertegenwoordiger van de verwerker houdt een register van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht.*

Wat kunt u doen?

De AVG stelt eisen aan de inhoud van het verwerkingsregister. Dit dient de volgende gegevens te bevatten:

a) De naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;
b) de verwerkingsdoeleinden;
c) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
d) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
e) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;
f) indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
g) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1 AVG.

De registratiehouder kan als uitgangspunt het verwerkingsregister van de verwerker gebruiken. Naast aanpassingen in de contactgegevens onder a) dienen de gevraagde gegevens onder b), c), d) en f) toegevoegd te worden.

De werkgroep Standaardovereenkomsten van de DGC heeft, naast templates voor de overeenkomsten, ook een format opgesteld voor het verwerkingsregister. Dit format voldoet aan de eisen die de AVG stelt aan dit register en kan door de registratiehouder gebruikt worden om het eigen verwerkingsregister op te bouwen. Het template is beschikbaar op de website van het SSC-DG.

[6] In het verwerkingsregister van de verwerker wijzigen slechts de naam en de contactgegevens van de (vertegenwoordiger van de) verwerkingsverantwoordelijke(n) voor rekening waarvan de verwerker handelt en de van de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke.

5 Wat wordt er getoetst?

Na inwerkingtreding van de gewijzigde Wkkgz moeten registratiehouders en hun dataverwerkers kunnen aantonen dat zij aan de gewijzigde wet- en regelgeving voldoen. Dit hoofdstuk beschrijft wat de DGC bij de toetsing van registratiehouders en dataverwerkers verwacht. De DGC gaat ervan uit dat registratiehouders, dataverwerkers en zorgaanbieders gebruikmaken van de standaardovereenkomsten.

5.1 Criterium 6 Pseudonimisatie

Criterium 6.1 Gebruik pseudoniemen en toegepaste methode
Er zal door de registratiehouder aangetoond moeten worden dat de organisatie-inrichting van de registratiehouder en dataverwerker voldoet aan wet- en regelgeving over de verwerking van gepseudonimiseerde gegevens. De eisen op basis waarvan de DGC dit vaststelt, worden zo spoedig mogelijk bekend gemaakt.

5.2 Criterium 8 Overeenkomsten

Criterium 8.1 Deelnameovereenkomst
Dit criterium vervalt na inwerkingtreding van de gewijzigde Wkkgz en wordt vervangen door criterium 8.4.

Criterium 8.2 Verwerkersovereenkomst
De registratiehouder toont aan dat de overeenkomst conform de eisen in criterium 8.2 is afgesloten. Hiervoor kan een kopie van de getekende overeenkomst als bewijsstuk worden aangeleverd. Toetsing vindt plaats door een controle op aanwezigheid, datering en ondertekening van de overeenkomst. Daarnaast controleert de DGC of eventuele wijzigingen die zijn aangebracht op de standaardovereenkomst in lijn zijn met de toetsingscriteria.

Criterium 8.3 Raamovereenkomst voor dienstverlening
De registratiehouder toont aan dat de overeenkomst conform de eisen beschreven in criterium 8.3 zijn afgesloten. Hiervoor kunnen een kopie van een overeenkomst en eventuele bijlagen als bewijsstukken dienen. Toetsing vindt plaats door een controle op aanwezigheid, volledigheid, datering en ondertekening van de overeenkomst en de bijlagen. Daarnaast controleert de DGC of eventuele wijzigingen die zijn aangebracht op de standaardovereenkomst in lijn zijn met de toetsingscriteria.

Criterium 8.4 Raamovereenkomst voor deelname
De registratiehouder toont aan dat de overeenkomst conform de eisen beschreven in criterium 8.4 zijn afgesloten. Hiervoor kan een kopie van één van de gesloten overeenkomsten inclusief bijlagen als bewijsstuk dienen. De DGC verwacht dus uitdrukkelijk niet dat alle overeenkomsten met de zorgaanbieders al gesloten zijn, maar wel dat er een start mee is gemaakt. Toetsing vindt plaats door een controle op aanwezigheid en volledigheid van de overeenkomst en de bijlagen. Daarnaast controleert de DGC of eventuele wijzigingen die zijn aangebracht op de standaardovereenkomst in lijn zijn met de toetsingscriteria.

5.3 Criterium 9 Compliance

Criterium 9.1 Beveiliging van de dataverwerking
De toetsing met betrekking tot naleving van artikel 32 lid 1 AVG door de registratiehouder zal plaats vinden op basis van de uitgevoerde DPIA (criterium 9.2) en de daaruit voortvloeiende beschrijvingen van getroffen maatregelen om geïdentificeerde risico's te mitigeren. Om aan te tonen dat de registratiehouder technische en organisatorische maatregelen heeft getroffen in lijn met de NEN7510/ISO27001 en NEN7512 wordt tenminste een '*in control*' statement van het bestuur van de registratiehouder verwacht.

Criterium 9.2 Er is een DPIA uitgevoerd
De ministeriële regeling vereist dat de DPIA op een onafhankelijke wijze wordt getoetst aan het voldoen aan wet- en regelgeving. Hiervoor dient de registratiehouder de DPIA als bewijsstuk aan te leveren bij de toetsing.

Het SSC-DG coördineert deze toets. Zij beheren een lijst van FG's die voldoen aan de deskundigheidseisen zoals vastgesteld door de DGC (zie toetsingscriterium 9.3). Het SSC-DG deelt de DPIA (beveiligd) met één van deze FG's, zodat hij of zij de DPIA kan beoordelen op wet- en regelgeving en de opgestelde eisen van de DGC. Deze FG brengt een onafhankelijk advies uit over de DPIA dat de DGC meeneemt in haar advies en dat aan Zorginstituut Nederland verstrekt wordt bij de aanvraag voor opname in het register.

Gedetailleerde informatie over het verloop van de onafhankelijke toetsing vindt u binnenkort op de website van het SSC-DG.

Criterium 9.3 FG
Bij de toetsing wordt gekeken of de door de registratiehouder aangestelde FG voldoet aan de minimumvereisten zoals die in toetsingscriterium 9.3 benoemd zijn. De DGC beoordeelt dit op basis van een aangeleverd cv of de openbare LinkedIn-pagina van deze persoon. Er wordt gekeken of de FG de juiste opleiding heeft gevolgd en ervaring heeft in/met de zorg(sector) (beide zoals gespecificeerd in het criterium).

Criterium 9.4 Verwerkingsregister
Bij de toetsing wordt gekeken of het register voldoet aan de eisen die de AVG stelt aan het verwerkingsregister. Dit toetst de DGC op basis van een kopie van het verwerkingsregister en omschrijving van de PDCA-cyclus voor het onderhoud van dit verwerkingsregister.

6 Aanvullende toetsing van registraties die vóór de wetswijziging een advies hebben ontvangen

De IGC en DGC zijn gestart met de toetsing van kwaliteitsregistraties voordat de gewijzigde Wkkgz in werking is getreden. Voor criteria 6, 8 en 9 van de DGC wordt er momenteel getoetst op basis van de huidige wet- en regelgeving; dat wil zeggen de situatie vóór de inwerkingtreding van de gewijzigde Wkkgz (zie toelichting op de juridische DGC-toetsingscriteria). Als een kwaliteitsregistratie opgenomen wil worden in het register van kwaliteitsregistraties van Zorginstituut Nederland, moet de registratiehouder aantonen dat zij voldoet aan de nieuwe wet- en regelgeving. Hiervoor wordt de registratiehouder door de DGC aanvullend getoetst op criteria 6, 8 en 9.

Voor wie en waarom is een aanvullende toets nodig?
De aanvullende toets is relevant voor registratiehouders van kwaliteitsregistraties die vóór de inwerkingtreding van de wetswijziging Wkkgz een definitief advies hebben ontvangen van de governancecommissies.

Vanaf de inwerkingtreding van de gewijzigde Wkkgz houdt het Zorginstituut een register bij voor kwaliteitregistraties. Zorginstituut Nederland neemt een kwaliteitsregistratie pas op in dit register wanneer deze aan de nieuwe wet- en regelgeving voldoet. Dit betekent dat de kwaliteitsregistraties die al een definitief advies van de commissies hebben ontvangen voor de wetswijziging Wkkgz, een aanvullende toets nodig hebben van de DGC. Hierin toont de registratiehouder aan dat de kwaliteitsregistratie aan de gewijzigde criteria (6, 8 en 9) voldoet.

Wat wordt er getoetst?
Tijdens de aanvullende toetsing worden criteria 6, 8 en 9 opnieuw getoetst door de DGC. In hoofdstuk 5 van deze handreiking wordt per criterium een toelichting gegeven op de eisen voor kwaliteitsregistraties na de wetswijziging Wkkgz.

Proces en planning van de aanvullende toets
Op de website van de Tweede Kamer is aangekondigd dat de behandeling van de wetswijziging Wkkgz naar week 36 (de eerste week van september) is verplaatst. Door deze verschuiving wijzigt ook de planning voor de aanvullende toetsing, zoals deze in versie 1.0 van deze handreiking stond.

In de oorspronkelijke planning zouden registratiehouders in week 38 (16-20 september) dienen aan te geven dat zij de aanvullende toets voor 1 januari 2025 willen doorlopen. Vervolgens zouden zij de bewijsstukken uiterlijk in week 42 (14-18 oktober) bij de DGC moeten aanleveren. Omdat het mogelijk is dat de wet nog wijzigt naar aanleiding van de bespreking in de Tweede Kamer – wat weer gevolgen kan hebben voor de bewijsstukken die registratiehouders aan moeten leveren – schuift de oorspronkelijke planning door. Daarmee start de aanvullende toets dus op een later moment.

Wij kunnen op dit moment nog geen nieuwe planning communiceren. Zodra hier meer over bekend is, delen we dit in deze handreiking en op onze website.