

## **NOTA VAN TOELICHTING**

### **ALGEMEEN DEEL**

#### 1. Inleiding

##### Algemeen

Met de Wet bevorderen samenwerking en rechtmatige zorg (hierna: de wet) is ingezet op een betere bestrijding van fraude in de zorg door de mogelijkheden voor gegevensuitwisseling en daarmee de samenwerking tussen in de wet genoemde instanties in dat kader te verbeteren. De wet verandert niets aan de reeds bestaande grondslagen voor uitwisselen van gegevens, maar vult deze aan. In het onderhavige Besluit bevorderen samenwerking en rechtmatige zorg (hierna: het besluit) zijn de gegevens aangewezen die op grond van de wet worden verwerkt en het bevat de nadere regels, uitwerking en invulling van de wet en de daarin opgenomen delegatiegrondslagen.

##### Wet bevorderen samenwerking en rechtmatige zorg

De wet voorziet in wettelijke grondslagen voor het verstrekken van persoonsgegevens, waaronder bijzondere persoonsgegevens en persoonsgegevens van strafrechtelijke aard. Het uitgangspunt daarbij is de verplichting tot het verstrekken van de in dit besluit aangewezen (persoons)gegevens, indien dat noodzakelijk is voor de bestrijding van fraude in de zorg. Van een dergelijke noodzaak is sprake indien de bestrijding van (de betreffende) fraude in de zorg zonder de verstrekking niet dan wel onvoldoende kan plaatsvinden. De kaders van privacyregelgeving, waaronder de Algemene verordening gegevensbescherming (hierna: AVG), gelden daarbij onverminderd. De verwerking van gegevens moet rechtmatig zijn en dient plaats te vinden met oog voor de gevoeligheid van de gegevens en met zorg voor de privacy van betrokkenen. Daartoe zijn hoge eisen en voorwaarden gesteld aan de gegevensverwerking en is voorzien in de noodzakelijke waarborgen. Gegevens in het zorgdomein gaan vaak over de gezondheid van mensen. Het zijn gevoelige persoonsgegevens die extra bescherming vereisen. Het medisch beroepsgeheim wordt met de wet niet doorbroken.

De wet bestaat uit twee onderdelen. Het eerste onderdeel van de wet maakt het voor de in artikel 2.1 van de wet genoemde instanties mogelijk onderling gegevens te verstrekken van partijen ten aanzien van wie de gerechtvaardigde overtuiging bestaat dat die hebben gefraudeerd in de zorg. Betrokken instanties zijn voornemens daartoe een centraal registratiesysteem te gebruiken, dat wordt aangeduid als Waarschuwingsregister zorgfraude. Het tweede onderdeel van de wet maakt het mogelijk dat de in artikel 2.4 van de wet genoemde instanties gegevens aan het Informatieknooppunt zorgfraude (IKZ) verstrekken in het geval dat er een aanleiding tot een vermoeden van fraude in de zorg (een 'signaal') bestaat. Het IKZ vult het signaal aan met gegevens die bij of krachtens enige andere wet zijn verkregen, die afkomstig zijn uit de daartoe in de wet aangewezen bronnen en andere noodzakelijke gegevens van betrokken instanties (hierna ook aangeduid als 'verrijken'). Het resultaat daarvan (een 'verrijkt signaal') verstrekt het IKZ vervolgens aan een of meer instanties die gelet op hun rol en wettelijke taak zijn aangewezen de betreffende fraude in de zorg aan te pakken ('geëigende instanties'). Het IKZ heeft zo een ondersteunende rol in de bestrijding van fraude in de zorg. Met deze opzet wordt de samenwerking door instanties efficiënter en kan met het oog op privacygevoelige gegevens ook zorgvuldig worden samengewerkt. Dat levert een betere informatiepositie van instanties op en stelt ze in staat efficiënter en, mede met het oog op privacy, zorgvuldig te beoordelen of sprake is van fraude in de zorg. Daarnaast heeft het IKZ ingevolge artikel 2.5 van de wet ook een taak om ten behoeve van de Minister van Volksgezondheid, Welzijn en Sport, welke taak nu is belegd bij de Minister voor Langdurige Zorg en Sport (hierna: de Minister voor LZS) en de betrokken

instanties trends en ontwikkelingen met betrekking tot fraude in de zorg te signaleren en daarover beleidsinformatie en statistische gegevens te ontwikkelen. Het IKZ heeft geen handhavende, toezichthoudende of opsporende functie, taken of bevoegdheden.

#### Terminologie

Onder het begrip fraude in de zorg wordt in dit besluit verstaan het opzettelijk misleidend handelen binnen het zorgdomein, met het oog op eigen of andermans gewin, voor zover het in de wet strafbaar gestelde feiten betreft. Voor de achtergrond en toelichting van deze begripsbepaling wordt verwezen naar paragraaf 2.1 van de memorie van toelichting bij de wet.<sup>1</sup> Het gaat bijvoorbeeld om spookzorg, pakketfraude, fraude met declaraties en fraude met persoonsgebonden budget (pgb).

Gezien het overkoepelende karakter van de wet met betrekking tot het zorgdomein, dat bestaat uit diverse domeinen (geografisch, soort zorg, etc.), moet het begrip zorg worden gelezen in de context van de domeinen waarop de wet betrekking heeft en waarbinnen de toezichthouders en opsporingsdiensten in het kader van de diverse zorgwetten opereren.<sup>2</sup> Onder zorg wordt hier ook maatschappelijke ondersteuning en jeugdhulp verstaan. In het verlengde daarvan is in artikel 1 van dit besluit het begrip aanbieder, dat net als het begrip zorgaanbieder een gevarieerde reikwijdte in diverse wetten heeft, gedefinieerd. De begrippen aanbieder en zorgaanbieder worden in deze toelichting beide gebruikt en daarmee worden dus zowel aanbieders van zorg als de verleners van maatschappelijke ondersteuning en jeugdhulp bedoeld. Voorts wordt in deze toelichting daar waar mogelijk gesproken over zorgbehoevende(n), aangezien door de brede reikwijdte van de wet sprake kan zijn van verzekerden, cliënten en patiënten. Alleen in specifieke gevallen of beschrijving van casuïstiek zullen laatstgenoemde termen worden gebruikt.

In deze nota van toelichting is ook wat betreft overige terminologie en definities aangesloten bij de memorie van toelichting bij de wet. Zo zijn de colleges van burgemeester en wethouders in de toelichting aangeduid als 'gemeenten'. Ook worden waar nodig ter verduidelijking specifieke vormen van verwerking, als bedoeld in artikel 4, onderdeel 2, AVG, genoemd, zoals verstrekken, verrijken en uitwisselen van persoonsgegevens. Waar het politiekegevens betreffen, moeten voornoemde begrippen overeenkomstig de invulling daarvan in de Wet politiekegevens worden uitgelegd.

#### Leeswijzer

In hoofdstuk 2 van deze nota van toelichting wordt aandacht besteed aan de bijzondere kadervormende aspecten naast de wet, zoals privacy, het medisch beroepsgeheim en het regime voor politiekegevens. In hoofdstuk 3 wordt ingegaan op de uitwerking van de regels voor het onderling verstrekken van gegevens in het geval dat een gerechtvaardigde overtuiging van fraude in de zorg bestaat. In hoofdstuk 4 is vervolgens de uitwerking van de regels met betrekking tot de rol en taken van het IKZ toegelicht. In het vijfde hoofdstuk wordt de gegevensbeschermingseffectbeoordeling die voor dit besluit is uitgevoerd beschreven. Het zesde hoofdstuk beschrijft de ontvangen adviezen ten aanzien van dit besluit. Aangesloten wordt met een artikelsgewijze toelichting.

#### 2. Bijzondere kadervormende aspecten: privacy, doenvermogen, medisch beroepsgeheim en politiekegevens

Het recht op privacy en de bescherming van de persoonlijke levenssfeer en het medisch beroepsgeheim, vormen waarborgen om persoonsgegevens te beschermen. Daarnaast geldt ten aanzien van politiekegevens een bijzonder regime. Enerzijds ook in het kader

---

<sup>1</sup> Kamerstukken II 2019/20, 35 515, nr. 3.

<sup>2</sup> Het betreft de Zorgverzekeringswet, Wet langdurige zorg, Wet maatschappelijke ondersteuning 2015 en Jeugdwet.

van de bescherming van persoonsgegevens, maar anderzijds met het oog op de opsporingstaak in het kader van het strafrecht.

Deze aspecten zijn in de wet en de daarbij behorende memorie van toelichting, met name in hoofdstuk 5, reeds aan de orde gekomen en spelen een belangrijke rol in dit besluit. Gelet daarop worden deze aspecten hier in het algemeen toegelicht, waarna ze voor zover nodig concreter aan bod komen in hoofdstukken drie en vier.

#### Privacy

Bij de totstandkoming van de wet is de afweging gemaakt dat het zwaarwegende algemeen belang bij de bestrijding van fraude in de zorg een mogelijke inmenging in de privacy van betrokkenen, rechtvaardigt. Voor een uitgebreide toelichting ten aanzien hiervan, waarbij onder andere wordt ingegaan op de voor deze afweging van belang zijnde elementen uit het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM) en het Handvest van de grondrechten van de Europese Unie (EU-Handvest), wordt verwezen naar de memorie van toelichting bij de wet (o.a. hoofdstuk 5). Daar is ook toegelicht hoe de AVG in vorenstaande afweging is meegenomen en hoe de AVG in acht is genomen bij de totstandkoming van de wet. De wet is zo ingericht dat gewaarborgd wordt dat het verwerken van persoonsgegevens, zoals het verstrekken, registreren en verrijken ervan, alleen is toegestaan indien die verwerking noodzakelijk is in het kader van bestrijding van fraude in de zorg. Dat betekent dat die verwerking nodig moet zijn omdat het in de wet bepaalde doel van de verwerking, te weten bestrijding van fraude in de zorg, anders redelijkerwijs niet kan worden verwezenlijkt. In de vraag of een verwerking van persoonsgegevens noodzakelijk is, ligt besloten of die verwerking proportioneel is en of de verwerking voldoet aan de eis van subsidiariteit. Of de verwerking proportioneel is, betreft de vraag naar effectiviteit en evenredigheid. Het legitieme doel dat wordt nagestreefd moet in verhouding staan tot het feit dat daarvoor persoonsgegevens moeten worden verwerkt. Als het doel van de verwerking op een wijze kan worden bereikt waarbij een geringere inbreuk wordt gemaakt op de privacy van betrokkene(n), dan moet gelet op de eis van subsidiariteit voor die mogelijkheid worden gekozen. Wat betreft de verwerking van bijzondere persoonsgegevens of persoonsgegevens van strafrechtelijke aard, geldt dat specifieke en passende maatregelen respectievelijk passende waarborgen moeten zijn geboden ter bescherming van de rechten en vrijheden van betrokkenen.

In dit besluit zijn onder andere vorenstaande waarborgen nader geregeld, ingevuld en uitgewerkt. Daarbij is als uitgangspunt genomen dat verwerkingsverantwoordelijken, verantwoordelijk zijn voor de rechtmatige en zorgvuldige omgang met persoonsgegevens en in dat kader de plichten uit de AVG moeten naleven. Zo moeten ingevolge artikel 24 AVG passende technische en organisatorische maatregelen worden getroffen om te waarborgen en aan te tonen dat de verwerking in overeenstemming met de AVG is. Een van de uitgangspunten is het in artikel 25 AVG opgenomen beginsel van privacy by design en privacy by default, dat betekent privacy door ontwerp en standaardinstellingen. Welke technische en organisatorische maatregelen moeten worden genomen, is afhankelijk van het geval. Rekening moet worden gehouden met de stand van de techniek, de uitvoeringskosten, de aard, omvang, context en het doel van de verwerking en de risico's voor de betrokkene. De maatregelen moeten onder andere waarborgen dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel van de verwerking. Het gaat ook om de hoeveelheid persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor gegevens worden opgeslagen en de toegankelijkheid ervan.

Op een aantal punten laat de AVG aan de nationale wetgever de ruimte voor nationale keuzes. Deze zijn uitgewerkt in de Uitvoeringswet Algemene verordening

gegevensbescherming (UAVG). Het gaat onder andere om bepalingen ten aanzien van rechten van betrokkenen van wie persoonsgegevens worden verwerkt. In onderhavig besluit zijn ook nadere regels opgenomen ter waarborging van de mogelijkheid tot uitoefening van deze rechten en de verantwoordelijkheidsverdeling tussen betrokken instanties.

#### Doenvermogen

De wet is gericht op de bescherming van burgers tegen fraude in de zorg door, met name, zorgaanbieders. De wet voorziet in grondslagen tot gegevensuitwisseling door betrokken instanties ten behoeve van een verbeterde aanpak van fraude in de zorg en heeft niet tot gevolg dat (veel) handelingen van burgers worden verwacht en dat een beroep op hun doenvermogen wordt gedaan. Dat doet er echter niet aan af dat het voor partijen die met de gevolgen van de wet te maken krijgen, duidelijk moet zijn wanneer wat van hen verwacht wordt en waar zij daarvoor terecht kunnen. Dit is meegenomen in de uitwerking van de wet in dit besluit en komt onder meer tot uiting in de hoge eisen en waarborgen die zijn gesteld ten aanzien van de kenbaarheid van processen en de mogelijkheden om tegen gegevensverwerking en de gevolgen daarvan op te komen.

#### Medisch beroepsgeheim

Zoals in de memorie van toelichting bij de wet reeds is toegelicht, wordt het medisch beroepsgeheim met de wet niet doorbroken. Het medisch beroepsgeheim is een groot goed. Het dient ter bescherming van de individuele zorgbehoevende en is een waarborg voor vrije toegang tot de gezondheidszorg. In artikel 1.2 van de wet is de uitwisseling van gegevens waarop het medisch beroepsgeheim rust uitgesloten.

Omdat in dit besluit is geregeld welke gegevens op grond van de wet wél verstrekt worden, wordt hier ter verduidelijking toegelicht op welke gegevens het medisch beroepsgeheim rust en derhalve niet op grond van de wet mogen worden verstrekt. Ook is toegelicht tot welke beroepsbeoefenaars het medisch beroepsgeheim zich richt.

Het medisch beroepsgeheim rust op alle gegevens die de zorgaanbieder in de uitoefening van zijn of haar beroep over de patiënt te weten is gekomen. Het medisch beroepsgeheim is niet beperkt tot medische zaken, ook de gezinssituatie of privéomstandigheden kunnen hieronder vallen. Ook op het enkele feit dat een zorgbehoevende een afspraak heeft met een zorgaanbieder, kan het medisch beroepsgeheim rusten.

Artikel 88 van de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG) bepaalt dat een ieder die een beroep op het gebied van de individuele gezondheidszorg uitoefent, de plicht heeft alles geheim te houden wat hem bij de uitoefening van zijn beroep is toevertrouwd. Ook in het Burgerlijk Wetboek (BW) is een geheimhoudingsbepaling opgenomen (artikel 7:457 BW). Dit onderdeel van het BW wordt ook aangeduid als Wet inzake de geneeskundige behandelingsovereenkomst (WGBO). Hieronder vallen alle zorgaanbieders die op grond van een behandelingsovereenkomst met de zorgbehoevende handelingen op het gebied van de geneeskunst verrichten. Een zorgaanbieder in de zin van de WGBO kan zowel een individuele hulpverlener als een organisatie zijn. Voor medewerkers die zelf geen medisch beroepsgeheim hebben maar bij de zorgverlening betrokken zijn, geldt een afgeleid medisch beroepsgeheim.

*Het gaat dan om medewerkers die beroepsmatig kennisnemen van behandelgegevens van de zorgbehoevende. Bijvoorbeeld een assistent of secretaresse, maar ook ICT-medewerkers.*

In het kader van het eerste onderdeel van de wet, zoals geregeld in artikel 2.1 e.v. van de wet, mogen geen gegevens worden uitgewisseld waarop het medisch beroepsgeheim rust. Dat betekent dat in het Waarschuwingsregister geen gegevens geregistreerd worden

waarop een medisch beroepsgeheim rust. De gegevensset voor het Waarschuwingsregister is beperkt tot noodzakelijke identificerende gegevens en administratieve kenmerken. Daarmee is gewaarborgd dat geen gegevens worden geregistreerd waarop een medisch beroepsgeheim rust.

Wat betreft het tweede onderdeel van de wet, zoals geregeld in 2.4 e.v. van de wet, geldt dat gegevens waarop het medisch beroepsgeheim rust niet aan het IKZ mogen worden verstrekt. De gegevensset voor het IKZ bevat echter wel gegevens waarop een medisch beroepsgeheim kan rusten. Betrokken instanties kunnen namelijk in sommige gevallen beschikken over deze gegevens en hebben dan een afgeleid medisch beroepsgeheim. Deze gegevens kunnen noodzakelijk zijn voor een effectieve en zorgvuldige verrijking van signalen van fraude in de zorg. Instanties zullen deze gegevens, voordat zij deze aan het IKZ verstrekken, zodanig moeten bewerken dat zij niet langer herleidbaar zijn tot een natuurlijke persoon. Als de gegevens niet langer te herleiden zijn tot een natuurlijke persoon, valt het niet langer onder het medisch beroepsgeheim en staat het medisch beroepsgeheim er niet meer aan in de weg om de gegevens aan het IKZ te verstrekken. Op deze manier rust er nooit een beroepsgeheim op gegevens die door het IKZ worden ontvangen.

*Declaratiegegevens bevatten medische gegevens, bijvoorbeeld informatie over de behandeling. Ook indicatiegegevens bevatten gegevens over de gezondheid. Op deze gegevens rust in de regel een medisch beroepsgeheim wanneer deze (direct of indirect) afkomstig zijn van de zorgaanbieder. Dit soort gegevens moeten door instanties geaggregeerd worden voordat ze aan het IKZ kunnen worden verstrekt.*

#### Politiegegevens

Persoonsgegevens die door betrokken instanties worden verwerkt als onderdeel van het toezicht dat zij op grond van hun wettelijke taak uitvoeren, vallen onder het toepassingsbereik van de AVG. Het toezicht is erop gericht om mensen en organisaties zich te laten houden aan de norm. Er zijn echter ook betrokken instanties, de bijzondere opsporingsdiensten (hierna: 'BOD's'), de Nederlandse arbeidsinspectie (NLA) en Fiscale inlichtingen- en opsporingsdienst (FIOD), die zich op grond van hun wettelijke taken bezighouden met de opsporing van strafbare feiten. Er wordt van opsporing gesproken indien sprake is van een 'onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen'. Persoonsgegevens die worden verwerkt als onderdeel van de opsporing, vallen onder het toepassingsbereik van de Wet politiegegevens (Wpg) en worden aangeduid als 'politiegegevens'. Vanaf het moment dat politiegegevens door het IKZ zijn ontvangen, is niet langer sprake van politiegegevens onder het regime van de Wpg. De gegevens zijn dan persoonsgegevens, mogelijk van strafrechtelijke aard, waarop de AVG van toepassing is. Voor het onderdeel van de wet dat ziet op het Waarschuwingsregister worden geen politiegegevens verwerkt.

In het kader van de wet gaat het dus om het verstrekken van politiegegevens door de NLA en FIOD aan het IKZ. Die verstrekking geschiedt op grond van en met inachtneming van de Wpg, waarmee het uitgangspunt voor de verstrekking van deze gegevens afwijkt van het uitgangspunt van verplichte verstrekking zoals dat voor de overige gegevens geldt. In de Wpg zijn categorieën van gegevensverwerking opgenomen. In het Besluit politiegegevens (Bpg) is aan de hand van die categorieën bepaald ten behoeve waarvan welke politiegegevens kunnen worden verstrekt. Teneinde de verstrekking van politiegegevens in het kader van de wet mogelijk te maken, wordt met dit besluit het Bpg gewijzigd. Met inachtneming van de systematiek van de Wpg, is aan het Bpg toegevoegd dat voornoemde BOD's ten behoeve van de uitvoering van de wet politiegegevens aan het IKZ kunnen verstrekken. De persoonsgegevens en niet-persoonsgegevens die de BOD's

verwerken blijken in de praktijk overigens zo nauw met elkaar verweven, dat daartussen geen onderscheid wordt gemaakt bij verstrekking van gegevens aan het IKZ.<sup>3</sup>

Ten aanzien van de FIOD geldt dat in het geval dat sprake is van een fiscaal strafrechtelijk onderzoek, ook de fiscale wet- en regelgeving van toepassing is. Voor gegevens die onderdeel uitmaken van een dergelijk onderzoek, is de geheimhoudingsplicht als bedoeld in artikel 67 van de Algemene Wet inzake Rijksbelastingen (hierna: 'AWR') van toepassing. Als deze gegevens onderdeel uitmaken van een verrijkt signaal dat door het IKZ aan een ziektekostenverzekeraar wordt verstrekt, worden deze gegevens ingevolge artikel 2.4, derde lid, van de wet, slechts verstrekt indien wordt voldaan aan de in dit besluit gestelde regels.

### 3. Gegevensverstrekking bij gerechtvaardigde overtuiging van fraude in de zorg ('het Waarschuwingregister zorgfraude')

#### 3.1 Inleiding

Dit onderdeel van de wet vormt de wettelijke grondslag voor gemeenten en ziektekostenverzekeraars om elkaar onderling gegevens, waaronder persoonsgegevens, te verstrekken van partijen ten aanzien van wie een gerechtvaardigde overtuiging bestaat dat zij fraude hebben gepleegd in de zorg. Genoemde instanties kunnen elkaar zo waarschuwen voor die partijen en indien nodig maatregelen treffen. Of de gerechtvaardigde overtuiging van fraude er in een bepaald geval is en of het noodzakelijk is de gegevens te verstrekken, moet worden vastgesteld overeenkomstig het bij ministeriele regeling vast te stellen protocol. Teneinde rechtsgelijkheid, rechtszekerheid en een zorgvuldige en rechtmatige verwerking van gegevens in het kader van dit onderdeel van de wet voor betrokken partijen te waarborgen, is het van belang dat betrokken instanties de afweging maken aan de hand van heldere, objectieve en uniforme criteria. Dat is ook noodzakelijk voor uitvoering van de in artikel 2.2 van de wet bedoelde toets van de gerechtvaardigde overtuiging door de gemeentelijk toezichthouder respectievelijk de Nederlandse zorgautoriteit (hierna: NZa) voorafgaand aan de verstrekking van gegevens. Ten behoeve daarvan zijn in dit besluit de voorwaarden om tot een gerechtvaardigde overtuiging komen en de eisen aan het protocol opgenomen. Ook zijn in dit besluit de gegevens aangewezen die op grond van de wet mogen worden uitgewisseld en zijn regels opgenomen ten aanzien de beveiliging van gegevens, de bewaartermijnen en de uitoefening van rechten van betrokkenen.

De verstrekking van gegevens in het geval van een gerechtvaardigde overtuiging van fraude in de zorg is techniekonafhankelijk geregeld. De wet noch dit besluit schrijft een systeem voor, maar betrokken instanties zijn voornemens hiertoe het Waarschuwingregister zorgfraude (hierna: 'Waarschuwingregister') te gebruiken. Het besluit bevat wel regels over wat in het protocol in algemene zin wordt opgenomen ten aanzien van een systeem dat door betrokken instanties zal worden gebruikt voor gegevensverstrekking, zodat op eenduidige wijze en met passende waarborgen uitvoering wordt gegeven aan de wet. Bij de toelichting van deze regels wordt het Waarschuwingregister genoemd en dan wordt bijbehorende terminologie, zoals het 'registreren' en 'raadplegen' van gegevens, gebruikt.

Persoonsgegevens die in het geval van gerechtvaardigde overtuigingen van fraude in de zorg worden verstrekt, worden geschaard onder persoonsgegevens van strafrechtelijke aard als bedoeld in artikel 10 AVG. Persoonsgegevens van dien aard mogen ingevolge de AVG alleen verwerkt worden als passende waarborgen zijn geboden ter bescherming van

---

<sup>3</sup> Met 'niet-persoonsgegevens' worden in dit besluit gegevens aangeduid die niet onder het begrip 'persoonsgegevens' als bedoeld in artikel 4, eerste lid, van de AVG.

de rechten en vrijheden van betrokkenen. Daar wordt met dit besluit en de bij ministeriële regeling vast te stellen protocol in voorzien. Ten aanzien van zowel persoonsgegevens als niet-persoonsgegevens gelden vergelijkbare waarborgen en maatregelen ten behoeve van een zorgvuldige en rechtmatige verwerking van gegevens. In dit hoofdstuk wordt daarom het begrip 'gegevens' gebruikt. Enkel wanneer er aanleiding toe is, wordt specifiek onderscheid gemaakt tussen persoonsgegevens en niet-persoonsgegevens.

### 3.2 Gerechtaardigde overtuiging en eisen aan het protocol

#### Gerechtaardigde overtuiging van fraude in de zorg

In artikel 2.1, eerste lid, van dit besluit zijn de voorwaarden opgenomen om tot een gerechtaardigde overtuiging van fraude in de zorg te komen. Deze voorwaarden zijn gebaseerd op jurisprudentie over het externe verwijzingsregister (EVR) van financiële instellingen. Dit is uitgebreid toegelicht in paragraaf 3.3 van de memorie van toelichting bij de wet.

Vereist is dat voldoende bewijs van betrokkenheid bij de fraude voorhanden is en sprake is van een vastgestelde gedraging die een zwaardere verdenking dan een redelijk vermoeden oplevert. Daartoe is nodig dat een betrokken instantie een zorgvuldig fraudeonderzoek heeft uitgevoerd aan de hand van de in het protocol beschreven werkwijze. Het onderzoek en de bewijsstukken moeten inzicht geven in de elementen van fraude in de zorg, zoals opzet, misleidend handelen binnen het zorgdomein en dat met eigen of andermans gewin als oogmerk. De gemeentelijk toezichthouder respectievelijk de NZa moeten op basis van dat onderzoek eveneens tot de conclusie komen dat sprake is van een gerechtaardigde overtuiging van fraude in de zorg. De gemeentelijke toezichthouder respectievelijk de NZa doen het onderzoek niet over, maar aan de hand van het dossier onderzoeken of ze op basis van het gepresenteerde bewijs tot hetzelfde oordeel komen.

#### Eisen aan het protocol

In hoofdstuk 5 van de memorie van toelichting bij de wet is toegelicht waarom de grondslag voor onderlinge gegevensuitwisseling tussen gemeenten en ziektekostenverzekeraars in het geval van een gerechtaardigde overtuiging van fraude in de zorg in algemene zin noodzakelijk en proportioneel is. De te maken afweging tot gegevensverstrekking in een individueel geval wordt vormgegeven in het protocol. Het gaat om aspecten zoals de omstandigheden van het geval, waaronder de mate van ernst van de fraude, de omvang van de gevolgen van de fraude voor het zorgdomein, de gevolgen (zowel persoonlijk als zakelijk) van de verwerking voor de betrokken partij, minderjarigheid van de betrokkene(n) of de afweging van een eerste overtreding van de wet tegenover recidive. Mede op basis van het uitgevoerde fraudeonderzoek moet onderbouwd worden waarom de gerechtaardigde overtuiging in het specifieke geval verstrekking, bijvoorbeeld door middel van registratie in het Waarschuwingsregister, rechtvaardigt. In het protocol wordt inzichtelijk gemaakt wanneer gebruik van die gegevens door andere betrokken instanties, bijvoorbeeld door raadpleging het Waarschuwingsregister, kan plaatsvinden bij de inkoop van zorg en wordt de daartoe te maken afweging vormgegeven.

Betrokken instanties dienen altijd zelf onderzoek te doen naar een partij ten aanzien van wie een gerechtaardigde overtuiging van fraude in de zorg bestaat en van wie zij gegevens hebben ontvangen. Zij moeten zorgvuldig bepalen welke beheersmaatregelen worden getroffen. Gedacht kan worden aan het doen van onderzoek naar fraude en het op basis van dat onderzoek doen van extra controles, het stellen van extra of scherpere voorwaarden of het niet aangaan dan wel beëindigen van een overeenkomst betreffende zorgverlening. In het protocol wordt inzicht gegeven in de mogelijke gevolgen die

betrokken instanties aan een waarschuwing kunnen geven en welke rechtsmiddelen daartegen open staan.

Gemeenten en ziektekostenverzekeraars moeten ook communiceren over de gegevensverwerking op grond van de wet. De wijze waarop zij dat doen wordt opgenomen in het protocol. Het gaat niet alleen om de informatieplicht op grond van de AVG, maar bijvoorbeeld ook om het proactief informatie verstrekken op de eigen website of aan een partij waarmee zij (voornemens zijn) een overeenkomst aan te gaan.

Hoewel de Autoriteit persoonsgegevens (hierna: AP) ingevolge de UAVG formeel toezichthouder is op de verwerking van persoonsgegevens en een betrokkene wiens persoonsgegevens worden verwerkt op grond van artikel 77 AVG een klacht in kan dienen bij de AP, zijn de betrokken instanties verantwoordelijk voor intern toezicht op juiste en zorgvuldige omgang met gegevens. Derhalve is in dit besluit voorgeschreven dat elke instantie daartoe een proces heeft ingericht. De uitgangspunten daarvoor worden in het protocol opgenomen. Als het de verwerking van persoonsgegevens betreft, is daarbij op grond van de AVG een belangrijke rol weggelegd voor de functionaris gegevensbescherming (FG) van de betrokken instanties. Uit de AVG volgt onder andere dat een betrokkene zich tot de FG van een verwerkingsverantwoordelijke instantie kan wenden voor alle aangelegenheden die verband houden met de verwerking van zijn persoonsgegevens en met de uitoefening van zijn rechten uit hoofde van de AVG. In het besluit is voorgeschreven dat betrokken instanties zorgdragen voor een vergelijkbaar niveau van bescherming als het om andere gegevens dan persoonsgegevens gaat. Het ligt in de rede dat de persoon die als FG functioneert, een soortgelijke functie vervult als het om de verwerking van andere gegevens dan persoonsgegevens gaat. Ook de uitgangspunten daarvoor worden in het protocol opgenomen. Tot slot wordt de in artikel 2.9 van de wet opgenomen geheimhoudingsplicht uitgewerkt in het protocol.

De overige eisen aan het protocol waarborgen een zorgvuldige en rechtmatige verwerking van gegevens. Het gaat dan bijvoorbeeld om eisen ten aanzien van te volgen procedures, de inrichting en het beheer van het systeem dat voor gegevensuitwisseling wordt gebruikt, de beveiliging van de te verwerken gegevens, de bewaartermijn en het verwijderen van gegevens, de uitoefening van de rechten van betrokkenen en de samenwerking van betrokken instanties. De overige onderdelen die in het protocol moeten terugkomen en die hierna worden toegelicht, moeten in samenhang worden gezien met de hiervoor genoemde en elders toegelichte onderdelen.

### 3.3 Gegevensset

Ingevolge de wet verstrekken betrokken instanties elkaar de bij algemene maatregel van bestuur (hierna: amvb) aangewezen gegevens. In onderhavig besluit zijn de betreffende gegevens aangewezen. In deze paragraaf wordt toegelicht welke gegevens door de betrokken instanties worden verstrekt. Conform artikel 5, eerste lid, onderdeel c, AVG en met het oog op het beginsel van privacy by design alsmede de voor de verwerking van persoonsgegevens van strafrechtelijke aard vereiste passende waarborgen, betreft de in dit besluit aangewezen set aan gegevens een zo minimaal mogelijke gegevensset. Met de verstrekking van minder gegevens zou het onderdeel van de wet waarop dit deel van het besluit betrekking heeft, niet effectief en zorgvuldig kunnen worden uitgevoerd. Het zijn de gegevens die noodzakelijk zijn teneinde bijvoorbeeld te kunnen vaststellen dat de 'waarschuwing' de juiste (rechts)persoon betreft. Ook zijn het gegevens die ten dienste staan aan de mogelijkheid tot het uitoefenen van rechten door betrokkene(n) van wie de gegevens worden verwerkt. De gegevensset is tot stand gekomen in afstemming met betrokken instanties.



Indien aan de voorwaarden tot verstrekking is voldaan, verstrekken instanties alle gegevens die van deze gegevensset onderdeel uitmaken. Instanties verstrekken in het kader van dit onderdeel de wet echter nooit meer of andere gegevens dan die in dit besluit zijn aangewezen. Het systeem dat door instanties wordt gebruikt teneinde de gegevens aan elkaar te verstrekken, moet ook zodanig zijn ingericht dat het niet mogelijk is dat minder gegevens of andere gegevens dan uit de gegevensset worden verstrekt. Gelet op de in artikel 2.1 van de wet opgenomen betrokken instanties, zullen in het kader van dit onderdeel van de wet geen persoonsgegevens als bedoeld in de Wpg worden verwerkt.

Van een rechtspersoon worden de administratieve kenmerken verstrekt. Het gaat om de naam, het adres, de vestigingsplaats, het Kamer van Koophandel (KvK)-nummer en het door ziektekostenverzekeraars gehanteerde nummer ter identificatie van de rechtspersoon, zoals een of meerdere AGB-code(s).

Van een natuurlijk persoon worden identificerende gegevens verstrekt. Het gaat om de naam, het adres, de woonplaats, de geboortedatum en het geslacht. Indien van toepassing worden van een natuurlijk persoon ook verstrekt het BIG-registratienummer, het KvK-nummer in relatie tot de natuurlijke persoon en een door ziektekostenverzekeraars gehanteerd nummer ter identificatie, zoals een of meerdere AGB-code(s), die gelieerd worden aan de natuurlijk persoon.

Daarnaast verstrekken gemeenten ten behoeve van andere gemeenten ook het burgerservicenummer (BSN). De in het kader van artikel 87 AVG en artikel 46 UAVG benodigde grondslag voor de verwerking van dit wettelijk identificatienummer door gemeenten in het kader van dit onderdeel van de wet, is opgenomen in artikel 10 van de Wet algemene bepalingen burgerservicenummer (hierna: Wabb). Voor ziektekostenverzekeraars geldt deze bepaling niet. Voor hen geldt ook geen andere wettelijke bepaling op grond waarvan zij het BSN in het kader van dit onderdeel van de wet mogen verwerken. Dat betekent dat zij het niet verstrekken, maar ook niet zien wanneer zij de gegevens raadplegen.

Voornoemde administratieve kenmerken van een rechtspersoon respectievelijk identificerende gegevens van een natuurlijk persoon zijn noodzakelijk, omdat de betrokken instanties daarmee zowel bij registratie als bij raadpleging van de verstrekte gegevens in staat zijn zorgvuldig en met voldoende zekerheid vast te stellen dat het om de juiste (rechts)persoon gaat. De NAW-gegevens, het geslacht, de geboortedatum en, indien van toepassing, het BIG-registratienummer en de AGB-code(s) van een natuurlijk persoon worden verstrekt, zodat ook ziektekostenverzekeraars, die het BSN voor dit doeleinde niet mogen gebruiken, met voldoende zorgvuldigheid en zekerheid kunnen vaststellen dat het om de juiste natuurlijke persoon gaat. Deze gegevens zijn ook noodzakelijk voor het praktisch en gericht kunnen raadplegen van gegevens.

Ten aanzien van zowel rechtspersonen als natuurlijke personen wordt het ook kenbaar gemaakt als een betreffende partij nog niet is geïnformeerd over de gegevensverwerking op grond van de wet. Dat kan bijvoorbeeld het geval zijn in het geval zijn als het informeren van betrokkene de bestrijding van het betreffende geval van fraude in de zorg onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In het protocol worden richtlijnen opgenomen ten aanzien van het afzien van informeren en het treffen van maatregelen ten behoeve van het zo spoedig mogelijk alsnog informeren van betrokkene(n).

Bij de verstrekking van gegevens worden ook de naam, een e-mailadres en een telefoonnummer van de verstrekende instantie vermeld. Dit is onder andere noodzakelijk voor het geval dat een partij van wie gegevens worden verwerkt zich voor de uitoefening

van zijn rechten wendt tot een van de betrokken instanties. Als de instantie tot wie de partij zich wendt niet zelf gegevens heeft verstrekt, kan de partij worden verwezen naar de instantie die dat wel heeft gedaan.

Wat betreft bijzondere persoonsgegevens, zoals gegevens over gezondheid als bedoeld in artikel 9, eerste lid, AVG, geldt dat geen medisch inhoudelijke gegevens worden verstrekt. In het naar verwachting uitzonderlijke geval van verstrekking van gegevens van een zorgbehoevende, bijvoorbeeld in het geval van samenspanning, is het wel mogelijk dat, min of meer indirect, gegevens over de gezondheid worden verstrekt. Dat kan bijvoorbeeld het geval zijn bij verstrekking door het zorgkantoor, waarbij duidelijk wordt dat de betrokkene Wlz-zorg ontvangt. De gegevens over gezondheid betreffen dan slechts de gegevens waaruit blijkt in welk domein de zorg aan desbetreffend zorgbehoevende, ten aanzien van wie een gerechtvaardigde overtuiging van fraude bestaat, wordt geleverd. Het betreft nooit gegevens waarop het medisch beroepsgeheim rust.

De verstrekking instantie legt de startdatum van de verstrekking, bijvoorbeeld de datum van registratie in het Waarschuwingsregister, vast in verband met de toepassing van de termijnen die gelden voor het verstrekken en bewaren van de gegevens. De datum van registratie is voor raadplegende instanties niet noodzakelijk en derhalve niet zichtbaar.

### 3.4 Beveiliging

Artikel 32 AVG verplicht de betrokken instanties de verwerking van persoonsgegevens te beveiligen. Instanties dienen hiertoe passende technische en organisatorische maatregelen te treffen, die een op het risico afgestemd beschermingsniveau waarborgen. Het vorenstaande geldt onverminderd voor gegevens niet zijnde persoonsgegevens. Gelet op de gevoeligheid van de gegevens die in het kader van dit onderdeel van de wet worden verwerkt en de (mogelijke) gevolgen voor betrokkenen van deze verwerking worden hoge eisen gesteld aan de beveiliging van het daarvoor gebruikte systeem, zoals het Waarschuwingsregister. Dit onder andere ter voorkoming van ongeoorloofde toegang tot of gebruik van de gegevens. Gemeenten en ziektekostenverzekeraars dragen gezamenlijk zorg voor een adequate beveiliging en, in het verlengde daarvan, de inrichting en het beheer van het Waarschuwingsregister. Dit wordt nader vormgegeven in het protocol.

In artikel 2.4, eerste lid, van dit besluit is bepaald dat voor de beveiliging van de gegevens eisen gesteld worden bij ministeriële regeling. De verstrekking en verwerking van gegevens wordt beveiligd en is op een bepaald vertrouwelijkheidsniveau bestand tegen incidentele gebeurtenissen of onrechtmatige of kwaadaardige acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen of doorgegeven gegevens in het gedrang brengen.

Teneinde vorenstaande beveiligingsniveau te waarborgen en gelet op de publiek-private samenwerking, is het voornemen bij ministeriële regeling de Baseline Informatiebeveiliging Overheid (BIO) voor te schrijven als beveiligingsnorm voor het Waarschuwingsregister.<sup>4</sup> De reden dit in een ministeriële regeling te doen, is voornamelijk van wetstechnische en pragmatische aard en wordt toegelicht in de artikelsgewijze toelichting. Het gaat bij de BIO om standaardnormeringen. In algemene zin betreft het onder andere informatiebeveiligingsbeleid, het organiseren van informatiebeveiliging, personeelsbeleid, het beheer van bedrijfsmiddelen, de toegangsbeveiliging, de fysieke beveiliging en beveiliging van de omgeving en de beveiliging van bedrijfsvoering en communicatiebeveiliging. In de praktijk komt dat bijvoorbeeld neer op versleuteling van de persoonsgegevens (zoals pseudonimisering), het regelen van screening en opleiding van personeel, het voeren van een autorisatiebeleid, het waarborgen van de

---

<sup>4</sup> Circulaire van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 23 mei 2019, Stcrt. 2019, 26526

geheimhoudingsplicht uit artikel 2.9 van de wet, het loggen van uitgevoerde acties en het classificeren, opslaan en verwijderen van te verwerken gegevens. Gedacht moet worden aan het scheiden van de verschillende bevoegdheden die er zijn binnen het Waarschuwingregister en deze moeten bij verschillende afdelingen of personen binnen de betrokken instanties worden belegd. Zo kan voor de verstreckende instanties worden geregeld dat de registratie van gegevens alleen gedaan worden door specifiek daartoe bevoegde medewerkers, het wijzigen alleen door andere medewerkers en het verwijderen door weer andere medewerkers. In aansluiting op het vastleggen van procedurevoorschriften omtrent de mogelijkheid tot het raadplegen van het Waarschuwingregister door instanties, te weten in het geval dat noodzakelijk is in het kader van bestrijding van fraude in de zorg, dient ook vastgelegd te zijn welke categorie medewerkers het Waarschuwingregister kan raadplegen. Dit kunnen namelijk alleen medewerkers zijn voor wie het raadplegen van het Waarschuwingregister noodzakelijk is voor de uitvoering van hun taak, bijvoorbeeld bij de inkoop van zorg. De beveiliging van het BSN verdient daarbij bijzondere aandacht. Van de betrokken instanties mogen namelijk alleen gemeenten dit gegeven in het kader van dit onderdeel van de wet verwerken.

De genoemde maatregelen staan voor een passend niveau van beveiliging ten aanzien van alle gegevens die in het Waarschuwingregister worden verwerkt, waaronder ook persoonsgegevens van strafrechtelijke aard kunnen vallen.

### 3.5 Termijnen van verstrekken van gegevens, bewaartermijnen en verwijderen van gegevens

#### Termijnen van registreren en bewaren

In artikel 2.5 van dit besluit zijn op grond van artikel 2.8, tweede lid, onderdeel b, van de wet regels gesteld met betrekking de bewaartermijn en de periode dat gegevens verstrekt kunnen worden. Als uitgangspunt daarbij is genomen artikel 5, eerste lid, onder e, AVG, waarin is bepaald dat persoonsgegevens niet langer worden bewaard dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.

Vanaf het moment van verstrekking, zoals in het Waarschuwingregister, zijn gegevens gedurende een termijn van vier jaar raadpleegbaar. In uitzonderlijke gevallen, omdat zwaarwegende omstandigheden dat noodzakelijk maken, kan een termijn van maximaal acht jaar worden toegepast. Er is voor twee termijnen gekozen, teneinde zoveel mogelijk rechtsgelijkheid, rechtszekerheid en uniformiteit te bereiken voor betrokken partijen en toch een mogelijkheid tot differentiatie in de te hanteren termijn te bieden aan betrokken instanties.

De afweging tussen het met de verwerking van gegevens te bereiken doelen, de inbreuk die met die verwerking wordt gemaakt op de privacy van betrokkene en de mogelijke gevolgen daarvan voor die betrokkene, ligt ook ten grondslag aan de gestelde termijnen. Als uitgangspunt is een termijn van vier jaar gesteld. De duur van deze termijn is bepaald op basis van de ervaring en behoefte van betrokken instanties, onder andere met het EVR van financiële instellingen. Teneinde met de registratie (de waarschuwing) het met de wet beoogde doel te bereiken, is de gestelde termijn noodzakelijk. Gelet op het zwaarwegende algemeen belang bij dat doel, de bestrijding van fraude in de zorg, is die termijn ook proportioneel. Als uitzondering is een termijn van maximaal acht jaar mogelijk. Die termijn kan noodzakelijk en proportioneel zijn gelet op de concrete omstandigheden van het geval.

Of de termijn van maximaal acht jaar in een bepaald geval kan worden toegepast, moet door de verstreckende instantie worden bepaald op basis van het in het protocol op te

nemen criterium, waarbij noodzakelijkheid en proportionaliteit belangrijke aspecten zijn. Bij het formuleren van het criterium worden aspecten betrokken zoals het betrokken financieel belang en verzwarende dan wel verzachtende omstandigheden. Verzwarende omstandigheden kunnen bijvoorbeeld zijn recidive, voortgezette handeling, bedreiging, stelselmatigheid, mate van georganiseerdheid, samenspanning. Ook het blijven ontkennen en het niet meewerken kunnen verzwarende omstandigheden vormen. Daarnaast kan gedacht worden aan omstandigheden als het aantal gemeenten, zorgverzekeraars of zorgbehoevenden dat door de fraude is geraakt, of de gezondheid van zorgbehoevenden in gevaar gekomen is en of sprake is van een schending van de beroepsintegriteit. Bij verzachtende omstandigheden kan bijvoorbeeld een rol spelen dat de fraude plaatsvond onder druk van derden. Ook het direct bekennen van (betrokkenheid bij) fraude in de zorg en het meewerken aan het fraudeonderzoek kunnen hierbij in overweging genomen worden. Indien de termijn van acht jaar wordt toegepast, behoeft dit passende waarborgen en maatregelen voor betrokkene(n). Daarbij wordt periodiek een toets gedaan na het verstrijken van de eerste vier jaar en waarbij steeds wordt beoordeeld of het toepassen van de termijn van acht jaar nog steeds noodzakelijk is of dat met een kortere termijn kan worden volstaan.

Als een instantie in de relatie met een partij op eigen gronden een gerechtvaardigde overtuiging van fraude in de zorg heeft jegens een partij die reeds door een andere instantie in het Waarschuwingregister is opgenomen, dan kan deze instantie eveneens tot registratie overgaan mits aan de daarvoor geldende voorwaarden wordt voldaan. Het feit dat de betreffende partij reeds is geregistreerd, wordt betrokken bij de afweging of de 'nieuwe' registratie noodzakelijk is. Voor een 'nieuwe' registratie geldt een eigen termijn van vier of (maximaal) acht jaar. Bij het bepalen van die termijn wordt een andere registratie van de betreffende partij in de afweging meegenomen. In het protocol komen deze aspecten en hoe daarmee om gegaan wordt, terug.

Gedurende de verstrekking van de gegevens, dat is bijvoorbeeld de periode waarin de gegevens in het Waarschuwingregister zijn geregistreerd en raadpleegbaar zijn, worden deze gegevens bewaard door de verstrekende instantie. De bewijsstukken waarover een verstrekende instantie beschikt en die ten grondslag liggen aan de gerechtvaardigde overtuiging van fraude, moeten gedurende deze periode ook door die instantie worden bewaard. Dit is noodzakelijk om bij de uitoefening van rechten door betrokkenen en in het geval van juridische procedures, inzicht te kunnen geven in de gemaakte afweging en onderbouwing van de verstrekking.

Zoals hierna wordt toegelicht, moet de verstrekking van de gegevens worden beëindigd na afloop van de daarvoor geldende termijn. Dat betekent dat bijvoorbeeld in het Waarschuwingregister geregistreeerde gegevens moeten worden verwijderd en die gegevens zijn dan niet langer raadpleegbaar. De verstrekende instantie bewaart nog wel die gegevens, die noodzakelijk zouden zijn om (eventueel achteraf) de rechtmatigheid van de verwerkingen te kunnen aantonen. De daarvoor geldende bewaartermijn hangt af van de termijnen waarbinnen nog rechtsmiddelen tegen de verwerking van de gegevens open staan.

Of instanties na beëindiging van verstrekking en de verwijdering van gegevens (nog anderszins) een grondslag hebben de gegevens te verwerken en bewaren, is afhankelijk van andere voor hen geldende wet- en regelgeving. In de wet- en regelgeving die specifiek voor de betreffende instantie geldt in relatie tot de wettelijke taak en rol die het uitoefent in het kader van bestrijding van fraude in de zorg, kan zijn geregeld of en gedurende welke termijn die instantie de geraadpleegde gegevens mag bewaren. Dit wordt inzichtelijk gemaakt in het protocol.

## Verwijdering

De betrokken instantie die gegevens aan andere instanties verstrekt, is verantwoordelijk voor die verwerking van gegevens. Die instantie is dan ook verantwoordelijk voor de beëindiging van de verstrekking van die gegevens door middel van verwijdering van de gegevens uit het voor die verstrekking gebruikte systeem zoals het Waarschuwingsregister. In het protocol worden procedurevoorschriften ten aanzien van de verwijdering van gegevens opgenomen.

Er zijn diverse gronden voor verwijdering. Indien ten aanzien van een partij, van wie de gegevens zijn verstrekt, niet langer de gerechtvaardigde overtuiging bestaat dat deze fraude heeft gepleegd, moet de verwerking van die gegevens ingevolge artikel 2.1, vierde lid, van de wet worden beëindigd en de gegevens moeten op dat moment verwijderd worden. Dit kan zich bijvoorbeeld voordoen indien nieuwe informatie beschikbaar is gekomen. Gedacht kan worden aan een periodieke toets op verstrekte gegevens door de verstrekke instantie. Ook kan aanleiding bestaan tot verwijdering van (een deel van) de gegevens, in het geval een betrokkene een beroep doet op het recht op verwijdering. Het recht daartoe is opgenomen in artikel 17 AVG, maar is het tevens van belang voor andere gegevens die in dit kader worden verwerkt. Ten aanzien daarvan zijn geen nadere regels in dit besluit opgenomen, anders dan wat betreft de mogelijkheid voor betrokkenen de rechten uit te kunnen oefenen. Tot slot moeten de gegevens uiterlijk na afloop van de toegepaste termijn worden verwijderd uit het centrale registratiesysteem.

Na verwijdering is uitsluitend voor de betrokken instantie die de gegevens heeft verstrekt zichtbaar dat de registratie uit het Waarschuwingsregister is verwijderd. Dit is noodzakelijk om in juridische procedures te kunnen aantonen dat de verstrekking daadwerkelijk is verwijderd. Voor andere instanties is niets meer van de verwijderde registratie te zien.

### 3.6 Uitoefening van de rechten van betrokkenen

Nationaalrechtelijk zijn de rechtsbeschermingsbepalingen uit de AVG uitgewerkt en ingevuld in paragraaf 3.3 UAVG. Waar nodig in het kader van de wet, zijn deze regels in onderhavig besluit nader uitgewerkt of ingevuld. In dit besluit is bepaald dat voor het geval dat niet-persoonsgegevens worden verwerkt, bijvoorbeeld op rechtspersonen betrekking hebbende gegevens, vergelijkbare rechten gelden. Het gaat bijvoorbeeld om het recht op inzage van gegevens of het recht op verwijdering van gegevens. Dat is nodig gelet op de (mogelijke) gevolgen die ook de verwerking van die gegevens, niet zijnde persoonsgegevens, kan hebben voor betrokkene(n). Ook voor het geval dat de gegevensverwerking niet om persoonsgegevens gaat, moet derhalve zijn geregeld tot wie een betrokkene zich kan wenden om zijn rechten te effectueren of bij een geschil over de juistheid of rechtmatigheid van de verwerking van die gegevens. Hoe betrokken instanties de mogelijkheid tot het uitoefenen van de rechten van betrokkenen (verder) regelen en invullen, wordt opgenomen in het protocol. Daarbij wordt ook ingegaan op de verdeling van (verwerkings)verantwoordelijkheden.

Uitgangspunt is dat de verstrekke instantie het aanspreekpunt is voor de betrokken partij wiens gegevens het betreft. Dit betekent dat de verstrekke instantie de uitvoering van de rechten van de betrokken partij ten aanzien van die verwerking faciliteert. Het is dan ook noodzakelijk te regelen dat het voor een betrokken partij, van wie gegevens worden verwerkt, duidelijk is bij wie het terecht kan voor het uitoefenen van zijn rechten. Indien een partij zich bij de 'verkeerde' instantie meldt, zal die partij naar de verantwoordelijke instantie doorverwezen moeten worden.

Naast de mogelijkheid om op grond van artikel 77 AVG een klacht in te dienen bij de AP, moet door instanties zijn voorzien in effectieve en kenbare processen voor de effectuering

van de rechten van betrokkenen. Daarbij is een belangrijke rol voor de FG weggelegd. Er moet een vergelijkbaar niveau van bescherming zijn geboden voor de gevallen waarin het om andere gegevens dan persoonsgegevens gaat.

Als sprake is van de verwerking van gegevens, informeert de verwerkingsverantwoordelijke betrokken instantie de betrokkene wiens gegevens het betreft conform artikel 14 AVG over die verwerking. Van het informeren kan in uitzonderingsgevallen worden afgezien, indien sprake is van een situatie als bedoeld in artikel 14, vijfde lid, AVG. Daarbij kan het gaan om de situatie dat de bedoelde verplichting de verwezenlijking van de doeleinden van die verwerking, te weten bestrijding van fraude in de zorg, onmogelijk dreigt te maken. Teneinde de mogelijke nadelige gevolgen voor de betrokken partij te beperken, zijn passende maatregelen vereist. Het geheel aan voorwaarden en maatregelen in dit besluit voorziet daar in zijn algemeenheid in. Wat betreft de hier genoemde uitzondering op de informatieplicht wordt in het protocol nader geregeld wanneer en op welke wijze van de uitzonderingsmogelijkheid gebruik wordt gemaakt en met welke maatregelen de mogelijke gevolgen daarvan voor betrokkene worden beperkt. Zo moet mogelijk worden gemaakt dat een betrokken partij ook bij toepassing van de uitzondering toch zo spoedig mogelijk wordt geïnformeerd.

### 3.7 Verantwoordelijkheid en samenwerking

Voor de verwerking van gegevens als bedoeld in het eerste onderdeel van de wet, zijn instanties ieder voor zich verantwoordelijk. Dat betekent dat de instantie die gegevens aan andere instanties verstrekt, zoals door registratie in een centraal registratiesysteem als het Waarschuwingsregister, verantwoordelijk is voor die verwerking. Een instantie die de gegevens vervolgens raadpleegt, is verantwoordelijk voor die verwerking. Indien het hier de verwerking van persoonsgegevens betreft, zijn de instanties verwerkingsverantwoordelijke zoals bedoeld in de AVG. Betrokken instanties, gemeenten en ziektekostenverzekeraars, zijn gezamenlijk verantwoordelijk, voor de werking, inrichting, beveiliging en het beheer van dat Waarschuwingsregister. Voor zover het hier de verwerking van persoonsgegevens betreft, gaat het om gezamenlijke verwerkingsverantwoordelijke als bedoeld in artikel 26 AVG.

In het protocol worden de respectieve verantwoordelijkheden voor de naleving van de wet- en regelgeving opgenomen en wordt inzichtelijk zijn gemaakt wat de rollen van en verhoudingen tussen de verantwoordelijken, verwerkers en betrokken instanties zijn. In dat kader worden bijvoorbeeld ook afspraken ten aanzien van aansprakelijkheid en het recht op schadevergoeding, bijvoorbeeld bij inbreuk op de AVG als bedoeld in artikel 82, zijn opgenomen.

Conform artikel 30 AVG nemen gemeenten en ziektekostenverzekeraars de verwerkingen van persoonsgegevens op in hun register van verwerkingen en verwijzen daarbij naar de instanties die bij de gezamenlijke verwerking betrokken zijn. In het protocol wordt bijvoorbeeld ten aanzien van rechtspersonen van wie gegevens worden verwerkt een soortgelijke waarborg opgenomen voor de verwerking van gegevens, niet zijnde persoonsgegevens. Wanneer de gemeenten en ziektekostenverzekeraars ten behoeve van de inrichting en het beheer van het Waarschuwingsregister verwerkers of subverwerkers inschakelen, sluiten zij daarmee overeenkomstig de vereisten uit de AVG de benodigde verwerkersovereenkomsten.

## 4. Informatieknooppunt zorgfraude

#### 4.1 Inleiding

In artikel 2.4 van de wet is voorzien in een grondslag voor het uitwisselen van gegevens, waaronder persoonsgegevens, door de in dat artikel genoemde betrokken instanties met het IKZ, die voor een of meerdere van die instanties noodzakelijk zijn voor de bestrijding van fraude in de zorg.<sup>5</sup> De instanties hebben elk een taak in de uitvoering van specifieke wetgeving in het zorgdomein en zijn in bepaalde gevallen verantwoordelijk voor het toezicht op de naleving van die wetgeving en belast met handhaving en opsporing. Door deze samenwerking en gegevensuitwisseling, met een ondersteunende taak voor het IKZ, hebben instanties een betere informatiepositie. Zo worden ze in staat gesteld efficiënter en, mede met het oog op privacy, zorgvuldig te beoordelen of sprake is van fraude in de zorg en die fraude te bestrijden. Het IKZ heeft geen handhavende, toezichhoudende of opsporende functie, taken of bevoegdheden.

Het verstrekken van gegevens door betrokken instanties en het IKZ, maakt onderdeel uit van hetgeen in de praktijk het uitwisselen en verrijken van signalen van fraude in de zorg wordt genoemd. In deze nota van toelichting wordt ook die terminologie uit de praktijk gebruikt. De verstrekking van gegevens door betrokken instanties aan het IKZ vindt plaats op twee te onderscheiden momenten in het proces. Het eerste moment is als een betrokken instantie in een bepaald geval een aanleiding tot vermoeden van fraude in de zorg ('signaal') heeft, dat voor een of meer van de instanties noodzakelijk is voor de bestrijding van fraude in de zorg in het kader van de aan die instanties opgedragen wettelijke taken. Dit wordt in deze toelichting aangeduid als het 'verstrekken van een signaal aan het IKZ'. De ontvangst van een signaal vormt voor het IKZ het startpunt voor de uitvoering van de taak tot het bijeenbrengen van gegevens ten aanzien van dat signaal ('verrijken'). Het IKZ vraagt daarbij onder andere gegevens uit bij betrokken instanties. Dan volgt het tweede moment waarop instanties aan het IKZ gegevens verstrekken en dat wordt in deze toelichting aangeduid als het 'verstrekken van gegevens aan het IKZ in het kader van verrijking'. Het IKZ verstrekt het resultaat van de verrijking ('verrijkt signaal') vervolgens indien en voor zover noodzakelijk aan een of meer geëigende instanties.

Op grond van artikel 2.5 van de wet heeft het IKZ voorts tot taak trends en ontwikkelingen met betrekking tot fraude in de zorg te signaleren en daarover beleidsinformatie en statistische gegevens te ontwikkelen en deze uit eigen beweging of op verzoek aan de Minister voor LZS of betrokken instanties te verstrekken.

In dit besluit is onder andere opgenomen welke gegevens op grond van de wet worden verwerkt. Ook zijn regels gesteld ten aanzien van de inrichting, het beheer en de beveiliging van de elektronische voorzieningen voor de verwerking van gegevens, de beveiliging van gegevens, de bewaartermijnen, de verwijdering van gegevens en de uitoefening van de rechten van betrokkenen. Zij moeten in samenhang met elkaar worden gezien en vormen tezamen de invulling en uitwerking van het kader van voorwaarden, vereisten, maatregelen en waarborgen waarbinnen de verwerking van gegevens in het kader van de wet moet plaatsvinden. Ten aanzien van de verwerking van zowel persoonsgegevens als niet-persoonsgegevens geldt als uitgangspunt dat een gelijkwaardig (hoog) niveau aan waarborgen wordt geboden.

#### 4.2. Verstrekking van een signaal door betrokken instanties aan het IKZ

---

<sup>5</sup> Het gaat om de colleges van burgemeester en wethouders (in de toelichting wordt gesproken over gemeenten), de ziektekostenverzekeraars (waaronder begrepen zorgverzekeraar, zorgkantoor of particuliere ziektekostenverzekeraar), de Inspectie gezondheidszorg en Jeugd (IGJ), de Nederlandse Zorgautoriteit (NZa), het Centrum Indicatiestelling zorg (CIZ), de Sociale Verzekeringsbank (SVB), de Nederlandse arbeidsinspectie (NLA), de rijksbelastingdienst, waaronder de Fiscale inlichtingen- en opsporingsdienst (FIOD).

#### 4.2.1 Algemeen

Het risico op een onjuiste of onzorgvuldige verstrekking van signalen door instanties aan het IKZ moet zoveel mogelijk worden beperkt. Niet alleen vanwege het voldoen aan wet- en regelgeving of de (mogelijke) gevolgen van een verstrekking van gegevens voor een betrokkene, maar ook omdat betrokken instanties en het IKZ gebaat zijn bij 'goede' signalen. Zo wordt onnodige administratieve belasting voorkomen en draagt de met de wet mogelijk gemaakte gegevensuitwisseling optimaal bij aan een efficiënte doch zorgvuldige samenwerking door betrokken instanties ten behoeve van bestrijding van fraude in de zorg. Op grond van artikel 2.8, eerste lid, onderdelen b en c, van de wet zijn in dit besluit regels ten aanzien van het afwegingsproces opgenomen en is ingekaderd wanneer er aanleiding is op grond van de wet gegevens aan het IKZ te verstrekken, in welke gevallen dat wordt gedaan en onder welke voorwaarden. Daarbij kan niet worden ontkomen aan een zekere abstractie. Het is niet alleen onmogelijk, maar gelet op de praktische uitvoerbaarheid ook ongewenst deze aspecten van de afweging concreet en tot in detail te omschrijven en te regelen. Er worden handvatten geboden zodat voor instanties duidelijk is hoe vorenstaande afwegingen moeten worden gemaakt en op welke wijze het uitvoeringsproces moet worden ingericht. Dat draagt ook bij aan transparantie voor partijen die hiermee te maken krijgen.

#### 4.2.2 Aanleiding tot, gevallen waarin en voorwaarden waaronder

##### *Aanleiding tot een vermoeden van fraude in de zorg (signaal)*

Voor verstrekking van gegevens aan het IKZ is vereist dat sprake is van een 'aanleiding tot een vermoeden van fraude in de zorg' oftewel een signaal. Met die aanduiding wordt de situatie bedoeld dat er feiten en omstandigheden zijn die erop kunnen wijzen dat fraude is of wordt gepleegd. Het begrip 'vermoeden' heeft in het kader van de wet en dit besluit de definitie die het in normale spraakgebruik heeft. Het moet in dit kader dan ook niet worden ingevuld volgens de normen die in de context van het strafrecht bepalend zijn voor de invulling van 'een redelijk vermoeden van schuld' aan een strafbaar feit.

Er zijn veel (verschijnings)vormen van signalen. Het kan bijvoorbeeld gaan om declaratiegedrag van een partij, het door een partij behaalde resultaat (dat bijvoorbeeld opvallend hoog is) of de wijze waarop het zorggeld door een partij is besteed. Deze gegevens kunnen blijken uit een enkele factuur, jaarrekening of melding. Deze gegevens zijn op zichzelf echter onvoldoende om conclusies aan te kunnen verbinden. Of daadwerkelijk sprake is van een vermoeden van fraude in de zorg, hetgeen nog een stap verder is dan de aanleiding tot dat vermoeden, is dan nog onduidelijk. Laat staan dat vastgesteld kan worden dat sprake is van fraude in de zorg. Afgewogen moet zijn of de beschikbare gegevens voldoende duidelijk en geloofwaardig zijn en of die daadwerkelijk een aanleiding tot een vermoeden van fraude in de zorg vormen.

##### *Gevallen waarin signalen aan het IKZ worden verstrekt*

Indien een betrokken instantie tot het oordeel komt dat sprake is van een signaal, dan moet het vervolgens afwegen of het ten behoeve van een of meerdere van de betrokken instanties noodzakelijk is dat gegevens aan het IKZ worden verstrekt. De betreffende instantie weegt daarbij ook af of de verstrekking voor de eigen organisatie noodzakelijk is. Er is sprake van een noodzaak als de fraude in de zorg zonder de gegevensverstrekking aan het IKZ niet dan wel onvoldoende efficiënt, zorgvuldig en op de praktijk gericht kan plaatsvinden.

Om de noodzaak te kunnen beoordelen, moeten instanties inzicht hebben in voor wie van de betrokken instanties, wanneer, welke gegevens uit de in dit besluit aangewezen gegevens noodzakelijk zijn. Dat is ook nodig omdat moet worden afgewogen of een signaal kan worden verstrekt zonder of met minder gegevens. Wanneer het signaal in dit



besluit aangewezen gegevens bevat die niet nodig zijn voor de verdere behandeling ervan, dan mogen deze gegevens niet worden verstrekt.

#### Voorbeelden

Grofweg kunnen de volgende gevallen zich voordoen.

Als een instantie ten aanzien van een signaal niet over voldoende gegevens beschikt en niet of onvoldoende actie kan ondernemen in het kader van diens wettelijke taak in de zorg, dan ligt gegevensverstrekking aan het IKZ voor de hand. Voor een efficiënte en zorgvuldige op de praktijk gerichte bestrijding van fraude in de zorg, is het voor de verstrekende instantie en al dan niet (een van) de andere betrokken instanties noodzakelijk dat de gegevens aan het IKZ worden verstrekt en dat verrijking van het signaal plaatsvindt. De samenwerking en gegevensuitwisseling met het IKZ verbetert de informatiepositie van de instantie die het verrijkte signaal vervolgens ontvangt. Dit is de situatie waarop de wet hoofdzakelijk is gericht.

*Hierbij gaat het bijvoorbeeld om de situatie van een zorgaanbieder waarvan bekend is dat deze actief is in meerdere gemeenten en in meerdere domeinen in de zorg. Er zijn signalen, maar er is samenwerking tussen instanties en samenvoeging van informatie noodzakelijk teneinde duidelijkheid te krijgen en indien nodig actie tegen de fraude te ondernemen. De verschillende 'puzzelstukjes' worden dan (mede) door uitwisseling van gegevens met het IKZ bij elkaar gebracht. Het gaat dan bijvoorbeeld om gegevens die bekend zijn bij andere gemeenten waarin de zorgaanbieder actief is of gegevens van die andere betrokken instanties, zoals de rijksbelastingdienst of de NLA, van die aanbieder hebben.*

*Het is overigens ook goed mogelijk dat de instantie die het signaal verstrekt, gelet op het gebrek aan informatie niet weet of een partij ook in andere gemeenten of domeinen actief is en dat samenwerking en gegevensuitwisseling met ondersteuning van het IKZ juist gelet daarop noodzakelijk is.*

Als een betrokken instantie ten aanzien van het signaal waarvan het kennis heeft genomen over voldoende gegevens beschikt teneinde uitvoering te kunnen geven aan diens wettelijke taak in de zorg en de rol die het daarbij heeft ten aanzien van het signaal en er zijn geen aanknopingspunten dat de gegevens voor andere betrokken instanties noodzakelijk zijn voor de bestrijding van fraude in de zorg, dan is het uitgangspunt dat gegevensverstrekking door die instantie aan het IKZ niet noodzakelijk is en niet plaatsvindt.

*Hierbij kan gedacht worden aan een signaal over een zorgaanbieder waarvan het bekend is dat het een kleine partij is, die in alleen een specifieke gemeente en in een specifiek domein actief is, en waarover voldoende informatie beschikbaar is bij die gemeente om een vervolg te geven aan het signaal (fraudeonderzoek, handhaving, etc.). De informatiepositie van de betreffende instantie is in dit geval voldoende en de instantie oordeelt op dat moment dat samenwerking met andere betrokken instanties, en de ondersteunende taak van het IKZ in dat kader, niet noodzakelijk is. Het is overigens mogelijk dat de verstrekking van de gegevens in een dergelijk geval wel noodzakelijk blijkt te zijn voor een van de andere betrokken instanties. Dat wordt duidelijk doordat een of meer van die instanties wel een signaal over de zorgaanbieder heeft verstrekt aan het IKZ. Door de instantie die zelf heeft afgezien van het verstrekken van het signaal, kunnen de gegevens dan alsnog worden verstrekt naar aanleiding van de gegevensuitvraag*

*die het IKZ in het kader van verrijking van het door andere instantie(s) ingediende signaal doet.*

Het enkele feit dat een instantie zelf actie op signalen kan of gaat ondernemen of heeft ondernomen, hoeft echter niet in de weg te staan aan het verstrekken van deze signalen aan het IKZ. In het geval dat gegevens ook voor andere betrokken instanties noodzakelijk zijn voor de bestrijding van fraude in de zorg in het kader van de aan die instanties opgedragen wettelijke taken, moet verstrekking ervan aan het IKZ plaatsvinden.

*Het is goed mogelijk dat een instantie voldoende informatie beschikbaar heeft om vervolg te geven aan een signaal, maar dat bekend is dat de partij die het betreft ook in andere gemeenten of andere domeinen binnen de zorg actief is en ook andere betrokken instanties met deze partij te maken hebben. In die situatie kan het voor die instanties noodzakelijk zijn dat het signaal ter verrijking aan het IKZ wordt verstrekt, zodat zij na ontvangst van het verrijkte signaal een betere informatiepositie hebben.*

#### *Voorwaarden*

Door elke betrokken instantie moet een proces zijn ingericht om de hiervoor beschreven afweging of sprake is van een signaal en tot het al dan niet verstrekken ervan aan het IKZ zorgvuldig te kunnen maken. Bij het maken van de afweging moeten heldere, objectieve en uniforme criteria worden gehanteerd en vastgelegd moet zijn op basis waarvan een afweging is gemaakt en waarom. Daarbij moet ingegaan worden op elementen van fraude in de zorg, zoals opzet, misleidend handelen binnen het zorgdomein en dat met eigen of andermans gewin als oogmerk. Ook moeten indicatoren, (bewijs)stukken en aanwijzingen worden gebruikt. Welke dat zijn moet bijvoorbeeld worden bepaald op basis van in de praktijk opgedane kennis en ervaring. Onder andere conclusies uit benchmarkgegevens kunnen een belangrijke bijdrage leveren aan het maken van een zorgvuldige beoordeling en afweging. In acht wordt genomen dat juist in deze fase nog gegevens ontbreken en aspecten onduidelijk zijn. Dat doet er niet aan af dat gewaarborgd wordt dat de gebruikte gegevens juist zijn. De specifieke taak en rol van een betrokken instantie en de (aard van de) gegevens waarover die instantie gelet daarop beschikt, vormen de context waarbinnen de afweging wordt gemaakt en het proces wordt ingericht. Zo beschikt de Sociale verzekeringsbank (hierna: SVB) bijvoorbeeld voor de uitvoering van haar taken alleen over de gegevens voor het uitvoeren van het trekkingsrecht. De SVB kan derhalve enkel die gegevens betrekken in de afweging of sprake is van een signaal en tot het al dan niet verstrekken ervan aan het IKZ. Tot slot moet in de inrichting van het proces de mogelijkheid openblijven dat kan worden bijgestuurd op (nieuwe) ontwikkelingen in de praktijk.

Hoewel de inrichting van het proces aan elk van de betrokken instanties zelf is, is afstemming onderling en met het IKZ nodig gelet op de samenwerking in dit proces specifiek en in de keten in het algemeen. De processen en gemaakte afspraken moeten worden vastgelegd, bijvoorbeeld in werkinstructies. Het is goed denkbaar dat bij die afspraken ook andere aspecten worden meegenomen, bijvoorbeeld met betrekking tot de termijn waarbinnen de afweging moet zijn gemaakt en een signaal wordt verstrekt aan het IKZ.

Hoewel de AP ingevolge de UAVG formeel toezichthouder is op de verwerking van persoonsgegevens, zijn de betrokken instanties elk zelf verantwoordelijk voor intern toezicht op de juiste en zorgvuldige verwerking van gegevens in het kader van de wet. Derhalve is voorgeschreven dat elke instantie daartoe een proces heeft ingericht. Als het

de verwerking van persoonsgegevens betreft, is daarbij op grond van de AVG een belangrijke rol weggelegd voor de FG van de betrokken instanties.

Voor de verstrekking van politiegegevens door de NLA en FIOD aan het IKZ geldt tot slot de voorwaarde dat dit op grond van en in overeenstemming met de Wpg plaatsvindt.

#### 4.2.3 Wijze van verstrekken aan het IKZ

In dit besluit zijn op grond van artikel 2.8, eerste lid, onderdeel a, van de wet regels gesteld met betrekking tot de wijze waarop gegevens door de betrokken instanties worden verstrekt aan het IKZ. Het gaat zowel om het verstrekken van signalen als om het in het kader van verrijking op uitvraag van het IKZ verstrekken van gegevens. Ten behoeve van efficiëntie en het voorzien in waarborgen en beveiliging is in artikel 3.23 van dit besluit voorgeschreven dat de verstrekking, net als overige verwerkingen op grond van dit onderdeel van de wet, elektronisch geschiedt. De systemen van instanties moeten daartoe dan ook zijn aangesloten op de elektronische voorzieningen van het IKZ. Daarbij kan gedacht worden aan een systeem waarbij gebruik wordt gemaakt van een portaalfunctie, waarin bestanden en berichten kunnen worden geüpload en gedownload, of een berichtenverkeerfunctie, waarbij sprake is van geïntegreerd berichtenverkeer in het systeem.

De rijksbelastingdienst heeft geen specifieke taak in het zorgdomein. De rijksbelastingdienst houdt echter wel toezicht op de naleving van fiscale wet- en regelgeving door partijen in het zorgdomein. Voor de uitvoering van haar taken beschikt de rijksbelastingdienst over een grote hoeveelheid vertrouwelijke en privacygevoelige gegevens. Om ervoor te zorgen dat belastingplichtigen bereid zijn deze gegevens aan de rijksbelastingdienst te verstrekken, geldt voor de rijksbelastingdienst de strikte geheimhoudingsplicht uit artikel 67 AWR. Deze geheimhoudingsplicht wordt in de wet doorbroken ten behoeve van de verstrekking van de in dit besluit genoemde noodzakelijke gegevens in het kader van de bestrijding van fraude in de zorg. De rijksbelastingdienst wordt niet verplicht via een geautomatiseerde koppeling gegevens aan het IKZ te verstrekken. Regels ten aanzien van de elektronische verstrekking van gegevens door de rijksbelastingdienst aan het IKZ worden opgenomen in een ministeriële regeling.

### 4.3 Verrijkingproces IKZ

#### 4.3.1 Algemeen

Alleen naar aanleiding van een van betrokken instanties ontvangen signaal start het IKZ met het bijeenbrengen van gegevens ten aanzien van dat signaal. Welke gegevens het IKZ kan uitvragen bij de andere betrokken instanties, is met name ingekaderd door de randvoorwaarden in artikel 3.15 van dit besluit en de in artikelen 3.1 tot en met 3.9 van dit besluit aangewezen gegevens. Het IKZ beoordeelt welke van deze gegevens voor de verrijking van een signaal noodzakelijk zijn met het oog op de bestrijding van de betreffende vorm van fraude. Bij het maken van die afweging wordt voortgebouwd op de afweging die de instantie heeft gemaakt bij het verstrekken van het signaal aan het IKZ. Ook in het verrijkingproces is het essentieel dat het wordt gedaan op basis van heldere, objectieve en uniforme criteria en indicatoren, (bewijs)stukken en aanwijzingen. Ervaring en kennis uit de praktijk zijn daarvoor leidend en bijvoorbeeld de conclusies uit benchmarkgegevens kunnen ook hier een belangrijke rol spelen. In acht moet worden genomen dat kan worden bijgestuurd op (nieuwe) ontwikkelingen in de praktijk.

In artikel 2.4, tweede lid, van de wet is bepaald welke andere dan de van instanties ontvangen gegevens het IKZ ten behoeve van het verrijkingproces kan gebruiken. Het gaat om gegevens die bij of krachtens enige andere wet zijn verkregen en de in dit besluit

aangewezen openbare gegevens uit het Handelsregister en het Jaardocument Maatschappelijke Verantwoording (JMV).

Het gebruik en de vastlegging van de aard en herkomst van de te verwerken gegevens moet ingevolge dit besluit zijn geborgd in het verrijgingsproces. Dit is onder andere noodzakelijk voor een goede taakuitoefening van de geëigende instantie aan wie het verrijkte signaal (mogelijk) verstrekt wordt. Het is bijvoorbeeld van belang voor de verantwoording van verrichtingen in het kader van strafrechtelijke vervolging.

Hoewel de inrichting van het verrijgingsproces aan het IKZ is in afstemming met betrokken instanties, is in artikel 3.16 van dit besluit bepaald welke onderdelen daarin in elk geval terug moeten komen. Dat waarborgt dat verwerking van gegevens zorgvuldig plaatsvindt en dat steeds de afweging wordt gemaakt of (verdere) verwerking van de gegevens noodzakelijk is.

Voorgescreven is dat het verrijgingsproces getrapt moet plaatsvinden. Een aantal treden van verrijking die het IKZ bij de inrichting van het verrijgingsproces moet hanteren, is opgenomen in dit besluit. Met het oog op een praktische toepassing is de mogelijkheid voor het IKZ opengelaten in afstemming met betrokken instanties treden toe te voegen of binnen de al dan niet in dit besluit opgenomen treden een nadere onderverdeling aan te brengen.

De eerste trede van verrijking staat in het teken van de beoordeling van de volledigheid en juistheid van een door een betrokken instantie aan het IKZ verstrekt signaal en de beoordeling van de reikwijdte daarvan.

Het eerste element is een van de manieren waarop invulling is gegeven aan het beginsel van privacy by design. Het voorkomt dat onnodig dan wel onjuiste gegevens worden verwerkt, waarmee een onrechtmatige inbreuk op de privacy van een betreffende betrokkene en onnodige uitvoeringslasten voor het IKZ worden voorkomen. Met juistheid wordt hier bedoeld op de identificerende gegevens of administratieve kenmerken van de betrokken partij en niet op de aanleiding tot het vermoeden van fraude in de zorg. Het IKZ doet alleen indien noodzakelijk, ter controle van gegevens, uitvraag van gegevens die in het kader van behandeling van het signaal reeds bij het IKZ bekend zijn. Uitgangspunt bij de uitvraag is ook dat het IKZ gegevens zoveel mogelijk bij de bron ophaalt. Teneinde het verstrekken van juiste informatie door de bevroagde instanties te waarborgen, alsmede ten behoeve van dataminimalisatie, is het mogelijk dat het IKZ de in dat kader noodzakelijke gegevens aan de bevroagde instantie verstrekt. Dit is inherent aan een zorgvuldig proces van gegevensuitwisseling. De bevroagde instanties mogen de in dit kader van het IKZ verkregen gegevens voor geen enkel ander doel gebruiken. In het geval dat de verstrekte gegevens niet juist zijn, deelt het IKZ dat mee aan de verstrekkende instantie. De onjuiste verstrekking komt niet in het systeem dat het IKZ voor verrijking gebruikt. In het geval de verstrekte gegevens onvolledig zijn, wordt de verstrekkende instantie door het IKZ in staat gesteld het signaal aan te vullen. Bij het uitblijven van de aanvulling zal het signaal eveneens niet in het voor verrijking gebruikte systeem terecht komen en worden verwijderd. De inrichting van het systeem, waarover meer in de volgende paragraaf, moet zo zijn vormgegeven dat het risico op onvolledige of onjuiste gegevens tot het minimum is beperkt. Indien een signaal vanwege voornoemde redenen niet door het IKZ is geaccepteerd, kan een instantie het signaal opnieuw indienen met de volledige en juiste gegevens.

Het tweede element, de reikwijdte van het signaal, betreft het domein waarop het signaal betrekking heeft en voor welk van de betrokken instanties (mogelijk) een rol is weggelegd. Dit wordt gezien als de eerste noodzakelijk stap in het bepalen van het vervolg van het verrijgingsproces. Is al op voorhand duidelijk binnen welk domein of welke domeinen een signaal zich afspeelt, dan kan aan de hand daarvan bepaald worden

bij welke instanties gegevens voor de verrijking van het signaal moet worden uitgevraagd. Wanneer een signaal zich bijvoorbeeld uitsluitend binnen het domein van de Zorgverzekeringswet (Zvw) afspeelt, ligt het voor de hand te starten met gegevens van de zorgverzekeraars en mogelijk van de NZa. Een dergelijk signaal geeft geen aanleiding om gegevens van gemeenten bij de verrijking te betrekken. Dat doet overigens niet af aan de mogelijkheid dat in een concreet geval, al dan niet gedurende het vervolg van het verrijkingproces, de noodzaak bestaat te verrijken met gegevens uit andere domeinen.

Bij de volgende trede gaat het IKZ na of ten aanzien van dat signaal reeds andere signalen bij het IKZ bekend zijn. Indien dat het geval is, kunnen signalen en de gegevens die daar onderdeel van uitmaken vervolgens bijeengebracht worden en gezamenlijk verder worden verwerkt. In een werkproces moet zijn vastgelegd wanneer signalen wel of niet gezamenlijk verder worden behandeld.

Pas als na de eerste verrijking blijkt dat noodzaak bestaat tot verrijking met de gevoelige gegevens, waaronder worden verstaan politiegegevens, gegevens over de gezondheid, persoonsgegevens van strafrechtelijke aard en fiscale gegevens, kan verrijking met deze gegevens plaatsvinden. Met het voorschrijven van deze trede wordt extra gewaarborgd dat de deze gegevens, gelet op hun aard, niet worden verwerkt in een te vroeg stadium van verrijking.

Door het IKZ moet, in afstemming met betrokken instanties, zijn vastgelegd op basis waarvan de stap naar een volgende trede in het verrijkingproces wordt genomen. Er moeten in dat kader beoordelingscriteria zijn geformuleerd, die gelet op de veranderlijke praktijk niet limitatief zijn en waarbij ook niet limitatief gedifferentieerd wordt op (groepen van) soorten gevallen. De hiervoor bij de voorgeschreven treden genoemde elementen, het domein waarop het signaal betrekking heeft en de gevoeligheid van bepaalde gegevens, kunnen ook worden gebruikt bij de verdere inrichting van het verrijkingproces. Andere elementen die hierbij kunnen worden betrokken zijn bijvoorbeeld het soort signaal en de vorm van fraude. Ook kan gedacht worden aan verrijking op basis van hoe belangrijk indicatoren zijn voor het onderbouwen van een vermoeden van fraude. Daarbij wordt dan begonnen met de belangrijkste, zodat op basis van die specifieke verwerking mogelijk al kan worden afgewogen of de verrijking moet worden voortgezet. Tot slot moet getrapte verrijking niet uitsluiten dat door het IKZ in verschillende treden andere gegevens bij eenzelfde instantie worden uitgevraagd.

#### 4.3.2 Wijze van verwerking door het IKZ

In dit besluit zijn ook nadere regels opgenomen ten aanzien van de wijze van verwerking van gegevens door het IKZ. Deze verwerking geschiedt, in aansluiting op de wijze van verstrekken van signalen door instanties aan het IKZ, elektronisch in de daartoe ingerichte voorzieningen van het IKZ. Zoals hiervoor aan de orde kwam, kan worden gedacht aan een systeem waarbij gebruik wordt gemaakt van een portaalfunctie of een berichtenverkeerfunctie. Het systeem van het IKZ waarin gegevens worden verwerkt in het kader van verrijking van signalen, wordt in deze toelichting aangeduid als het zaaksinformatiesysteem.

Het uitgangspunt is dat noodzakelijke gegevens in de fase van verrijking via een koppeling met de betrokken instanties, mits beschikbaar, elektronisch en automatisch aan het signaal worden toegevoegd. Het IKZ en de betrokken instanties hebben een inspanningsverplichting om naar deze beoogde situatie toe te werken. In een ministeriële regeling worden resultaatsverplichtingen opgenomen ten aanzien van de minimaal geldende normen en afspraken ten aanzien van de wijze van verwerking. Indien ontwikkelingen daar aanleiding toe geven, wordt de ministeriële regeling daarop aangepast. De verwerking van de persoonsgegevens door het IKZ in het kader van

verrijking vindt overigens niet uitsluitend geautomatiseerd plaats. Het deel dat is geautomatiseerd, betreft het (trapsgewijs) ophalen en bijeenbrengen van de gegevens. Menselijke tussenkomst is nodig op de momenten dat de verwerking van gegevens in de verschillende treden in het proces wordt getoetst aan de daarvoor geldende voorwaarden. Indien niet wordt voldaan aan die voorwaarden, vindt geen verdere verwerking plaats. Er is dan ook nooit sprake van een uitsluitend op geautomatiseerde verwerking gebaseerd besluit, zoals bedoeld in artikel 22 AVG. In het kader van dataminimalisatie kan bij de inrichting van het systeem gedacht worden aan een 'hit – no hit' systeem, waarbij voorafgaand aan de uitvraag van gegevens bij betrokken instanties eerst wordt nagegaan of over de gegevens van betrokkene wordt beschikt.

Voor het in het kader van verrijking raadplegen van de daartoe in de wet aangewezen bronnen, gebruiken de daartoe bevoegde medewerkers van het IKZ de voor die bronnen beschikbare mogelijkheden. De gegevens worden vervolgens net als de andere gegevens door het IKZ verwerkt in de gebruikte elektronische voorzieningen.

Een uitzondering op het uitgangspunt van geautomatiseerde verrijking geldt voor gegevens van de rijksbelastingdienst. Aanleiding voor dit onderscheid is de van de andere betrokken instanties afwijkende rol van de rijksbelastingdienst binnen het zorgdomein en het afwijkende kader waarbinnen de rijksbelastingdienst over gegevens beschikt. Regels ten aanzien van de elektronische gegevensuitwisseling door de rijksbelastingdienst aan het IKZ in het kader van verrijking worden opgenomen in een ministeriële regeling. Voor de NLA en FIOD geldt de uitzondering dat de verstrekking van politiegegevens aan het IKZ ook in het kader van de verrijking van gegevens plaatsvindt op grond van en met inachtneming van de Wpg.

#### 4.3.3 Overige elementen van inrichting en vormgeving van werkprocessen

Andere elementen die bij de inrichting en vormgeving van de werkprocessen van het IKZ aan de orde moeten komen, betreffen onder andere het resultaat waartoe de verrijking van een signaal moet leiden en het eind van het verrijkingproces. Gedacht kan ook worden aan termijnen waarbinnen bepaalde acties in het verrijkingproces moeten worden ondernomen en hoe het op te leveren 'product' wordt vormgegeven. Wat betreft het eind van het verrijkingproces gaat het er met name om dat het proces zo is ingeregeld dat het tijdig wordt beëindigd zodra niet (langer) aan de voorwaarden voor verrijking wordt voldaan.

#### 4.4 Gegevensset

In de artikelen 3.1 tot en met 3.9 van dit besluit is conform artikel 2.4, eerste lid, van de wet per betrokken instantie aangewezen welke gegevens worden verstrekt. Elk gegeven uit deze gegevensset kan noodzakelijk zijn voor de bestrijding van fraude in de zorg en per geval en per fase van het proces moet worden beoordeeld welk gegeven of welke gegevens uit deze set daadwerkelijk verstrekt of anderszins verwerkt moet(en) worden. Bij het verstrekken van een signaal aan het IKZ, is die beoordeling aan de betreffende betrokken instantie. Bij het verstrekken van gegevens in het kader van verrijking is die beoordeling aan het IKZ. Ten aanzien van dit laatstgenoemde uitgangspunt zijn er twee bijzonderheden. Voor politiegegevens die afkomstig zijn van de BOD's geldt het uitgangspunt niet, omdat die instanties op grond van de Wpg een eigen afweging tot verstrekking van gegevens maken. Daarnaast geldt voor gegevens over afgeronde onderzoeken, dat instanties zelf een afweging maken welke gegevens daaruit op het signaal betrekking hebben en noodzakelijk zijn om te verstrekken. Een instantie verstrekt alleen de gegevens die in de voor die instantie aangewezen gegevensset in dit besluit zijn opgenomen en doet dat alleen indien en voor zover het over de betreffende gegevens beschikt.

Met het aanwijzen van een zo minimaal mogelijke set aan gegevens, waarbinnen vervolgens per geval wordt afgewogen welk van de gegevens in een concreet geval noodzakelijk is, wordt invulling gegeven aan artikel 5, eerste lid, onderdeel c, AVG en het beginsel van privacy by design. Het is niet mogelijk met een beperktere set aan gegevens in dit besluit te volstaan. Elk van de gegevens uit de set kan noodzakelijk zijn voor de bestrijding van fraude in de zorg en door op voorhand de set nog verder te beperken, zou het onderdeel van de wet waarop dit deel van het besluit betrekking heeft niet effectief en zorgvuldig kunnen worden uitgevoerd. De in dit besluit aangewezen identificerende gegevens en administratieve kenmerken zijn bijvoorbeeld noodzakelijk om zorgvuldig vast te stellen over welke natuurlijke persoon of rechtspersoon het signaal gaat. Indien een kleinere set aan gegevens zou worden aangewezen, zou dat leiden tot een (groter) risico op het onnodig of onjuist verwerken van gegevens. De gegevensset is tot stand gekomen in afstemming met betrokken instanties.

In deze paragraaf worden de in dit besluit aangewezen gegevens toegelicht. Per gegeven wordt toegelicht wat daaronder wordt begrepen en waarom het noodzakelijk en proportioneel is dat dit gegeven onderdeel uitmaakt van de gegevensset.

In onderhavig besluit is niet bepaald welke van de aangewezen gegevens uit de set in een bepaald geval verstrekt moeten worden. Het is, afhankelijk van het moment in de procedure, aan een betrokken instantie respectievelijk het IKZ om voor elke specifieke verstrekking of andere gegevensverwerking op grond van de wet de afweging maken of deze past binnen het kader van de wet- en regelgeving en de AVG. Dat betekent dat het van het geval afhankelijk is welke gegevens uit de gegevensset verwerkt worden. De verwerking van specifiek die gegevens in dat geval moet door de betrokken instantie dan wel het IKZ kunnen worden onderbouwd voor wat betreft noodzakelijkheid, proportionaliteit en subsidiariteit.

Gegevens die niet in dit besluit zijn aangewezen, voldoen per definitie niet aan de voorwaarden en mogen op grond van de wet dan ook niet door betrokken instanties worden verstrekt aan het IKZ. Tenzij het andere gegevens betreft als bedoeld in artikel 2.4, tweede lid, van de wet, mogen voornoemde gegevens ook niet door het IKZ worden verwerkt en worden door verstrekt aan de geëigende instantie(s). Dat laat overigens onverlet dat instanties de gegevens die zij verstrekken kunnen toelichten en duiden voor een goed begrip ervan.

Politiegegevens, dat zijn persoonsgegevens die worden verwerkt door de NLA en FIOD, vallen onder de Wpg en gelet daarop geldt voor die gegevens een apart regime. In dit besluit is aangesloten bij de wet- en regelgeving systematiek van de Wpg. Het Bpg is aangepast om verstrekking van politiegegevens aan het IKZ mogelijk te maken. De NLA en FIOD leggen in een werkdocument vast komen welke politiegegevens zij verstrekken aan IKZ. In het besluit is opgenomen welke gegevens van rechtspersonen, niet-politiegegevens, zij aan het IKZ verstrekken.

#### 4.4.1 Het signaal

Een signaal bestaat, afhankelijk van het concrete geval, uit een of meer van de bij dit besluit aangewezen gegevens. Deze gegevens ondersteunen dan wel onderbouwen ten aanzien van een partij in een concreet geval de aanleiding tot het vermoeden van fraude in de zorg.

Het signaal dat instanties aan het IKZ verstrekken of het IKZ na verrijking aan de geëigende instantie(s) verstrekt, moet op basis van de verstrekte gegevens uit de gegevensset een omschrijving bevatten van de aanleiding tot het vermoeden van fraude in de zorg. De samenhang tussen de verschillende verstrekte gegevens wordt daarbij

toegelicht en er wordt ingegaan op de aard van het vermoeden en de elementen van fraude in de zorg, zoals opzet, misleidend handelen binnen het zorgdomein en dat met eigen of andermans gewin als oogmerk. Ook moet de voor verstrekking van het (verrijkte) signaal gemaakte afweging zijn opgenomen. De omschrijving bevat geen gegevens die geen onderdeel uitmaken van de gegevensset.

Bij het verstrekken van een signaal aan het IKZ, verstrekken instanties ook de gegevens uit de gegevensset die het signaal onderbouwen. Het gaat bijvoorbeeld om jaarrekeningen of bepaalde gegevens uit het Handelsregister. Hoewel het IKZ zelfstandig het Handelsregister kan raadplegen met betrekking tot een signaal, is het denkbaar dat instanties bepaalde momentopnamen uit deze bron als onderdeel van het signaal aan het IKZ verstrekken.

Hetgeen instanties moeten verstrekken aan het IKZ in het kader van verrijking, wijkt in zoverre van het vorenstaande af dat enkel en alleen de in die fase van verrijking door het IKZ uitgevraagde gegevens moeten worden verstrekt. Zoals eerder aan de orde kwam, doet het IKZ daarbij alleen indien noodzakelijk ook uitvraag van gegevens die het in het kader van de behandeling van het signaal al heeft en vraagt het slechts die gegevens die de bevraagde instantie op grond van dit besluit verstrekt. Het IKZ kan betrokken instanties in het kader van verrijking vragen of zij ten aanzien van de betreffende partij ook over signalen van fraude in de zorg beschikken. Indien daarvan sprake is, verstrekt een instantie ook hier een omschrijving van de aanleiding tot fraude in de zorg.

#### 4.4.2 Administratieve kenmerken en identificerende gegevens

Onder identificerende gegevens van een natuurlijk persoon worden in dit besluit verstaan naam, adres, woonplaats, geboortedatum, geslacht, BIG-registratienummer, Stichting Kwaliteitsregister Jeugd (SKJ) registratienummer, KvK-nummer in relatie tot een natuurlijk persoon en een door ziektekostenverzekeraars gehanteerd nummer ter identificatie zoals een of meerdere AGB-code(s) die gelieerd worden aan de natuurlijk persoon.

Onder administratieve kenmerken van een rechtspersoon worden in dit besluit verstaan naam, adres en vestigingsplaats, KvK-nummer van de rechtspersoon en het door ziektekostenverzekeraars gehanteerde nummer ter identificatie van de rechtspersoon zoals een of meerdere AGB-code(s).

Met de beschikking over deze gegevens en kenmerken kan het IKZ zorgvuldig en met voldoende zekerheid vaststellen dat het om de juiste (rechts)persoon gaat. Het KvK-nummer stelt het IKZ in staat zelfstandig het Handelsregister te raadplegen. De gegevens zijn ook noodzakelijk voor het praktisch en gericht kunnen inrichten van het werkproces en de systemen van het IKZ. Zo kunnen de gegevens gebruikt worden om de verschillende treden van verrijking zorgvuldig te kunnen uitvoeren. Het combineren van identificerende gegevens en administratieve kenmerken met de hierna genoemde handelsgegevens, is essentieel om bepaalde verbanden en netwerken aan het licht te brengen. Indien noodzakelijk kan een duiding van de relatie tussen verschillende natuurlijke en rechtspersonen die betrokken zijn bij het signaal worden verstrekt. In bepaalde gevallen is het noodzakelijk om de identificerende gegevens van bestuurders van een rechtspersoon te controleren. Dat kan het geval zijn bij een signaal over een partij waarvan een bestuurder betrokken is bij de vermoedelijke fraude. Het IKZ controleert de identificerende gegevens van die bestuurder en daaruit kan bijvoorbeeld ook blijken dat deze al bij een eerder signaal betrokken was.

#### 4.4.3 Handelsgegevens

Onder handelsgegevens worden in dit besluit de volgende gegevens verstaan: omvang van het personeelsbestand, informatie over het cliëntenbestand (het aantal zorgbehoevenden en de locaties waar zij de zorg, hulp of ondersteuning ontvangen),



informatie over dochterondernemingen en concernrelaties en bestuurders. Ook (andere) op grond van de wet voor het IKZ toegankelijke gegevens in het Handelsregister vallen onder het in dit besluit gehanteerde begrip handelsgegevens en kunnen worden verstrekt als dat noodzakelijk is. Dat kan als onderdeel van het signaal, maar bijvoorbeeld ook als gegevens zijn gewijzigd en instanties over de oude gegevens beschikken en het IKZ niet door middel van raadpleging van het Handelsregister de beschikking zou kunnen krijgen over die oude doch, mede gelet daarop, noodzakelijke informatie.

Handelsgegevens zijn noodzakelijk om een inschatting te maken van de aard en omvang van de vermoedelijke fraude waarop het signaal betrekking heeft. De hoeveelheid personeel moet passend zijn bij de hoeveelheid zorgbehoevenden en de hoeveelheid zorg die geleverd wordt. Bijvoorbeeld de jaarrekeningen maken het vervolgens mogelijk om het vorenstaande te kunnen afzetten tegen de financiële gegevens van de betreffende partij.

*Een voorbeeld van een signaal waarbij verwerking van handelsgegevens noodzakelijk kan zijn, betreft een geval waarin de zorgbehoevende zorg ontvangt in Maastricht, terwijl de zorgverlener woonachtig is in Groningen. Om zo'n signaal verder te kunnen onderzoeken is informatie nodig over het werkgebied, waaruit blijkt waar de zorgbehoevende zorg ontvangt, en over het personeelsbestand, waaruit blijkt in welk gebied de zorgverlener woonachtig is. Wanneer deze informatie naast elkaar gelegd wordt, kan zo'n signaal geverifieerd worden.*

#### 4.4.4 Gegevens over het zorgdomein en de soort zorg

Onder gegevens over het zorgdomein en de soort zorg wordt in dit besluit het volgende verstaan: gegevens over het domein waarin de zorgaanbieder zorg levert, dan wel de zorgbehoevende zorg ontvangt, en gegevens over de leveringswijze (dat wil zeggen, als zorg in natura of via een persoonsgebonden budget) en gegevens over de soort zorg die wordt geleverd of ontvangen. Het is noodzakelijk over deze gegevens te beschikken om bijvoorbeeld het proces van verrijken zorgvuldig te kunnen laten plaatsvinden en de meest geëigende instantie(s) te bepalen. Als duidelijk is om welk domein, leveringswijze en soort zorg het gaat, kan gericht met specifiek daarvoor relevante gegevens worden verrijkt. De meest geëigende instantie die het verrijkte signaal verder oppakt, heeft de gegevens op haar beurt nodig om te kunnen onderzoeken of sprake is van een overtreding van relevante wet- en regelgeving.

In het geval van verstrekking van gegevens van een zorgbehoevende, is het mogelijk dat gegevens over de gezondheid als bedoeld in artikel 9 AVG worden verstrekt. Dit kan zich voordoen indien ten aanzien van een zorgbehoevende aanleiding bestaat tot een vermoeden van fraude in de zorg, bijvoorbeeld in het geval van samenspanning. Uit gegevens die in een dergelijk geval mogelijk worden verwerkt over het domein, de leveringswijze en de soort zorg, kan bijvoorbeeld dan blijken dat de zorgbehoevende een voorziening heeft in beschermd wonen op grond van de Wmo 2015.

In artikel 1.2 van de wet is bepaald dat geen gegevens worden verstrekt waarop een medisch beroepsgeheim rust. Een uitzondering op het verbod tot verstrekken van deze gegevens geldt wanneer de betrokkene wiens medische gegevens het betreft toestemming geeft. Daarvan kan sprake zijn als deze betrokkene zelf een melding van een vermoeden van fraude in de zorg doet bij een betrokken instantie en daarbij gegevens over zijn gezondheid verstrekt, bijvoorbeeld een factuur van een behandeling.

#### 4.4.5 Conclusies uit benchmarkgegevens

Om een signaal van fraude in de zorg te kunnen beoordelen, kan het noodzakelijk zijn dit signaal af te zetten tegen wat gebruikelijk is in het domein waarop het signaal betrekking

heeft. Afwijkingen in de gegevens van de partij over wie het signaal gaat ten opzichte van de verzameling(en) van gegevens van de partijen waarmee vergeleken is, kunnen wijzen op fraude.

Om voornoemde vergelijking te kunnen doen, moet worden gekeken naar de verzameling(en) van gegevens van partijen die gelet op bepaalde kenmerken vergelijkbaar zijn met de partij op wie het signaal betrekking heeft. Het gaat om kenmerken zoals de aard van de verleende zorg, de regio waarin partijen actief zijn en de omvang van hun praktijk. De gegevens waarmee een signaal wordt vergeleken, worden in dit besluit als conclusies uit benchmarkgegevens aangeduid. Het gaat om conclusies uit analyses die zijn uitgevoerd op een of meerdere verzamelingen van gegevens van andere partijen. De conclusies uit benchmarkgegevens die instanties aan het IKZ verstrekken, mogen geen gegevens bevatten die te herleiden zijn tot individuele (rechts)personen anders dan de (rechts)persoon ten aanzien van wie een aanleiding tot een vermoeden van fraude in de zorg bestaat.

Instanties die over benchmarkgegevens beschikken, moeten de conclusies uit die benchmarkgegevens aan het IKZ verstrekken. Dat kan bijvoorbeeld het geval zijn als zij een signaal verstrekken en zij het benchmark bij de afweging tot verstrekking hebben gebruikt. Ook kan het IKZ in het kader van verrijking conclusies uit benchmarkgegevens bij instanties opvragen als het IKZ die in een specifiek geval noodzakelijk acht voor de verrijking van een signaal en de in dat kader te maken afweging voor (verdere) verwerking.

#### 4.4.6 Informatie over lopende en afgeronde onderzoeken

Informatie over lopende en afgeronde onderzoeken vormen een belangrijk onderdeel voor de verrijking van een signaal. De meest geëigende instantie die het verrijkte signaal ontvangt, weet door deze informatie of de partij waarover het signaal gaat door een van de betrokken instanties wordt onderzocht of al eerder is onderzocht in verband met fraude in de zorg. Deze informatie vormt dan ook een belangrijke indicatie en kan door de meest geëigende instantie worden betrokken in het verdere onderzoek naar het verrijkte signaal. Als bekend is dat er een lopend onderzoek is, kan bilateraal of multilateraal mogelijk afstemming plaatsvinden teneinde bijvoorbeeld te voorkomen dat het onderzoek wordt doorkruist.

Het gaat om informatie over lopende en afgeronde onderzoeken in verband met fraude in de zorg, voor zover het gegevens betreft die betrekking hebben op het signaal en binnen de gegevensset vallen. De informatie over lopende onderzoeken omvat enkel de informatie dát er een onderzoek loopt. Daarbij kan een indicatie worden gegeven van het tijdstip van afronding van het onderzoek, zodat daar bij het vervolproces rekening mee kan worden gehouden. In het geval van afgeronde onderzoeken gaat het om noodzakelijke inhoudelijke informatie met betrekking tot het signaal. Ook de onderliggende stukken van het onderzoek worden, voor zover dat past binnen de gegevensset, verstrekt. Het kan ook informatie over de afdoening zoals de opgelegde maatregel bevatten, tenzij wet- en regelgeving, zoals de Wet justitiële en strafvorderlijke gegevens (Wjsg), zich daartegen verzet.

Anders dan bij de andere gegevens die in het kader van verrijking door het IKZ worden uitgevraagd, is bij dit gegeven, voor zover het afgeronde onderzoeken betreft, gelet op de aard ervan wel ruimte voor een afweging door de verstreckende instantie. De onderzoeken bevatten naar verwachting immers meer informatie dan in het kader van de wet en de in dit besluit aangewezen gegevens mag worden verwerkt en noodzakelijk is. Gelet daarop alsmede gelet op aspecten zoals dataminimalisatie, wordt met de afweging door instanties mogelijk gemaakt dat niet volledige onderzoeken worden verstrekt.

Betrokken instanties wegens af welke informatie uit een onderzoek binnen de gegevensset past en noodzakelijkerwijs verstrekt moeten worden. Voor de BOD's geldt ook hier dat zij politiegegevens met inachtneming van de Wpg verstrekken.

*Het kan bijvoorbeeld gaan om een onderzoek door de IGJ, in verband met een geval van fraude in de zorg en mogelijke zorgverwaarlozing als gevolg daarvan, dat essentiële informatie bevat ten aanzien van het signaal. Of een rapport van een zorgverzekeraar die al eerder een fraudeonderzoek heeft uitgevoerd naar de partij waar het signaal over gaat.*

*Wanneer bijvoorbeeld een gemeente wordt aangewezen als meest geëigende instantie, is het voor die gemeente noodzakelijk om te weten bij welke gemeenten de partij waarover het signaal gaat nog meer bekend is en of een van de andere gemeenten al eens een rechtmatigheidsonderzoek heeft uitgevoerd naar de partij waarover het signaal gaat. De uitkomsten van een fraude- of rechtmatigheidsonderzoek kunnen belangrijke aanwijzingen bevatten die noodzakelijk zijn voor de verdere behandeling van het signaal door de geëigende instantie. Indien in een eerder fraude- of rechtmatigheidsonderzoek geconcludeerd werd dat sprake was van fraude, zal de meest geëigende instantie naar aanleiding van het signaal waarschijnlijk verder onderzoeken of opnieuw sprake is van fraude. Bleek uit het fraude- of rechtmatigheidsonderzoek juist dat geen sprake was van fraude, kan dat een aanwijzing zijn dat het signaal niet verder opgevolgd dient te worden door het IKZ of de meest geëigende instantie.*

#### 4.4.7 Gegevens rijksbelastingdienst

De rijksbelastingdienst verstrekt de noodzakelijke gegevens uit de aangifte inkomstenbelasting, aangifte loonheffing, aangifte omzetbelasting en uit de aangifte vennootschapsbelasting. Tevens verstrekt de rijksbelastingdienst indicaties over het aangiftegedrag en betaalgedrag van deze belastingen en of er openstaande schulden zijn. Bijvoorbeeld of de aangifte op tijd is gedaan en of tijdig aan de betalingsverplichting voldaan is. De rijksbelastingdienst en het IKZ maken werkafspraken waarin wordt afgesproken welke gegevens uit de genoemde aangiften de rijksbelastingdienst precies verstrekt. Ook treden de rijksbelastingdienst en het IKZ met elkaar in overleg over de interpretatie van deze gegevens. Een voorlopige aangifte en een vastgestelde aangifte zijn bijvoorbeeld verschillend van aard en ook de tijd die verstreken is sinds het doen van de aangifte moet worden meegewogen. Bij de verstrekking van deze gegevens geldt dat een afweging nodig is door de rijksbelastingdienst. De genoemde aangiften bevatten mogelijk meer informatie dan voor de verrijking van het betreffende signaal noodzakelijk is. Met inachtneming van het principe van dataminimalisatie verstrekt de rijksbelastingdienst enkel die gegevens die noodzakelijk zijn.

*De gegevens over de omzet kunnen worden afgezet tegen de gegevens over de winst en personeelskosten. De uitkomst daarvan kan een aanwijzing zijn of sprake is van fraude in de zorg. Bijvoorbeeld wanneer een partij een hoge omzet heeft, terwijl er maar enkele personeelsleden in dienst zijn die slechts een laag loon ontvangen. Dan zou sprake kunnen zijn van fraude. Vermogen en schulden uit de vennootschapsbelasting en inkomstenbelasting kunnen een aanwijzing zijn om te controleren of een onderneming bijvoorbeeld in korte tijd veel vastgoed verwerft. Bij een nieuwe partij met een klein cliëntenbestand die in korte tijd een grote hoeveelheid panden verwerft, zou bijvoorbeeld sprake kunnen zijn van fraude met zorggeld. Onderzocht zal moeten worden of in vastgoed wordt geïnvesteerd in plaats van dat het geld naar de zorg gaat waarvoor het is bedoeld.*

*Een ander voorbeeld waarom gegevens uit de inkomstenbelasting nodig kunnen zijn, is wanneer het zorggeld waarmee (mogelijk) gefraudeerd wordt uiteindelijk ten goede komt aan een natuurlijke persoon die hier onterecht van profiteert. Dat kan blijken uit een onverklaarbaar hoog banksaldo of veel vastgoed zonder dat daar een hypotheek tegenover staat. Dit is op zichzelf geen bewijs voor fraude in de zorg, maar het zijn gegevens die een signaal vormen of noodzakelijk kunnen zijn om vast te stellen of sprake is van fraude.*

#### 4.4.8 Declaratiegegevens

Declaratiegegevens worden ter bescherming van de privacy van betrokkenen slechts op geaggregeerd niveau verstrekt. Dat betekent dat de gegevens door andere instanties dan de verstrekker, niet te herleiden mogen zijn tot individuele personen. Het moet onwaarschijnlijk zijn dat uit de gegevens door welke partij dan ook, met inzet van (voor het doel) redelijke middelen, personen kunnen worden geïdentificeerd.

Declaratiegegevens betreffen informatie over de overeengekomen, in rekening gebrachte en geleverde prestaties. Het gaat dan ook om gegevens over de periode waarin deze prestaties geleverd zijn, aan welke (groepen of categorieën van) zorgbehoevende(n) deze prestaties geleverd zijn, de tarieven van de prestaties in relatie tot betaling van de prestaties, de periode waarover is uitgekeerd en over de omzet per ziektekostenverzekeraar of verstrekker. Het kan ook gaan om informatie over vaste maandlonen en gegevens over betalingen en bankrekeningnummers. Omdat geen gegevens aan het IKZ verstrekt worden waarop een medisch beroepsgeheim rust, worden de declaratiegegevens uitsluitend op geaggregeerd niveau verstrekt.

Om na te gaan of sprake is van fraude in de zorg, is inzicht nodig in wat is overeengekomen, wat is gedeclareerd en wat is vergoed of uitgekeerd. Op basis van de declaratiegegevens, in combinatie met andere gegevens of nader onderzoek door de geëigende instantie die het signaal opvolgt, kan onderzocht worden of de gemaakte afspraken zijn nagekomen en of de zorg is geleverd die in rekening is gebracht. Onderzocht kan worden of duurdere behandelingen zijn gedeclareerd dan daadwerkelijk overeengekomen zijn of dat mogelijk andere vormen van fraude met declaraties hebben plaatsgevonden.

#### 4.4.9 Indicatiegegevens

Gegevens over de indicatiebesluiten worden ter bescherming van de privacy van betrokkenen slechts op geaggregeerd niveau verstrekt. Dat betekent dat de gegevens door andere instanties dan de verstrekker, niet te herleiden mogen zijn tot individuele personen.

Het betreft het aantal afgegeven indicaties en beschikkingen en informatie over de zorgprofielen met betrekking tot de aanbieder waarover het signaal gaat. Omdat geen gegevens aan het IKZ verstrekt worden waarop een medisch beroepsgeheim rust, worden de indicatiegegevens uitsluitend op geaggregeerd niveau verstrekt. Dit betekent bijvoorbeeld dat een zorgkantoor de informatie verstrekt dat ten aanzien van de partij over wie het signaal gaat, tien indicatiebesluiten bekend zijn. Daarnaast kan het noodzakelijk zijn om informatie over de aard van de zorgprofielen te verstrekken. Het feit dat een aanbieder zich uitsluitend toelegt op de zwaarste zorgprofielen kan een aanwijzing voor fraude vormen, omdat daarmee de hoogste bedragen gemoeid zijn. Uiteraard vormt zo'n gegeven nooit op zichzelf een aanwijzing voor fraude in de zorg en moet het altijd in samenhang met alle andere gegevens worden gezien. Gegevens over de aard van de zorgzwaartepakketten kunnen bijvoorbeeld worden afgezet tegen declaratiegegevens van de ziektekostenverzekeraars, gemeenten en de SVB. Hieruit kan blijken of de bedragen die gedeclareerd zijn al dan niet overeenkomen met de zorg waarvoor geïndiceerd is.

#### 4.4.10 Gegevens van bijzondere opsporingsdiensten

Gelet op de wet- en regelgevingssystematiek van de Wpg, zijn de politiegegevens die de NLA en FIOD verstrekken, generieker in dit besluit opgenomen dan dat is gedaan met de andere gegevens. Het is aan deze BOD's om op basis van de generieke aanduiding te komen tot een lijst van gegevens die zij verstrekken aan IKZ en zij leggen dit vast in een werkdocument.

Politiegegevens die in het kader van de wet door de BOD's worden verwerkt, betreffen gegevens die in het kader van de uitvoering van de dagelijkse politietaak (meldingen en signalen) en onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (fraudeonderzoek) door de NLA en FIOD worden verwerkt op grond van artikel 8 respectievelijk artikel 9 Wpg.<sup>6</sup> Het ligt in de rede dat het gaat om gegevens die onderdeel uitmaken van de gegevensset zoals die in dit besluit is opgenomen ten aanzien van de andere betrokken instanties. Het betreft dan het signaal van fraude in de zorg, identificerende gegevens van een natuurlijke persoon, administratieve kenmerken van een rechtspersoon, handelsgegevens, gegevens over het zorgdomein en de soort zorg waarin de aanbieder zorg levert dan wel de zorgbehoevende zorg ontvangt. Tevens betreft het informatie over afgeronde onderzoeken voor zover noodzakelijk in verband met het betreffende signaal.

De NLA en FIOD verstrekken politiegegevens op grond van en met in achtneming van de Wpg. Indien de Wpg aanleiding geeft deze gegevens niet te verstrekken, dan wordt een signaal niet aan het IKZ verstrekt. Dat geldt eveneens voor het verstrekken van politiegegevens door de BOD's in het kader van verrijking. Indien daar aanleiding toe bestaat, delen de NLA respectievelijk FIOD slechts aan het IKZ mee dat geen politiegegevens worden verstrekt. Daaruit blijkt dan niet of niet over die gegevens wordt beschikt of dat er een andere aanleiding is de politiegegevens niet te verstrekken. Uit het enkele feit dat een bijzondere opsporingsdienst beschikt over politiegegevens, zou immers al strafrechtelijke informatie afgeleid kunnen worden over de persoon wiens gegevens het betreft.

Vanaf het moment dat deze politiegegevens door het IKZ worden ontvangen, worden deze gegevens aangemerkt als persoonsgegevens waarop de AVG van toepassing is. Dan is mogelijk sprake van persoonsgegevens van strafrechtelijke aard zoals bedoeld in artikel 10 AVG. Overigens kan tijdens het verrijkingproces op enig moment ook anderszins sprake zijn van een persoonsgegeven van strafrechtelijke aard. Persoonsgegevens van strafrechtelijke aard mogen ingevolge de AVG alleen verwerkt worden als passende waarborgen zijn geboden ter bescherming van de rechten en vrijheden van betrokkene(n). De in dit besluit opgenomen voorwaarden, vereisten, maatregelen en waarborgen geven hier invulling aan.

#### 4.5 Verstrekking van gegevens door het IKZ aan geëigende instantie(s)

##### *Wijze waarop*

Overeenkomstig de verstrekking van signalen en gegevens door instanties aan het IKZ en de verwerking van gegevens in het kader van verrijking door het IKZ, vindt verstrekking van een verrijkt signaal door het IKZ aan geëigende instanties elektronisch plaats en wordt hiervoor gedacht aan een systeem met portaalfunctie of een berichtenverkeerfunctie. Het ligt in de rede dat het gehanteerde elektronische systeem voor andere onderdelen van het proces van het IKZ, ook voor de verstrekking van het verrijkte signaal door het IKZ aan geëigende instanties wordt gebruikt.

---

<sup>6</sup> Kamerstukken II 2019/20, 35 515, nr.3, blz. 29-30

Ook voor deze verstrekking gelden afwijkende regels ten aanzien van de rijksbelastingdienst. De verstrekking van verrijkte signalen door het IKZ aan de rijksbelastingdienst, vindt in afwijking van de andere verstrekkingen niet plaats via een geautomatiseerde koppeling met het elektronische systeem.

#### *Gevallen waarin door het IKZ gegevens worden verstrekt na verrijking*

##### Verrijkt signaal

In het geval het resultaat van de verrijking door het IKZ noodzakelijk is voor een of meer instanties die gelet op hun rol en wettelijke taak zijn aangewezen de betreffende fraude in de zorg aan te pakken, verstrekt het IKZ dat resultaat aan die geëigende instantie(s). Per geval is verschillend welk van de instanties daartoe geëigend is of zijn. Gelet op de verschillende wettelijke taken en rollen van betrokken instanties, is de verwachting dat bepaalde instanties vaker en andere instanties minder vaak als een van de geëigende instanties worden aangemerkt. Per geval is ook verschillend welke instantie(s), welke gegevens uit het verrijkte signaal ontvangt dan wel ontvangen. Een en ander hangt bijvoorbeeld af van het rechtsgebied waarbinnen een signaal verder moet worden opgepakt, bijvoorbeeld het bestuursrecht of het strafrecht. Ook het domein waarbinnen het signaal zich voordoet kan bepalend zijn voor deze afweging. Voor een signaal waarvan duidelijk is dat het zich uitsluitend voordoet in het gemeentelijk domein, is het goed mogelijk dat bijvoorbeeld ziektekostenverzekeraars niet de meest geëigende instanties zijn. Het domein hoeft echter niet relevant te zijn bij deze afweging. Dat geldt bijvoorbeeld ten aanzien van de betrokkenheid van de IGJ. Fraude in de zorg en zorgverwaarlozing kunnen vaak zo nauw met elkaar verweven zijn, dat zij niet los van elkaar kunnen worden gezien, ongeacht in welk domein van de zorg het zich afspeelt. Gelet daarop ligt het in de verwachting dat de IGJ met regelmaat als een van de geëigende instanties wordt aangemerkt. Ook voor de rijksbelastingdienst geldt dat het domein niet relevant is. Fiscale fraude kan zich immers in ieder domein in de zorg voordoen en als daarvan sprake is, kan de rijksbelastingdienst een geëigende instantie zijn.

Vorenstaande betekent ook dat als verrijking van een signaal niet een resultaat oplevert waarvan het noodzakelijk is dat het aan de geëigende instantie(s) wordt verstrekt, geen verstrekking van dat verrijkte signaal door het IKZ aan die instantie(s) plaatsvindt. Zo kwam aan de orde dat instanties voor die beoordeling inzicht moeten hebben in voor wie van de betrokken instanties, wanneer, welke gegevens noodzakelijk (kunnen) zijn in het kader van de aan die instanties opgedragen wettelijke taken in het kader van bestrijding van fraude in de zorg. Dit kader is voor de verstrekking van gegevens door het IKZ aan geëigende instanties eveneens van groot belang. Afstemming hierover tussen het IKZ en betrokken instanties ligt eens te meer in de rede. Mede met het oog hierop is in de wet daarom de mogelijkheid tot gerichte verstrekking door het IKZ opgenomen (zie hierna). Het is overigens niet aan het IKZ te oordelen of sprake is van fraude in de zorg.

##### Gerichte verstrekking (om de meest geëigende instantie(s) te bepalen)

In het geval er meerdere geëigende instanties zijn, kan het noodzakelijk zijn dat het IKZ met specifiek deze instanties in overleg treedt teneinde te bepalen wat met het betreffende signaal wordt gedaan. Het gaat dan om de afweging aan welke geëigende instantie(s) het verrijkte signaal al dan niet wordt verstrekt. In artikel 2.4, vierde lid, van de wet is daarom bepaald dat het IKZ en instanties elkaar in dat geval en voor dit doel bij dit besluit aangewezen gegevens, waaronder persoonsgegevens, gericht kunnen verstrekken. Deze set aan gegevens is opgenomen in artikel 3.13 van dit besluit en beperkt dan de gegevensset voor verstrekkingen op grond van artikel 2.4, eerste en derde lid, van de wet. Voor het doel van gerichte verstrekking zijn immers niet alle

gegevens uit die laatstgenoemde set noodzakelijk. Dit is een maatregel in het kader van privacy by design.

Hierbij wegen het IKZ en de betreffende geëigende instanties af welke gegevens noodzakelijk zijn om in afstemming met elkaar te bepalen wie van de geëigende instanties het resultaat van de verrijking moet(en) ontvangen, gelet op hun rol en wettelijke taak in de bestrijding van fraude in de zorg.

De voor dit doel te verstrekken gegevens zullen in elk geval een korte omschrijving of samenvatting van het signaal omvatten. Het verstrekken van gegevens wordt ook hierbij tot het noodzakelijke beperkt. Gedurende het gehele proces van verrijking moet steeds de aard en herkomst van de gegevens duidelijk zijn en worden vastgelegd. Dat geldt hier eens te meer, zodat achteraf ook kan worden geduid welke afweging is gemaakt ten aanzien van de meest geëigende instantie(s).

Het is aan de in het specifieke geval geëigende instanties om indien nodig afspraken te maken over de vervolgaanpak. Bijvoorbeeld ten aanzien van welke van de instanties als eerst met het signaal verder gaat en een onderzoek start. Door afspraken te maken over de vervolgaanpak, kan voorkomen worden dat instanties onnodig tegelijkertijd actie ondernemen op een signaal of elkaar bij een lopend onderzoek naar of de aanpak van een specifiek geval frustreren.

#### *Voorwaarden*

Door het IKZ moet in afstemming met de betrokken instanties een proces zijn ingericht, om de hiervoor beschreven afweging tot het al dan niet verstrekken van gegevens en het bepalen van de meest geëigende instantie(s), zorgvuldig te kunnen maken. Gewaarborgd moet ook zijn dat elk van die instanties niet meer gegevens uit het verrijkte signaal ontvangt dan noodzakelijk voor de uitvoering van de wettelijke taak.

Voor de verstrekking van gegevens van de rijksbelastingdienst en de FIOD, voor zover het gegevens uit een fiscaal strafrechtelijk onderzoek betreft, geldt aanvullend de voorwaarde dat het IKZ toestemming van de betreffende instantie(s) moet hebben om deze gegevens, als die onderdeel uitmaken van het verrijkte signaal, te verstrekken aan ziektekostenverzekeraars. Achtergrond van deze voorwaarde is dat sprake is van een doorbreking van de fiscale geheimhoudingsplicht naar privaatrechtelijke instanties en dat daarbij grote terughoudendheid worden betracht. Het is aan de rijksbelastingdienst en de FIOD vast te leggen in welke gevallen en onder welke voorwaarden de toestemming voor verstrekking van de fiscale gegevens door het IKZ aan ziektekostenverzekeraars wordt verleend of niet. Met het oog op rechtsgelijkheid en rechtszekerheid voor betrokkene(n) alsmede gelet op een werkbare situatie voor het IKZ en de ziektekostenverzekeraars, moeten heldere, objectieve en uniforme criteria zijn geformuleerd. In het kader van transparantie moet dit kader voor afweging ook openbaar toegankelijk zijn.

Hoewel de AP ingevolge de UAVG formeel toezichthouder is op de verwerking van persoonsgegevens, is het IKZ zelf verantwoordelijk voor intern toezicht op de juiste en zorgvuldige omgang met gegevens. Derhalve is voorgeschreven dat het IKZ daartoe een proces heeft ingericht. Het ligt in de rede dat daarover afstemming met betrokken instanties. Als het de verwerking van persoonsgegevens betreft, is daarbij op grond van de AVG een belangrijke rol weggelegd voor de FG.

#### 4.6 Onderzoek en analyse van trends en ontwikkelingen

Het IKZ heeft naast het verrijken van gegevens, de taak trends en ontwikkelingen te signaleren en beleidsinformatie en statistische informatie met betrekking tot fraude in de zorg te ontwikkelen. Het IKZ verstrekt voornoemde gegevens uit eigen beweging en op verzoek aan de Minister voor LZS en betrokken instanties.

De wet bepaalt dat het IKZ de persoonsgegevens waarover het in het kader van de in artikel 2.4, eerste tot en met vierde lid, van de wet beschreven taak beschikt, mag verwerken voor onderzoek en analyse. Ten aanzien van de mogelijkheid om persoonsgegevens te mogen verwerken ten behoeve van dat doel, is in de wet daartoe een specifieke grondslag gecreëerd voor zover dit persoonsgegevens zijn waarover het IKZ in het kader van de verrijkingstaak de beschikking heeft en waarvan de verwerking voor de uitvoering van de onderzoek en analyse taak noodzakelijk is. Voor de verwerking van andere persoonsgegevens, biedt deze wet geen grondslag. Dit sluit overigens niet uit dat op grond van andere wet- en regelgeving een grondslag zou kunnen bestaan om persoonsgegevens te verwerken.

Het algemene uitgangspunt voor het gebruik van niet-persoonsgegevens is dat het raadplegen van bronnen en gebruik van informatie moet passen binnen de taak en rol van het IKZ op grond van de wet (doelbinding). Daarnaast moet het IKZ bij het gebruik van die gegevens de specifiek daarvoor geldende wet- en regelgeving in acht nemen. De wet noch dit besluit bevatten daaromtrent regels.

Hoewel onderzoek en analyse indien en voor zover noodzakelijk kan worden uitgevoerd met de in het kader van verrijking verkregen persoonsgegevens, bevatten de uitkomsten ervan nooit persoonsgegevens. De uitkomsten van onderzoek en analyse zijn nooit herleidbaar tot individuele personen. Uit de wet volgt het uitgangspunt is dat de uitkomsten ook niet tot individuele rechtspersonen of signalen zijn te herleiden. Dat past niet bij het doel van deze verwerking en deze taak van het IKZ. Ook zou het mogelijk onevenredig en nadelige gevolgen voor die rechtspersonen kunnen hebben.

Bij het signaleren van trends en ontwikkelingen en het ontwikkelen van statistische informatie en beleidsinformatie gaat het om het inzichtelijk maken van ontwikkelingslijnen en neigingen die zich (gedurende een langere termijn) voordoen op het gebied van fraude in de zorg en in welke richting dat gebeurt. Het IKZ stelt instanties met deze gegevens in de gelegenheid hun toezichhoudende, handhavende en opsporende taken beter uit te voeren. Op het moment dat ontwikkelingen zichtbaar worden, kunnen de instanties zelf doelgericht onderzoek doen of maatregelen treffen. Bovendien verstevigt deze kennis de mogelijkheden voor instanties om te anticiperen op de gesignaleerde ontwikkelingen. De noodzaak tot het verwerken van persoonsgegevens in het kader van deze taak is daarin gelegen dat de gegevens waarover het IKZ in het kader van verrijking beschikt en op basis waarvan deze tweede taak van het IKZ in beginsel wordt uitgevoerd, persoonsgegevens bevat.

*Het gaat daarbij bijvoorbeeld om de gegevens van eenmanszaken, die herleidbaar zijn tot een natuurlijke persoon en daarom op grond van de AVG beschouwd moeten worden als persoonsgegevens. Ook kan het gepseudonimiseerde gegevens betreffen. Ook gepseudonimiseerde gegevens moeten worden beschouwd als persoonsgegevens en derhalve is een grondslag voor het verwerken van persoonsgegevens hier noodzakelijk.*

Het is dan ook noodzakelijk dat in het kader van de uitvoering van deze taak die specifieke persoonsgegevens verwerkt kunnen worden. Daar komt bij dat (nieuwe) fenomenen beter in beeld kunnen worden gebracht als bijvoorbeeld duidelijk is om welke zorgaanbieder(s) het gaat en in welke regio en welk domein deze zorgaanbieder actief is en persoonsgegevens kunnen onderdeel uitmaken van deze informatie. In artikel 2.6 van de wet is echter uitgesloten dat het IKZ profileert zoals bedoeld in artikel 4, onder 4, AVG. Geen enkele vorm van geautomatiseerde verwerking van persoonsgegevens waarbij uitsluitend aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een



natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen, mag plaatsvinden. Door het IKZ worden geen personen in categorieën (profielen) ingedeeld op basis van hun persoonsgegevens en er is geen sprake van het in kaart brengen van personen met een verhoogd risico (op betrokkenheid bij fraude in de zorg). Tot slot vindt door het IKZ ook geen (geautomatiseerde individuele) besluitvorming plaats als bedoeld in artikel 22 AVG.

De Minister voor LZS kan de informatie ten aanzien van signalering van trends en ontwikkelingen en ontwikkelde beleidsinformatie en statistische informatie, eveneens zonder persoonsgegevens of gegevens over (individuele) rechtspersonen, van het IKZ bijvoorbeeld ontvangen in het kader van beleidsvorming en wet- en regelgeving. Dit gelet op zijn verantwoordelijkheid voor het zorgstelsel in het algemeen en ten aanzien van het IKZ in het bijzonder.

Door het IKZ moet een proces zijn ingericht dat een zorgvuldige gegevensverwerking in het kader van deze taak waarborgt. Dit kan het IKZ bijvoorbeeld doen door voor deze taak gebruik te maken van een van het zaaksinformatiesysteem afgezonderde omgeving, dat in deze toelichting wordt aangeduid als de analyseomgeving. Hierbij worden de kaders gevormd door de in dit besluit opgenomen regels. Het uitgangspunt is dat het IKZ vooraf in het jaarplan inzichtelijk maakt welke onderzoeken en analyses het voornemens is het betreffende jaar uit te voeren. Hierbij moet de mogelijkheid open worden gelaten dat op actuele ontwikkelingen kan worden ingespeeld.

#### 4.7 Waarborgen

De hierna toegelichte regels die gelden voor de gehele werking van het IKZ en zijn het sluitstuk van het kader van voorwaarden, vereisten, maatregelen en waarborgen waarbinnen de verwerking van gegevens in het kader van de wet moet plaatsvinden. Gelet op de gevoeligheid van alle in dit kader te verwerken gegevens, zijn de principes uit de AVG, zoals privacy by design en privacy by default, gegevensbescherming door ontwerp en standaardinstellingen, leidend bij alle gegevensverwerkingen.

##### 4.7.1 Inrichting, het beheer en de beveiliging van de elektronische voorzieningen en beveiliging van gegevens

###### *Algemeen*

In artikel 2.7 van de wet is bepaald dat het IKZ zorgdraagt voor de instandhouding van elektronische voorzieningen. Het betreft de voorzieningen voor de verwerking van de gegevens in het kader van het verrijken van signalen, het verstrekken van verrijkte signalen, het doen van gerichte verstrekkingen en voor het verrichten van onderzoek en analyse. Op grond van artikel 2.8 van de wet moeten regels worden gesteld over, voor zover hier van belang, de inrichting, het beheer en de beveiliging van die voorzieningen en ten aanzien van de beveiliging van de te verwerken gegevens. Een aantal van deze regels zijn opgenomen in dit besluit en voor het overige is in dit besluit bepaald dat de regels worden opgenomen in een ministeriele regeling.

Gelet op de publiek-private samenwerking waarin het IKZ een wettelijke taak heeft en de gevoeligheid van gegevens die het IKZ in dat kader verwerkt, bestaat het voornemen ten aanzien van de beveiliging van de voorzieningen en gegevens(verwerking) door het IKZ bij ministeriële regeling de BIO voor te schrijven. De reden dit in een ministeriële regeling te doen is voornamelijk van wetstechnische en pragmatische aard en wordt toegelicht in de artikelsgewijze toelichting. Het gaat bij de BIO om standaardnormeringen. Hierna

wordt in algemene bewoordingen toegelicht wat de toepasselijkheid van de BIO betekent. Ter illustratie komt in deze paragraaf een aantal onderdelen uit de BIO aan de orde.

De hiervoor beschreven verantwoordelijkheid van het IKZ voor de instandhouding van elektronische voorzieningen conform de voorgeschreven normen, geldt eens te meer omdat het IKZ verwerkingsverantwoordelijke is als bedoeld in de AVG vanaf het moment dat het van een betrokken instantie persoonsgegevens verstrekt krijgt. Dit doet overigens niet af aan de verantwoordelijkheden van de betrokken instanties die de gegevens verwerken.

Bij de nadere regels die in dit besluit zijn opgenomen, is ten aanzien van de inrichting, het beheer en de beveiliging van de elektronische voorzieningen en de beveiliging van gegevens aangesloten bij de AVG. In de artikelen 24, 25 en 32 verplicht die verordening de verwerkingsverantwoordelijke, in dit geval het IKZ, tot het nemen van passende technische en organisatorische maatregelen om de privacy te kunnen waarborgen en aan te kunnen tonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd.

#### *Inrichting en beheer*

De verwerking van de gegevens vindt plaats in elektronische voorzieningen die door het IKZ ingericht en beheerd worden. De elektronische voorzieningen bestaan uit verschillende onderdelen, waaronder in elk geval een zaakinformatiesysteem voor het verrijken van gegevens en een daarvan afgezonderde analyseomgeving voor het onderzoeken en analyseren van gegevens. Bij de inrichting van de voorzieningen moeten onder andere maatregelen worden getroffen die waarborgen dat alleen die medewerkers van het IKZ toegang hebben tot en bevoegd zijn tot de verwerking van specifiek die gegevens die zij nodig hebben voor de uitvoering van hun taken, zo volgt uit artikel 3.21 van dit besluit. Ook moeten ingevolge dat artikel maatregelen zijn getroffen die waarborgen dat gegevens die in de analyseomgeving worden verwerkt, voor opname in die omgeving worden ontdaan van gegevens, waaronder persoonsgegevens, die niet noodzakelijk zijn voor onderzoek en analyse.

Het IKZ zorgt ervoor dat een elektronische voorziening is ingericht waarop de betrokken instanties hun systemen kunnen aansluiten en signalen van fraude in de zorg aan het IKZ kunnen verstrekken. Zoals eerder toegelicht kan worden gedacht aan een portaalfunctie, waarin bestanden en berichten kunnen worden geüpload en gedownload, of een berichtenverkeerfunctie, waarbij sprake is van geïntegreerd berichtenverkeer in het systeem. Een belangrijk onderdeel hierbij is de koppeling tussen de systemen van de betrokken instanties en het systeem van het IKZ. Het IKZ zorgt ervoor dat het systeem van het IKZ geschikt is en blijft om koppeling met de systemen van de betrokken instanties mogelijk te maken. De betrokken instanties zorgen voor een continue zorgvuldige aansluiting op het systeem van het IKZ. Het is aan betrokken instanties de werkprocessen zo in te richten dat het duidelijk is welke signalen zij reeds hebben ingediend, zodat voorkomen wordt dat herhaaldelijk dezelfde signalen of signalen betreffende hetzelfde geval worden verstrekt.

Ongeacht de norm die wordt voorgeschreven, ligt het voor de hand dat in het kader van inrichting en beheer de wijze waarop de voorzieningen van het IKZ functioneren wordt vastgelegd in een systeembeschrijving. Hierbij worden informatie en bedrijfsmiddelen geïdentificeerd en wordt aandacht besteed aan eigenaarschap en monitoring van het gebruik. Ook wordt vastgelegd hoe het IKZ aan de geldende eisen voldoet. Deze systeembeschrijving wordt bovendien regelmatig geactualiseerd.

#### *Beveiliging van elektronische voorzieningen en gegevens*

De elektronische voorzieningen en gegevens moeten zijn beveiligd conform de bij ministeriële regeling gestelde nadere eisen. Uitgangspunt zal zijn dat het IKZ en de instanties ervoor zorgen dat de verstrekking en verwerking van gegevens door middel van elektronische uitwisseling, beveiligd worden en op een bepaald vertrouwelijkheidsniveau bestand zijn tegen incidentele gebeurtenissen of onrechtmatige of kwaadaardige acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen of doorgegeven gegevens in het gedrang brengen.

Zoals hiervoor aan de orde kwam, wordt eraan gedacht de BIO voor te schrijven. Wat betreft de aansluiting op de elektronische voorzieningen van het IKZ, bijvoorbeeld voor het verstrekken van gegevens, moet door betrokken instanties die privaatrechtelijk van aard zijn (de ziektekostenverzekeraars) worden voldaan aan beveiligingsnormen die ten minste gelijkwaardig zijn aan de voor het IKZ gestelde normen. Overheidsinstanties dienen hiervoor te voldoen aan de BIO. Ongeacht de beveiligingsnorm die wordt voorgeschreven, ligt het voor de hand dat het volgende geregeld wordt en als uitgangspunt wordt genomen.

Het IKZ en de betrokken instanties verantwoorden zich over de toepassing van de beveiligingsnormen bij de inrichting, het beheer en het gebruik van de elektronische voorzieningen. Dit doet het IKZ middels een informatiebeveiligingsbeleid dat wordt opgesteld. Als onderdeel van het informatiebeveiligingsbeleid voert het IKZ periodiek een risicoanalyse uit conform een algemeen geaccepteerde risicoanalyse-methode. Het IKZ laat periodiek een audit uitvoeren om te toetsen of de inrichting en het gebruik van de elektronische voorzieningen voldoen aan de bij ministeriële regeling voorgeschreven norm. Ook betrokken instanties verrichten een dergelijke periodieke audit.

Waar nodig voor de waarborging van een zorgvuldige gegevensverwerking, zal binnen het IKZ gelet daarop gedifferentieerd worden in autorisatieniveaus van medewerkers. Het gaat dan bijvoorbeeld om autorisaties ten aanzien van de toegang tot elektronische voorzieningen, die ervoor zorgen dat de medewerkers die werkzaamheden uitvoeren voor het onderdeel verrijking (de eerste taak van het IKZ) geen toegang hebben tot de gegevens die gebruikt worden voor het onderdeel onderzoek en analyse (de tweede taak van het IKZ). Zo wordt onder andere voorkomen dat medewerkers die signalen verrijken, daarbij andere gegevens raadplegen dan die noodzakelijk zijn voor het signaal dat verrijkt wordt. Ook betrokken instanties moeten bij de inrichting van processen werken met differentiatie in autorisatieniveaus.

Ten aanzien van de technische maatregelen worden nadere eisen eveneens uitgewerkt bij ministeriële regeling. Zo kunnen passende maatregelen op praktijkniveau worden gewaarborgd, waarbij ook adequaat kan worden bijgestuurd als (nieuwe) ontwikkelingen daarom vragen.

#### 4.7.2 Inrichting en het beheer van en de verantwoording door het Informatieknooppunt zorgfraude

Gelet op de verantwoordelijkheid van de Minister voor het zorgstelsel en zijn verantwoordelijkheid voor het IKZ, zoals nader toegelicht in paragraaf 4.2 van de memorie van toelichting bij de wet, zijn de bevoegdheden van de Minister voor LZS in dit besluit nader geregeld. In dit besluit zijn regels opgenomen ten aanzien van vaststellen van het jaarplan van het IKZ. De Minister voor LZS moet het jaarplan goedkeuren en hij heeft de bevoegdheid tot het geven van aanwijzingen ten aanzien van het plan. Zoals in paragraaf 4.7.6 van de toelichting op onderhavig besluit aan de orde komt, moeten deze nadere regels hun weerslag vinden in de statuten van de als IKZ aan te wijzen instelling.

Bij ministeriële regeling worden ook nadere eisen gesteld aan de inrichting en het beheer

van het IKZ. Ook in dit kader bestaat het voornemen de BIO voor te schrijven. Hierna worden uitgangspunten daarbij beschreven en de maatregelen toegelicht waaraan kan worden gedacht in dit kader.

Het is in de eerste plaats aan het IKZ te waarborgen dat medewerkers over voldoende opleiding, kennis en ervaring beschikken, voor hun specifieke functie in het algemeen en ten aanzien van (fraude in de verschillende domeinen binnen) het zorgdomein in het bijzonder. Daarbij dienen het IKZ en de betrokken instanties gezamenlijk te waarborgen dat de benodigde kennis en ervaring aan de medewerkers van het IKZ ter beschikking staat door middel van samenwerking in de keten. Ten tweede moet het IKZ er zorg voor dragen dat aan de geheimhoudingsplicht, opgenomen in artikel 2.9 van de wet, wordt voldaan en de medewerkers zorgvuldig en vertrouwelijk met de hen onder ogen komende gegevens omgaan. Daarop zien onder andere de regels ten aanzien van beveiliging van gegevens, maar dat moet ook in het hiervoor genoemde personeelsbeleid zijn gewaarborgd. Bij indiensttreding vindt een screening plaats ter verificatie van de achtergrond van alle kandidaten. Dit wordt uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's. Het ligt in de rede dat het IKZ daartoe een screeningsbeleid vaststelt. Bij indiensttreding en bij functiewijziging kan een Verklaring Omtrent het Gedrag (VOG) gevraagd worden. Wat betreft de arbeidsvoorwaarden in dit kader schrijft de BIO voor dat contractuele overeenkomsten met medewerkers en contractanten hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie moeten vermelden. Betrokkenen, intern en extern, moeten hier op gewezen worden bij aanstelling of functiewisseling. Er wordt ten aanzien van medewerkers zorggedragen voor bewustzijn, opleiding en training ten aanzien van informatiebeveiliging. Er moet ook een aansluiting zijn bij een klokkenluidersregeling, zodat iedereen anoniem en veilig beveiligingsissues kan melden. Tot slot is een formele en gecommuniceerde disciplinaire procedure voorgeschreven, zodat actie kan worden ondernomen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.

In onderhavig besluit zijn ook regels opgenomen over de wijze waarop de noodzakelijke verantwoordingsinformatie van het IKZ door de Minister voor LZS wordt ontvangen. Dit geschiedt schriftelijk en vindt zowel periodiek als op incidenteel verzoek van de Minister plaats. De termijnen voor het aanleveren van de informatie dienen (per geval) te worden afgesproken.

#### 4.7.3 Financiering en financiële verslaglegging door het IKZ

In artikel 2.8, eerste lid, onderdeel i, van de wet, is bepaald dat bij of krachtens amvb regels worden gesteld met betrekking tot de financiering en de financiële verslaglegging door het IKZ. Het IKZ voert een wettelijke taak uit en zal daarvoor een subsidie conform de Awb ontvangen van de Minister voor LZS. De Minister voor LZS zal gelet daarop zicht moeten houden op de doelmatige en doeltreffende uitvoering van de wettelijke taak en de rechtmatige en doelmatige besteding van het publieke geld.

#### 4.7.4 Bewaartermijnen en verwijdering van gegevens

*Bewaartermijnen en verwijdering van gegevens na het verstrijken van de bewaartermijn*  
In artikel 2.7, tweede lid, onderdeel a, van de wet, is bepaald dat bij amvb regels worden gesteld met betrekking tot de bewaartermijnen. De AVG schrijft voor dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk is voor het doel waarvoor ze worden verwerkt.

#### Verrijking

Voor de gegevens die worden verwerkt ten behoeve van de eerste taak van het IKZ, het verrijken van signalen en vervolgens verstrekken van het resultaat daarvan, geldt een maximale bewaartermijn van vijf jaar.

De gegevens die het IKZ ten behoeve van de uitvoering van deze taak ontvangt van betrokken instanties, worden indien zij juist en volledig zijn in het zaakinformatiesysteem van het IKZ opgeslagen in een dossier. Ook de gegevens die het IKZ op grond van artikel 2.4, tweede en vierde, van de wet verwerkt, worden in dat dossier opgeslagen. Op het moment dat een dossier wordt geopend in het zaakinformatiesysteem, begint een bewaartermijn van vijf jaar te lopen. De bewaartermijn geldt voor het dossier als geheel vanaf het moment dat het dossier is geopend. Als na opening van het dossier op een later moment gegevens worden toegevoegd aan het dossier, dan worden ook die gegevens verwijderd op het moment dat het dossier verwijderd moet worden.

Het is noodzakelijk om het volledige dossier gedurende vijf jaar te bewaren in het zaakinformatiesysteem. In de eerste plaats zodat een dossier gedurende die periode geraadpleegd kan worden indien dat noodzakelijk is. Dat kan zich bijvoorbeeld voordoen wanneer over eenzelfde partij meer (nieuwe) signalen bij het IKZ worden ingediend. Zo kan het zijn dat over een bepaalde partij eerst een signaal door een gemeente wordt ingediend, gevolgd door een signaal ingediend door een ziektekostenverzekeraar, waarna enkele weken of maanden later via de NZa een signaal wordt ingediend. Bij verrijking van de opvolgende signalen kan dan worden opgemerkt dat eerder reeds een of meer signalen over die partij zijn verstrekt aan het IKZ. Ten tweede is het noodzakelijk dat het IKZ inzichtelijk kan maken en kan onderbouwen op basis waarvan is besloten een signaal op een bepaalde wijze te verrijken. Ook kan dan worden onderbouwd op basis waarvan het resultaat van de verrijking vervolgens aan een of meer geëigende instantie(s) is verstrekt.

Nadat de bewaartermijn van vijf jaar is verstreken, worden de gegevens uit het zaakinformatiesysteem verwijderd en worden de gegevens voor zover nodig bewaard in een afgezonderde archiefomgeving. De gegevens zijn dan uitsluitend nog beschikbaar voor een beperkt aantal medewerkers van het IKZ, met als enig doel de afhandeling van klachten en gerechtelijke procedures. Deze gegevens worden pas verwijderd nadat tegen die verwerkingen en de rechtmatigheid daarvan geen rechtsmiddelen meer open staan.

#### Onderzoek en analyse

Voor de tweede taak van het IKZ, het doen van onderzoek en analyse, geldt één bewaartermijn van tien jaar. De gegevens worden gedurende die periode bewaard in de afgezonderde analyseomgeving, waarin de gegevens ten behoeve van vorenstaande taak worden verwerkt. De duur van de bewaartermijn is gerechtvaardigd, omdat het noodzakelijk is om uitspraken over trends en fenomenen te kunnen doen. De gegevens moeten immers over een langere periode kunnen worden onderzocht en geanalyseerd. De bewaartermijn van tien jaar gaat in op het moment dat het dossier waartoe de gegevens behoren, wordt geopend in het zaakinformatiesysteem. De startdatum van de termijn is daarmee gelijk aan die voor het verrijken van signalen. Andere gegevens die het IKZ voor de uitvoering van deze tweede taak uit zelfstandig geraadpleegde bronnen toevoegt, volgen de voornoemde termijn. Nadat de termijn van tien jaar is verstreken worden de gegevens uit de analyseomgeving verwijderd. De gegevens worden daarna voor zover nodig voor de afhandeling van klachten en gerechtelijke procedures nog bewaard. Deze gegevens worden pas verwijderd nadat tegen die verwerkingen en de rechtmatigheid daarvan geen rechtsmiddelen meer open staan. De resultaten van de onderzoeken en analyses door het IKZ, die geen persoonsgegevens of gegevens over individuele rechtspersonen bevatten, zijn vrijgesteld van deze bewaartermijn.

*Verwijdering van gegevens voor het verstrijken van de bewaartermijn*

Gedurende het proces van verrijken kan op enig moment blijken dat geen aanleiding (meer) tot een vermoeden van fraude bestaat. Dat kan zich voordoen als (evident) blijkt dat onjuiste feiten, omstandigheden, aannames of interpretaties aanleiding hebben gegeven tot het vermoeden. In dat geval verwijdert het IKZ het signaal op dat moment uit het zaaksinformatiesysteem. De gegevens worden dan nog wel bewaard in de afgezonderde archiefomgeving, ten behoeve van de afhandeling van klachten en gerechtelijke procedures. In dat geval draagt het IKZ er ook zorg voor dat het signaal wordt verwijderd uit de analyseomgeving voor de tweede taak van het IKZ. Ten behoeve van de volledigheid en juistheid van statistische analyses blijft dan enkel nog een nummer geregistreerd met daaraan toegevoegd een code waaruit blijkt dat het signaal is verwijderd omdat de aanleiding tot een vermoeden van fraude is weggefallen. Tot slot meldt het IKZ bij de betrokken instantie die het signaal heeft verstrekt, dat het signaal verwijderd is omdat niet langer een aanleiding tot een vermoeden van fraude bestaat. Andersom kan het ook voorkomen dat een instantie die het signaal heeft ingediend, tot de conclusie komt dat niet langer een aanleiding tot een vermoeden van fraude bestaat. Dan dient die betrokken instantie dit ook aan het IKZ te melden, zodat het IKZ het signaal uit de eigen systemen kan verwijderen.

Wanneer sprake is van een verrijkt signaal dat reeds aan een of meer geëigende instanties is verstrekt en de meest geëigende instantie komt op basis van eigen onderzoek tot de conclusie dat er niet langer een aanleiding tot een vermoeden van fraude is, dan meldt die instantie dat aan het IKZ. Dit is inherent aan zorgvuldig proces van gegevensuitwisseling. Het IKZ moet dan het signaal uit de eigen systemen verwijderen. Gelet op het belang van de partij op wie dat signaal betrekking heeft, moet het IKZ ook de verstreckende instantie en de andere geëigende instantie(s) aan wie het verrijkte signaal is verstrekt, hierover informeren. Ook in dit kader is het van belang dat betrokken instanties de werkprocessen zo hebben ingericht dat het duidelijk is welke signalen zij reeds hebben ingediend. Zo kan voorkomen worden dat, al dan niet na verwijdering van het signaal door het IKZ, niet herhaaldelijk dezelfde signalen of signalen betreffende hetzelfde geval worden verstrekt.

Vorenstaande situaties dienen te worden onderscheiden van de situatie dat het IKZ gedurende het verrijkingsproces na afweging van het geval tot het oordeel komt dat (op dat moment) niet wordt voldaan aan de voorwaarden het verrijkingsproces voort te zetten. Er is onvoldoende grond voor verdere verwerking, maar de aanleiding tot het vermoeden van fraude in de zorg is ook niet weggenomen. In dat geval worden de gegevens conform de geldende bewaartermijn bewaard en kan het verrijkingsproces binnen de geldende voorwaarden en termijnen mogelijk worden hervat indien daar aanleiding toe is.

Ook kan de uitoefening van de rechten door een betrokkene op grond van de AVG, zoals het recht op gegevenswissing in artikel 17, aanleiding vormen tot verwijdering van gegevens.

#### 4.7.5 Uitoefening van de rechten van betrokkenen

In artikel 2.8, tweede lid, onderdeel b, van de wet, is bepaald dat bij amvb regels worden gesteld met betrekking tot de uitoefening van de rechten van betrokkenen. De rechten van betrokkenen zijn voor zover het persoonsgegevens betreft geregeld in de AVG en de UAVG. De verantwoordelijke instantie die een signaal met gegevens verstrekt, is en blijft verantwoordelijk voor die verwerking van gegevens. Het IKZ is verwerkingsverantwoordelijke voor de persoonsgegevens die binnen het IKZ worden verwerkt en respecteert de rechten van betrokkenen en faciliteert de uitvoering daarvan. Het IKZ is ook verantwoordelijk voor de verwerking van gegevens, anders dan persoonsgegevens. Het uitgangspunt is dat het IKZ ook ten aanzien van de verwerking

van die gegevens een hoge mate van zorgvuldigheid betracht en de rechten van betrokkenen daarbij respecteert. Ook voor het geval dat de gegevensverwerking niet om persoonsgegevens gaat, moet derhalve zijn geregeld tot wie een betrokkene zich kan wenden met bijvoorbeeld een verzoek tot inzage of verwijdering en bij een geschil over de juistheid of rechtmatigheid van de verwerking van die gegevens.

Het IKZ richt met het oog op vorenstaande verantwoordelijkheden een proces in en draagt zorg voor de kenbaarheid van openstaande rechtsmiddelen. Daarbij is een belangrijke rol weggelegd voor de FG, tot wie een betrokkene zich ingevolge de AVG kan wenden voor alle aangelegenheden die verband houden met de verwerking van zijn persoonsgegevens en met de uitoefening van zijn rechten uit hoofde van de AVG. Het ligt in de rede dat de persoon die als FG functioneert, een soortgelijke functie vervult als het om de verwerking van andere gegevens dan persoonsgegevens gaat.

Conform artikel 14 AVG informeert het IKZ de betreffende natuurlijke persoon of rechtspersoon, als sprake is van verwerking van persoonsgegevens, over de verwerking. Van het informeren kan in uitzonderingsgevallen worden afgezien, indien sprake is van een situatie als bedoeld in artikel 14, vijfde lid, AVG. Daarbij kan het gaan om de situatie dat de bedoelde verplichting de verwezenlijking van de doeleinden van die verwerking, te weten bestrijding van fraude in de zorg, onmogelijk dreigt te maken. Teneinde de mogelijke nadelige gevolgen voor de betrokken partij te beperken, zijn passende maatregelen vereist. Het geheel aan voorwaarden en maatregelen in dit besluit voorziet daarin. Wat betreft de hier genoemde uitzondering op de informatieplicht, is het aan het IKZ ervoor zorg te dragen dat een betrokken partij desalniettemin zo spoedig mogelijk wordt geïnformeerd.

#### 4.7.6 De aanwijzing van het Informatieknooppunt zorgfraude en daaraan verbonden voorschriften

In artikel 2.8, onderdeel j, van de wet, is bepaald dat nadere regels worden gesteld aan het aanwijzen van een instelling als het Informatieknooppunt zorgfraude. In dit besluit is daar invulling aan gegeven. Voorgeschreven is dat een als zodanig aan te wijzen instelling een rechtspersoon dient te zijn. Bij de aanwijzing moet rekening worden gehouden met de brede schakering van betrokken instanties, zowel publiek als privaat en zowel centraal als decentraal, om zoveel mogelijk recht te doen aan de positie van betrokken instanties. Ook moet de gewenste (on)afhankelijke positie van de instelling worden afgewogen. In dit kader geldt al de rijksbrede afspraak dat een bestuurder van de instelling niet tevens een ambtenaar kan zijn en moet gewaarborgd worden dat bestuurders van de instelling geen tegenstrijdige belangen hebben. Tevens moet de onafhankelijkheid van de medewerkers van de instelling gewaarborgd worden. Het soort gezag en de aard van de (rechts)handelingen die het heeft of die verricht kunnen worden spelen eveneens een rol bij de aanwijzing. Ook moet de rol van de centrale overheid (VWS) en de algemene verantwoordelijkheid van de Minister voor LZS voor het zorgdomein en de inrichting en het functioneren van het zorgstelsel in acht worden genomen. Onderdeel daarvan is hoe het IKZ, gelet op de taak in het bestrijden van fraude in de zorg, beleidsmatig onder zijn verantwoordelijkheid valt. Benoeming, bezoldiging, schorsing en ontslag van bestuurders van de instelling geschiedt door de Minister voor LZS.

De instelling moet in staat zijn te voldoen aan de in de wet en onderhavig besluit opgenomen voorwaarden en waarborgen. Het gaat onder andere om de voorwaarden ten aanzien van de zorgvuldige verwerking van gegevens en de daarvoor benodigde inrichting van processen en voorzieningen, de beveiliging van de elektronische voorzieningen en gegevens en het ter beschikking hebben van voldoende kennis en kunde. Hetgeen in de wet en onderhavig besluit is opgenomen, moet zijn weerslag vinden in de (oprichtings)statuten van de betreffende instelling. Er moet een duidelijke binding zijn tussen de in statuten opgenomen taken van de aan te wijzen instelling en de aan die

instelling in deze wet opgedragen wettelijke taken (doelbinding). De bezoldiging bedraagt nimmer meer dan de bezoldiging die kan worden toegekend op grond van het Besluit vergoedingen adviescolleges en commissies. Transparantie is van groot belang en in dat kader moet ook geborgd zijn dat de Minister voor LZS inzicht heeft in de nevenfuncties van het bestuur, de directie en medewerkers van de aan te wijzen instelling. De (oprichtings)statuten of de wijziging daarvan moeten worden goedgekeurd door de Minister voor LZS.

#### 4.8 Wijziging besluit basisregistratie personen

Met artikel 4.2 is het Besluit basisregistratie personen (Besluit BRP) gewijzigd. Hiermee zijn de werkzaamheden van het IKZ aangewezen als werkzaamheden met een gewichtig maatschappelijk belang ten behoeve waarvan systematisch gegevens uit de basisregistratie kunnen worden verstrekt. Bij de aanwijzing is tevens bepaald welke BRP-gegevens ten hoogste kunnen worden verstrekt aan het IKZ. De werkzaamheden betreffen het uitvoeren van de taak, bedoeld in artikel 2.4, derde lid, van de wet ten behoeve van de bestrijding van fraude in de zorg (het Informatieknoppunt zorgfraude).

Het primaire doel van de basisregistratie personen (BRP) is het verstrekken van persoonsgegevens aan overheidsorganen. Aan niet-overheidsorganen ('derden') kunnen slechts systematisch gegevens worden verstrekt indien deze derden werkzaamheden verrichten met gewichtig maatschappelijk belang waarvoor BRP-gegevens noodzakelijk zijn. In bijlage 4 bij het Besluit BRP (hierna: bijlage 4) zijn deze werkzaamheden en derden aangewezen. Op grond van artikel 3.3, tweede lid, van de Wet basisregistratie personen (Wet BRP) worden enkel werkzaamheden aangewezen die samenhangen met een overheidstaak, strekken tot het in stand houden van een voorziening voor burgers die onderwerp is van overheidszorg, of waarbij anderszins gelet op de overheidsbemoediging met die werkzaamheden, ondersteuning daarvan door gegevensverstrekking uit de BRP gerechtvaardigd is. Bij separaat te nemen besluit van de minister van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK), zal verder ten aanzien van het IKZ worden bepaald welke gegevens over welke categorieën van personen aan de betreffende derde worden verstrekt en in welke gevallen en op welke (technische) wijze deze verstrekking plaatsvindt (hierna: autorisatiebesluit). Het kan enkel gegevens betreffen die betrekking hebben op degene over wie het IKZ een signaal van fraude in de zorg heeft ontvangen. De systematische verstrekking van gegevens houdt in dat binnen de grenzen van de autorisatie de gevraagde gegevens, in principe voor onbepaalde tijd, op geautomatiseerde wijze uit de BRP worden verstrekt.

##### 4.8.1 Gewichtig maatschappelijk belang en noodzaak gegevensverstrekking

Door zowel de politiek, de zorgpraktijk als de maatschappij, wordt fraude in de zorg gezien als een groot maatschappelijk probleem en een zeer kwalijk fenomeen. Zorgbehoevenden moeten daadwerkelijk de zorg krijgen die zij nodig hebben en waar zij recht op hebben en mogen niet de dupe worden van zorgaanbieders die frauderen, noch wat betreft de toegang tot en kwaliteit van zorg noch financieel. Daar komt bij dat jaarlijks veel geld omgaat in de zorgsector, dat wordt opgebracht door de premie- en belastingbetaler. Burgers moeten erop kunnen vertrouwen dat middelen die bestemd zijn voor de zorg ook daadwerkelijk aan zorg worden besteed. Het is onacceptabel dat misbruik wordt gemaakt van maatschappelijke voorzieningen voor eigen (financieel) gewin. Fraude tast niet alleen de betaalbaarheid van de zorg aan, maar ondermijnt ook het vertrouwen in de integriteit van zorgaanbieders en gaat ten koste van solidariteit en de bereidheid van mensen om bij te dragen aan de kosten van de gezondheidszorg. Zowel zorgbehoevenden als de maatschappij moeten dan ook worden beschermd tegen fraude. Er is sprake van een zwaarwegend algemeen belang en dit belang is een prioriteit van de minister voor LZS. Daarnaast is ook vanuit de Tweede Kamer bij herhaling aangegeven dat fraude in de zorg onacceptabel is en effectief dient te worden aangepakt. Het



tegengaan van fraude in de zorg is aldus een onderwerp van overheidszorg en de werkzaamheden van het IKZ hangen daarmee direct samen. Daarnaast vallen de werkzaamheden van het IKZ onder de stelselverantwoordelijkheid van de minister voor LZS. Op grond van de wet wijst de minister voor LZS de instelling aan die deze werkzaamheden zal uitvoeren. Daarmee houdt de minister voor LZS de eindregie over waar deze werkzaamheden worden belegd. Het vorengaande rechtvaardigt het aanwijzen van de werkzaamheden van het IKZ in bijlage 4 van het Besluit BRP als werkzaamheden met een gewichtig maatschappelijk belang.

De systematische gegevensverstrekking is noodzakelijk. Bij de uitvoering van de gegevensbeschermingseffectbeoordeling in het kader van de totstandkoming van dit besluit is naar voren gekomen dat het risico op verwerking van onjuiste gegevens door het IKZ onvoldoende is afgedekt met een controle van bepaalde gegevens aan de andere in de wet opgenomen bronnen. Op basis van ervaring in de praktijk hebben betrokken instanties gewezen op de mogelijke onjuistheden in gegevens en de risico's van een te beperkte controle op de juistheid van gegevens door het IKZ. Bij onvoldoende controlemiddelen kan het niet alleen voorkomen dat het IKZ onjuiste gegevens ontvangt, en zo (mogelijk) ten onrechte (persoons)gegevens verwerkt, deze onjuiste gegevens kunnen vervolgens – in de vorm van een verrijkt signaal - ook bij de betrokken instanties terecht komen. Het verstrekken van gegevens uit de BRP dient dan ook enkel ter verificatie van de gegevens die het IKZ over de betrokkene op wie het signaal van fraude betrekking heeft van betrokken partijen verkrijgt en vervolgens verder verwerkt. Hiermee wordt het risico op de verwerking van onjuiste gegevens beperkt en kan worden voorkomen dat het IKZ een verrijkt signaal verstuurt dat betrekking heeft op de verkeerde persoon. Om het verzamelen en verrijken van gegevens door het IKZ efficiënt en betrouwbaar te laten verlopen is systematische gegevensverstrekking uit de BRP aan het IKZ dan ook gerechtvaardigd. Hoewel het IKZ ten behoeve van de betrokken instanties een ondersteunende taak heeft bij de bestrijding van fraude in de zorg, is het IKZ verwerkingsverantwoordelijk voor de persoonsgegevens die het verwerkt. Bij deze verantwoordelijkheid en zelfstandige taak, past dat het IKZ zelf de mogelijkheid heeft de gegevens die het verwerkt aan de hand van de BRP op juistheid en actualiteit te controleren.

#### 4.8.2 Beperking gegevensverstrekking

De aanwijzing bevat een beperking van de categorieën gegevens die kunnen worden verstrekt aan het IKZ. Het betreft hier de algemene gegevens over de burgerlijke staat (waaronder naam en geboortedatum), het adres en het naamgebruik door de ingeschrevene op wie het signaal van fraude betrekking heeft. Deze gegevens zijn voor het IKZ noodzakelijk om de ontvangen signalen te verifiëren en actualiseren. Het IKZ is op grond van de wet niet bevoegd om het BSN te verwerken. Dat gegeven zal dan ook niet worden verstrekt.

#### 4.8.3 Rechten van betrokkenen

De rechten die de betrokkene heeft op grond van de Wet BRP (Hoofdstuk 3, afdeling 2 Wet BRP) en de AVG zijn van toepassing op de verstrekking van gegevens aan derden (hier: IKZ). Zo heeft de betrokkene op grond van artikel 3.22 Wet BRP recht op inzage in de verstrekking van diens eigen gegevens uit de BRP aan een derde. De betrokkene heeft niet de mogelijkheid de verstrekking tegen te houden. De verstrekkingbeperking (artikel 3.21 Wet BRP) wordt niet van toepassing verklaard. Dit betekent dat een betrokkene de verstrekking van gegevens die op hem betrekking hebben aan deze derden niet kan verhinderen. Bij de afweging ten aanzien van de verstrekkingbeperking speelt de vraag in hoeverre de burger zelf redelijkerwijs kan besluiten dat hem betreffende gegevens niet aan een derde mogen worden verstrekt, ook als dat primair voor hem negatieve gevolgen kan hebben, en in hoeverre de goede

taakuitoefening van de betreffende derde in het algemeen in de knel zou komen door mogelijke verstrekingsbeperkingen. Met name deze laatste overweging maakt dat ten aanzien van de aan te wijzen werkzaamheden de verstrekingsbeperking niet van toepassing is. De reden hiervoor is gelegen in het gewichtig maatschappelijk belang van de werkzaamheden (zie hiervoor paragraaf 4.8.1 van deze toelichting) en de noodzaak tot raadpleging van de BRP daarbij. Wat betreft de aanwijzing van het IKZ voor het uitvoeren van de taken, bedoeld in artikel 2.4, derde lid, van de wet geldt dat toegang tot de BRP wordt verleend zodat daarmee fraude in de zorg op een doelmatige en zorgvuldige wijze kan worden tegengegaan. Wanneer een betrokkene het verstrekken van zijn BRP-gegevens aan het IKZ zou kunnen verhinderen, zou het doel van de aanwijzing worden ondermijnd.

## 5. Gegevensbeschermingseffectbeoordeling

Voor dit besluit is conform artikel 35 AVG een Privacy Impact Assessment (PIA), ook wel gegevensbeschermingseffectbeoordeling genoemd, uitgevoerd. In de PIA is toegelicht waar het assessment op ziet en is op hoofdlijnen de context beschreven waarbinnen deze plaatsvindt. Daarbij is ingegaan op de aanleiding voor dit besluit, het beoogde doel van het besluit en de onderdelen waaruit het besluit bestaat. Vervolgens is aandacht besteed aan de mogelijke verwerkingen van persoonsgegevens, de doeleinden van de verwerkingen, welke instanties bij de verwerkingen betrokken zijn (en wie daarbinnen toegang tot de persoonsgegevens hebben) en welke categorieën persoonsgegevens worden verwerkt. Ook zijn de belangen bij de gegevensverwerking uiteengezet. Tevens is uitgeschreven op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. De rechtmatigheid van de gegevensverwerkingen zijn ook beoordeeld. Daarbij is aandacht besteed aan de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkene. Tot slot zijn de risico's voor betrokkenen beschreven en beoordeeld, waarna de daarop geformuleerde maatregelen zijn toegelicht. In de hoofdstukken 1 tot en met 4 van deze nota van toelichting komen al deze onderdelen aan de orde.

## 6. Verantwoording ontvangen adviezen

### 6.1 Autoriteit persoonsgegevens

De AP is op grond van artikel 36, vierde lid, AVG geraadpleegd over dit besluit. De AP heeft kenbaar gemaakt er geen opmerkingen over te hebben.

De AP heeft ook advies uitgebracht over het met artikel 4.2 gewijzigde Besluit BRP. De AP adviseert om het voorstel tot derdenverstrekking aan het IKZ niet eerder te behandelen dan nadat het wetsvoorstel Wbsrz door de Tweede Kamer is aangenomen. Dit advies is opgevolgd.

Onverminderd het bovenstaande, adviseert de AP over de voorgestelde verstrekking aan het IKZ verder als volgt. Het concept bepaalt welke persoonsgegevens systematisch uit de basisregistratie personen worden verstrekt aan het IKZ. Het betreft de algemene gegevens als bedoeld in artikel 2.7, eerste lid, onder a, onder 1<sup>o</sup>, 7<sup>o</sup> en 10<sup>o</sup> van de Wet BRP. De noodzaak van het verstrekken van een aantal van deze gegevens spreekt niet voor zich en is ook niet in de toelichting aangetoond. Het betreft de gegevens over de ouders, het huwelijk, dan wel geregistreerd partnerschap en eerdere huwelijken of eerder geregistreerde partnerschappen, de echtgenoot dan wel geregistreerd partner en eerdere echtgenoten of geregistreerde partners, en de kinderen. De AP adviseert om de derdenverstrekking aan het IKZ in het concept te beperken tot de gegevens waarvan de noodzaak in de toelichting is aangetoond. Dit advies is opgevolgd. Gegevens over

gerelateerden (zoals ouder, partner en kind) kunnen op grond van dit besluit niet verstrekt worden aan het IKZ. De gegevensset (derdenverstrekking) is zo beperkt tot de identificerende gegevens die het IKZ op grond van hoofdstuk 3, paragraaf 1, van dit besluit mag verwerken. Het betreft alleen gegevens van de betrokkene op wie het signaal van fraude in de zorg betrekking heeft. Door verstrekking vanuit de BRP kan het IKZ de juistheid van deze gegevens controleren.

## 6.2 Uitvoeringstoetsen

Betrokken instanties zijn in de gelegenheid gesteld om de uitvoerbaarheid van het besluit te toetsen. De uitkomsten van deze toetsen zijn in deze paragraaf samengevat en daarbij is een verantwoording opgenomen hoe deze uitkomsten al dan niet zijn verwerkt in het besluit.

### *CIZ*

Het CIZ heeft in haar uitvoeringstoets aangegeven dat het, om uitvoering van de informatie-uitwisseling tijdig te kunnen voorbereiden en borgen, van belang is dat het CIZ voor de (werk)processen met de ketenpartners (landelijk) afgestemde, duidelijke afspraken implementeert om verzoeken voor het delen van signalen in het kader van fraude tijdig te kunnen doorgeven en te kunnen verrijken.

Het CIZ heeft risico's en de daarbij te nemen maatregelen aangegeven. Hierna worden enkele benoemd. De impact van een aangekondigde ministeriële regeling is onduidelijk, waardoor precieze invulling van taken en werkzaamheden nog onbekend zijn. Hierover blijft het CIZ in contact met het ministerie van VWS om uitvoeringsconsequenties tijdig te kunnen bespreken. Een ander risico is dat er te weinig capaciteit (en budget) is om aanpassingen in werkproces en systeeminrichting tijdig te realiseren. Hiervoor zal er structureel overleg met het IKZ zijn om de impact van aanpassingen te inventariseren en tijdig af te stemmen met het ministerie van VWS. Er zouden ook meer verzoeken van instanties kunnen komen om signalen te verrijken dan eerder is ingeschat. Er zal dan meer capaciteit beschikbaar gesteld worden om tijdig aan de verzoeken te kunnen voldoen.

Het CIZ verwacht de gegevensuitwisseling met het IKZ te kunnen uitvoeren binnen de reguliere werkzaamheden en het reguliere budget. Wel merkt het CIZ op dat gezien de aantallen verstrekkingen die het verwacht, een systeemkoppeling disproportioneel is. Zoals aangegeven in paragraaf 4.3.3 van deze toelichting is het uitgangspunt dat de noodzakelijke gegevens, indien beschikbaar, in de fase van verrijking via een koppeling met de betrokken instanties automatisch aan het signaal worden toegevoegd. Om deze werkwijze te bereiken hebben het IKZ en de betrokken instanties een inspanningsverplichting. In een ministeriële regeling worden resultaatsverplichtingen opgenomen ten aanzien van de minimaal geldende normen en afspraken ten aanzien van de wijze van verwerking.

### *Inspectie Gezondheidszorg en Jeugd*

De IGJ merkt op dat de formulering van 3.13 (thans artikel 3.14) van dit besluit leidt tot een beperking van de beschikbare informatie die kan worden gedeeld, omdat voornoemd artikel inkadert op welke wijze aan te leveren signalen moeten worden onderbouwd. De regering heeft het artikel zo geformuleerd om een balans te creëren tussen enerzijds het in regelgeving vastleggen onder welke voorwaarden een signaal aan het IKZ verstrekt kan worden, zonder het te ver in te perken en anderzijds het voor betrokkenen transparant en duidelijk te maken wanneer hun gegevens, waaronder persoonsgegevens, verwerkt kunnen worden. Het is daarbij uitdrukkelijk niet de bedoeling dat alle beschikbare informatie wordt gedeeld. Het dient te gaan om de strikt noodzakelijke gegevens ten

behoefte van de bestrijding van fraude in de zorg. Welke gegevens dat kunnen zijn, is ingekaderd in de in dit besluit aangewezen gegevensset.

De IGJ vraagt hoe de zinsnede "die betrokken zijn bij een aanleiding tot een vermoeden van fraude in de zorg" in artikel 3.3 van dit besluit zich verhoudt tot de zinsnede "die noodzakelijk zijn voor een of meerdere van de in dit lid genoemde instanties voor de bestrijding van fraude in de zorg in het kader van de aan die instanties opgedragen wettelijke taken" in artikel 2.4, eerste lid, van de wet. Deze artikelen sluiten op elkaar aan. In artikel 2.4, eerste lid, van de wet wordt bepaald dat de bij amvb aangewezen gegevens door instanties verstrekt worden aan het IKZ ten behoeve van het in dat lid genoemd doel. Artikel 3.3 van dit besluit geeft vervolgens aan welke gegevens ten behoeve van dat doel door de IGJ verstrekt worden.

In paragraaf 4.4.6 van deze toelichting is een voorbeeld over informatie over lopende en afgeronde onderzoeken opgenomen. Doordat de onderzoeken van de IGJ niet zijn gericht op de aanpak van fraude in de zorg, maar op de kwaliteit en veiligheid van de zorgverlening, doet de IGJ de suggestie om dit voorbeeld aan te vullen, bijvoorbeeld door aan te geven dat het gaat om onderzoeken in verband met fraude in de zorg 'en mogelijke zorgverwaarlozing als gevolg daarvan'. Deze suggestie is overgenomen.

De IGJ geeft verder aan dat voor professionals die werken in de jeugdhulp en jeugdbescherming registratie in het register van de SKJ meer gebruikelijk is als identificerend gegeven. De IGJ adviseert om ook het SKJ-registratienummer op te nemen in het besluit als onderdeel van de te verstrekken gegevens. Dit is overgenomen. In artikel 1 van het besluit is dit opgenomen onder de definitie van identificerende gegevens van een natuurlijke persoon.

#### *NLA*

De NLA maakt in de uitvoeringstoets opmerkingen over de ICT van het IKZ. Allereerst maakt de NLA een voorbehoud ten aanzien van de bepalingen uit artikel 3.25, tweede lid, (thans artikel 3.23, tweede en derde lid) van het besluit. Zodra meer bekend is rondom de aansluiting wil de NLA beslissen of het aansluit bij de geautomatiseerde gegevensuitwisseling. Daarnaast geeft de NLA aan dat het vastleggen van regels ten aanzien van de beveiliging van gegevens in een ministeriele regeling, minder flexibel is en minder risicogericht gestuurd kan worden. Beveiligingsdreigingen vragen om snelle interventies. De regering deelt uiteraard het laatstgenoemde standpunt. Beveiliging van gegevens, waaronder persoonsgegevens, is van groot belang. Derhalve moet snel een aanpassing mogelijk zijn bij (nieuwe) dreigingen. Tegelijkertijd verplicht de AVG bij het verwerken van persoonsgegevens het nemen van passende technische of organisatorische maatregelen waardoor een passende beveiliging gewaarborgd is. Daarvoor is het nodig dat de regels voor beveiliging in regelgeving worden vastgelegd. Er is gekozen om deze regels in een ministeriele regeling op te nemen zodat deze regels voor eenieder bekend zijn, maar juist ook, zoals aangegeven in de artikelsgewijze toelichting, omdat een ministeriële regeling makkelijker en sneller kan worden aangepast dan een besluit. Een ander punt dat uit de uitvoeringstoets naar voren komt gaat over het voornemen om de BIO voor te schrijven, maar dat daarbij het Basis beveiligingsniveau (BBN) ontbreekt en de vraag of de BIO voldoende het risico kan dekken met betrekking tot de verwerking van bijzondere persoonsgegevens. De regering merkt hier nogmaals op dat in deze toelichting het voornemen is uitgesproken om de BIO voor te schrijven, waarmee een inzicht is gegeven in waaraan gedacht wordt. De daadwerkelijke regels komen zoals aangegeven terug in een ministeriele regeling. De opmerking van de NLA over het BBN wordt meegenomen.

De NLA merkt in de uitvoeringstoets verder op dat in het besluit en de daarbij behorende toelichting duiding ontbreekt over de hoeveelheid signalen die door de NLA worden ingebracht en de hoeveelheid signalen die door het IKZ wordt verrijkt. Dit kan volgens de NLA van invloed zijn op de beschikbare opsporingscapaciteit bij de NLA. De regering wijst erop dat de hoeveelheid signalen die door de NLA wordt ingebracht, een interne aangelegenheid is. Daarnaast komen bij het IKZ signalen van verschillende instanties binnen. Hoeveel dat er in totaal zullen zijn, welke daarvan voor verrijking in aanmerking komen, hoeveel daarvan na verrijking naar de verschillende instantie(s) gaat (gaan), is iets dat op voorhand niet kan worden aangegeven.

Ten slotte bevestigt de NLA dat gegevens over natuurlijke personen vallen onder het gesloten verstrekkingenregime van de Wpg en gegevens over rechtspersonen niet. Wel is het zo dat gegevens die de NLA bij het verrichten van haar taak verwerkt over natuurlijke en rechtspersonen, dusdanig nauw met elkaar verweven zijn dat het niet uitvoerbaar is om verschillende verstrekkingenregimes te hanteren. Vanwege deze nauwe verwevenheid in de uitvoering, heeft de regering het besluit aangepast door tussen persoonsgegevens en niet-persoonsgegevens voor Wpg-gegevens geen onderscheid te maken.

#### *NZa*

De NZa vraagt of voldoende is geborgd dat de informatie die door de betrokken instanties aan het IKZ worden verstrekt en door het IKZ vervolgens aan andere instanties wordt verstrekt, door die andere instantie slechts mag worden gebruikt ten behoeve van diens eigen wettelijke taken. Dit is geborgd. Allereerst door de doelbinding zoals geformuleerd in artikel 2.4, eerste en derde lid, van de wet, waarin staat dat verstrekking van een signaal aan het IKZ en het verstrekken van een verrijkt signaal door het IKZ aan een instantie, alleen kan als die verstrekkingen noodzakelijk zijn voor de bestrijding van fraude in de zorg. Daarnaast is in artikel 2.9, eerste lid, van de wet een geheimhoudingsplicht opgenomen, waardoor de ontvangen gegevens, waaronder persoonsgegevens, niet voor een ander doel mogen worden verwerkt dan op grond van de wet is toegestaan. Een andere vraag die de NZa stelt is in welke mate de Wet openbaarheid van bestuur (hierna: Wob) van toepassing is op de gegevens bij en handelingen van het IKZ. De Wob geeft in artikel 1a aan welke bestuursorganen onder de reikwijdte van de Wob vallen. Het IKZ is geen bestuursorgaan en valt derhalve niet onder de opsomming onder voornoemd artikel. Dit is onder de op 1 mei 2022 in werking getreden Wet open overheid (Woo) niet anders.

De NZa geeft verder aan dat zij op grond van de Wmg ook toezien op 'niet-basisverzekerde zorg' en doet een suggestie om artikel 3.14 (thans artikel 3.15) van het besluit aan te vullen. Deze suggestie wordt niet overgenomen, omdat door een wijziging van de omschrijving van fraude in de zorg en de tekst van artikel 2.4 van de wet de 'niet-basisverzekerde zorg', zoals de NZa dat aangeeft, onder de reikwijdte van die bepaling valt. In het verlengde daarvan is ook de omschrijving van het begrip zorg, hulp of ondersteuning in artikel 1 van het besluit aangepast.

De NZa merkt op dat er geen concrete invulling is van het begrip 'aanleiding tot een vermoeden van fraude', waardoor het voor hen niet duidelijk is of 'opzettelijke misleiding' vereist is om van een aanleiding tot een vermoeden van fraude te spreken. Zoals in de definitie in artikel 1.1 van de wet is opgenomen, gaat het bij fraude in de zorg om het opzettelijk misleidend handelen. De wet noch het besluit vereist dat een instantie bij het verstrekken van een signaal aan het IKZ het opzettelijk misleidend handelen dient te hebben bewezen. Er dient wel sprake te zijn van een aanleiding tot een vermoeden van opzettelijk misleidend handelen.

Volgens de NZa zijn de begrippen 'aanbieder' en 'zorg', door de in het besluit gehanteerde definities van deze begrippen, voor hen mogelijk ingeperkt ten opzichte van de reikwijdte die thans geldt voor de NZa op basis van de Wmg. Die gedachte deelt de regering niet. In artikel 2.4, eerste lid, van de wet staat namelijk dat verstrekking door instanties (waaronder de NZa) aan het IKZ plaatsvindt, indien de verstrekking noodzakelijk is voor de bestrijding van fraude in de zorg in het kader van de aan die instanties opgedragen wettelijke taken. De NZa is toezichthouder op de Wmg. De in die wet gehanteerde definities vallen derhalve onder het bereik van dit besluit.

De NZa geeft aan onduidelijkheid te lezen in paragraaf 4.4 over de gegevensset, omdat enerzijds wordt gezegd dat per geval moet worden bekeken welke gegevens uit de wet verstrekt worden en anderzijds dat niet kan worden gewerkt met een beperktere set. Deze passage is iets aangescherpt om aan te geven dat wordt bedoeld dat niet kan worden volstaan met het opnemen van een beperktere set in het besluit.

De NZa vraagt hoe de noodzakelijkheid van aanlevering van gegevens zich verhoudt tot het doel van fraudebestrijding, omdat er een verschil zou zitten in de gegevens die de NZa aanlevert bij verrijken van een signaal en de gegevens die de NZa aanlevert bij het verstrekken van een signaal. In artikel 3.9 van het besluit is opgenomen welke gegevens de NZa aan het IKZ, indien beschikbaar, verstrekt. Deze gegevensset geldt zowel voor de verstrekking van een signaal als voor de verrijking van signalen. Daarmee is er dus geen verschil, zoals de NZa aangeeft. Wel geldt bij iedere gegevensverwerking de vraag of een eventuele verwerking noodzakelijk is. Per geval zal daarom moeten worden afgewogen welke gegevens in dat specifieke geval worden verstrekt aan het IKZ.

Daarnaast geeft de NZa aan dat in het besluit niet wordt stilgestaan bij de taak onderzoek en analyse van het IKZ. De regering verwijst naar artikel 2.5 van de wet waarin deze taak is opgenomen. Zoals in dat artikel is aangegeven verwerkt het IKZ voor die taak, indien noodzakelijk, de gegevens bedoeld in artikel 2.4, eerste tot en met vierde lid, van de wet. Die gegevens zijn in het besluit aangewezen. Daarnaast wordt ten aanzien van de taak onderzoek en analyse ook een en ander geregeld in de artikelen 3.17, 3.20 en 3.21 van het besluit.

In de uitvoeringstoets heeft de NZa ook enkele opmerkingen gemaakt met betrekking tot de AVG. Deze opmerkingen leiden niet tot wijzigingen, mede gezien het feit dat de AP dergelijke opmerkingen niet heeft gemaakt.

Voor opmerkingen in deze uitvoeringstoets die betrekking hebben op de wet en al bij de uitvoeringstoets van de wet zijn ingebracht en beantwoord, verwijst de regering naar de memorie van toelichting bij de wet.

#### *Rijksbelastingdienst*

De rijksbelastingdienst concludeert in de uitvoeringstoets dat het besluit waarschijnlijk uitvoerbaar is. Voor een definitief oordeel over de uitvoerbaarheid zijn de uitkomsten van de ministeriele regeling en de werkafspraken van essentieel belang. Tevens geeft de rijksbelastingdienst aan dat er nog geen zekerheid is over het aantal verzoeken dat IKZ aan de rijksbelastingdienst voor een verrijking zal gaan doen. Hierna worden nog enkele andere punten uit de uitvoeringstoets van de rijksbelastingdienst benoemd.

De rijksbelastingdienst geeft aan dat het op basis van het besluit die voor uitvoeringstoets is voorgelegd, benchmarks moet verstrekken aan het IKZ. Dit is voor de rijksbelastingdienst nu niet mogelijk en zou ontwikkeld moeten worden. Dit ziet de rijksbelastingdienst als niet uitvoerbaar. Als gevolg hiervan is artikel 3.5 van het besluit gewijzigd. Onderdeel c van dat artikel is geschrapt. Het uitgangspunt bij het verstrekken

van conclusies uit benchmarkgegevens is namelijk dat de verstreckende instantie deze al heeft en niet specifiek voor de verstrekking aan het IKZ moet uitvoeren of ontwikkelen.

De rijksbelastingdienst merkt in de uitvoeringstoets op dat voor de FIOD geldt dat, zonder aanpassing van het Bpg, verstrekking aan het IKZ niet mogelijk is. Door aanpassing van het Bpg ontstaat een wettelijke rechtsgrond voor gegevensverstrekking aan het IKZ. De regering merkt op dat de aanpassing van het Besluit politiegegevens in artikel 4.1 van dit besluit is opgenomen.

Daarnaast maakt de rijksbelastingdienst een opmerking over artikel 3.25 (thans artikel 3.23) van het besluit dat gaat over een inspanningsverplichting om geautomatiseerd uit te wisselen. Voor de rijksbelastingdienst wordt in het derde lid van dat artikel een uitzondering gemaakt die vervolgens niet geldt voor de FIOD. Daarmee zou voor de FIOD een verplichting kunnen ontstaan om wel geautomatiseerd te moeten uitwisselen. De regering deelt die zienswijze niet. De regering hoeft de FIOD niet in voornoemd artikel uit te sluiten, omdat een dergelijke verplichting alleen via het Bpg kan worden opgelegd.

#### *Sociale verzekeringsbank*

De SVB geeft in de uitvoeringstoets aan geen handhavende taak op het gebied van fraude te hebben en ook geen bevoegdheden om op eigen initiatief onderzoek te verrichten. De SVB komt tot de conclusie dat de SVB niet de aangewezen instantie is om signalen dusdanig zorgvuldig te (kunnen) onderzoeken en de afweging te maken om het door te sturen naar het IKZ. De regering is van mening dat de SVB, ondanks het niet hebben van een handhavende taak, weldegelijk signalen kan verstrekken aan het IKZ. Die signalen kunnen namelijk noodzakelijk zijn voor een of meerdere van de in artikel 2.4, eerste lid, van de wet genoemde instanties voor de bestrijding van fraude in de zorg. In artikel 3.13 (thans artikel 3.14) van het besluit zijn vervolgens elementen genoemd die moeten worden meegenomen in de afweging of een signaal aan het IKZ kan worden verstrekt. Dat is zo opgenomen om te voorkomen dat ieder signaal, ook die nauwelijks een aanleiding tot een vermoeden van fraude in de zorg vormen en wanneer het dus niet proportioneel is, aan het IKZ worden verstrekt zonder enig vooronderzoek. Het hebben van een handhavende taak is daarbij niet als vereiste genoemd voor verstrekking van een signaal.

Daarnaast merkt de SVB op niet alle gegevens te kunnen leveren zoals opgenomen in artikel 3.7 in het besluit dat voor uitvoeringstoets is voorgelegd en verzoekt het artikel aan te passen. De gegevensset van de SVB is hierop aangescherpt en mede naar aanleiding van deze opmerking zijn ter verduidelijking de artikelen 3.1 tot en met 3.9 aangepast door in de aanhef op te nemen "voor zover deze daarover beschikt".

De SVB vraagt, verwijzend naar paragraaf 4.4.8 van deze toelichting, wat het praktisch gezien betekent als een budgethouder betrokken is bij een aanleiding tot een vermoeden van fraude, terwijl het een vereiste is dat declaratiegegevens geaggregeerd moeten worden aangeleverd. Bij het opvragen van declaratiegegevens, gaat het om declaratiegegevens van zorgaanbieders. Aangezien die declaratiegegevens medische gegevens bevatten, worden ze geaggregeerd. Hierdoor wordt het medisch beroepsgeheim niet doorbroken. In het geval een budgethouder, een natuurlijke persoon, betrokken is bij een aanleiding tot een vermoeden van fraude kunnen wel persoonsgegevens worden gedeeld, maar gegevens waar het beroepsgeheim op rust, mogen niet verstrekt worden aan het IKZ.

#### *VNG*

De VNG concludeert in de uitvoeringstoets dat het besluit goed uitvoerbaar is voor gemeenten. Wel geeft de VNG aan dat het gebruik van het Waarschuwingregister en het

uitwisselen van gegevens met het IKZ zal achterblijven als niet aan enkele randvoorwaarden is voldaan.

De VNG geeft aan dat de capaciteit bij gemeenten om onderzoek te doen naar misstanden bij zorgaanbieders beperkt is. De regering is van mening dat het Waarschuwingsregister en het IKZ gemeenten juist kunnen helpen. Beide onderdelen van de wet zullen bijdragen aan de aanpak van fraude in de zorg door gemeenten. Door het Waarschuwingsregister kunnen gemeenten eerder gewaarschuwd worden over zorgaanbieders die frauderen en door het IKZ kunnen gemeenten straks signalen ontvangen die verrijkt zijn en hen zullen helpen bij het uitvoeren van de toezichthoudende taak.

Een andere randvoorwaarde is dat naast onderzoek naar kwaliteit van zorg meer onderzoek moet worden gedaan naar fraude in de zorg. Dit besluit gaat over de aanpak van fraude in de zorg, terwijl de gemeenten bij het toezicht houden van de zorg zich vooral richten op de kwaliteit van de zorg. Gemeenten hebben echter ook een taak op het toezicht houden van de rechtmatigheid van de zorg en bij die taak kunnen zij gebruik maken van het Waarschuwingsregister en het IKZ.

Ten slotte merkt de VNG op dat gemeenten wat aan het Waarschuwingsregister en het IKZ moeten hebben. Daarbij spreekt de VNG van een relatieve verplichting voor gemeenten: "Het wordt aan de gemeente zelf overgelaten om te bepalen of registreren of melden nodig is.". Dit is echter niet juist. Gemeenten hebben voor verstrekking een eigen verantwoordelijkheid om af te wegen of de te verstrekken gegevens noodzakelijk zijn voor de bestrijding van fraude in de zorg. Indien die afweging leidt tot de conclusie dat sprake is van een noodzakelijkheid om te verstrekken, is sprake van een verplichting om te verstrekken.

#### *Zorgverzekeraars Nederland*

ZN geeft aan dat de aanvullende verzekering ontbreekt in artikel 1 van het besluit, waardoor gegevens over een aanvullende verzekering niet met het IKZ gedeeld kunnen worden of een gerechtvaardigde overtuiging van fraude met een aanvullende verzekering niet via het Waarschuwingsregister gedeeld kunnen worden. De regering is van mening dat de aanvullende verzekering niet ontbreekt. Dit blijkt uit de begripsomschrijving van ziektekostenverzekeraar in artikel 1.1 van de wet. Daarnaast wordt in artikel 2.4, eerste lid, van de wet geen limitatieve lijst met wetten genoemd. De Wmg, waar de aanvullende verzekering genoemd wordt, valt onder de reikwijdte van artikel 2.4, eerste lid, van de wet. In artikel 2.1 van de wet komt dit mogelijk minder duidelijk naar voren gekomen. Daardoor kan het lijken alsof geen gegevens over de aanvullende verzekering via het Waarschuwingsregister verstrekt kunnen worden. Om deze onduidelijkheid weg te nemen heeft de regering via een nota van wijziging de aanvullende verzekering toegevoegd artikel 1.1 en 2.1, eerste lid, van de wet.

Volgens ZN blijkt uit artikel 3.15 (thans artikel 3.16) van het besluit onvoldoende dat de uitvraag van gegevens (de verrijking) getrapd zal plaatsvinden. De regering merkt op dat de getrapte verrijking van gegevens, dat een onderdeel is van het verwerkingsproces, voldoende blijkt uit de systematiek van het besluit en de toelichting daarop.

ZN merkt op dat er een verschil is tussen 'gezondheidsgegevens' en 'gegevens waarop het medisch beroepsgeheim rust'. Dat op het enkele feit dat iemand een afspraak heeft met een hulpverlener het medisch beroepsgeheim rust, klopt volgens ZN niet. In hoofdstuk 2 van deze toelichting staat dit genuanceerder geformuleerd.

ZN vraagt of het bij declaratie- en indicatiegegevens gaat over 'niet tot natuurlijke personen herleidbare gegevens' of om 'geaggregeerde gegevens'. Waar het volgens de



regering hier om gaat is dat de gegevens die verstrekt worden aan het IKZ niet tot natuurlijke personen herleidbaar moeten zijn. Dat kan bereikt worden door de gegevens te aggregeren.

#### *Gebruikersoverleg BRP*

Ten aanzien van artikel 4.2 waarin de wijziging van het Besluit BRP is opgenomen is het gebruikersoverleg BRP conform artikel 1.15 van de Wet BRP geconsulteerd. Vanuit het gebruikersoverleg zijn geen bezwarende reacties gekomen.

#### 6.3 Internetconsultatie

Tijdens de internetconsultatie, die liep van 4 september 2020 tot en met 16 oktober 2020, hebben verschillende (branche)organisaties een reactie gegeven op het conceptbesluit.<sup>7</sup>

Hierna worden de belangrijkste punten benoemd en beschreven.

Artikel 4.2 van het besluit, waarin de wijziging van het Besluit BRP is opgenomen, maakte onderdeel uit van een amvb waarin meerdere derden, waaronder levensverzekeraars en klinisch genetische centra, werden aangewezen voor toegang tot de BRP. Een ontwerp van dat besluit is van 27 juli 2021 tot en met 7 september 2021 aangeboden voor internetconsultatie. In dat kader zijn er 84 reacties ontvangen. Verderop in deze paragraaf wordt ingegaan op de consultatiereacties voor zover die zien op de voorgestelde aanwijzing van het IKZ.

Een vraag die tijdens de internetconsultatie naar voren kwam was of een signaal over slechte kwaliteit van zorg ook een signaal van fraude in de zorg kan zijn. De regering merkt op dat het kan voorkomen dat een signaal over fraude in de zorg zo verweven is met slechte kwaliteit van zorg, dat deze twee niet los van elkaar kunnen worden gezien. Daarnaast werd de vraag gesteld of hetgeen in het besluit is geregeld, ook van toepassing is op een vertegenwoordiger waarbij het vermoeden bestaat dat hij betrokken is bij fraude in de zorg. De wet en het besluit regelen dat gegevens over natuurlijke personen en rechtspersonen uitgewisseld kunnen worden. Een vertegenwoordiger is hierbij niet uitgesloten. Tijdens de internetconsultatie is ook ingebracht dat er bij een onterechte opname in het Waarschuwingsregister geen mogelijkheden zijn voor de betrokken om zich hiertegen te verweren. Gepleit werd voor een laagdrempelige klachtenprocedure. Uit de AVG volgt onder andere dat een betrokkene zich tot de FG van een verwerkingsverantwoordelijke instantie kan wenden voor alle aangelegenheden die verband houden met de verwerking van zijn persoonsgegevens en met de uitoefening van zijn rechten uit hoofde van de AVG. Het gaat daarbij onder andere om klachten en verzoeken ten aanzien van die gegevensverwerking en de rechten in dat kader. In het besluit is voorgeschreven dat betrokken instanties zorgdragen voor een vergelijkbaar niveau van bescherming als het om andere gegevens dan persoonsgegevens gaat. Daarnaast is aangegeven dat zorgaanbieders ook direct op de hoogte zouden moeten worden gesteld van de signalen die vanuit een instantie naar het IKZ worden gestuurd, zodat zorgaanbieders de kans krijgen om ertegen in verweer te gaan. Daarbij is ook gesteld dat signalen over frauderende zorgaanbieders al op basis van enig vermoeden of zelfs 'onderbuikgevoelens' kunnen worden ingebracht bij het IKZ. Het IKZ is op grond van artikel 14 AVG verplicht de natuurlijke persoon of rechtspersoon te informeren als sprake is van een verwerking van persoonsgegevens. Hiervan kan alleen in uitzonderingsgevallen, genoemd in artikel 14, vijfde lid, AVG, worden afgeweken. Wat betreft het verstrekken van signalen aan het IKZ kan geen sprake zijn van het verstrekken op basis van 'onderbuikgevoelens'. Betrokken instanties kunnen signalen alleen verstrekken aan het IKZ als deze verstrekking noodzakelijk is voor de bestrijding van fraude in de zorg. De regering heeft in het besluit voorgeschreven opgenomen ten

---

<sup>7</sup> Waaronder de Koninklijke Nederlandse Beroepsorganisatie van Accountants, Platform Burgerrechten en een gezamenlijke reactie van de Vereniging Gehandicaptenzorg Nederland, de Nederlandse ggz en ActiZ.

aanzien van de afweging of het verstrekken van een signaal noodzakelijk is voor de bestrijding van fraude in de zorg.

Ten aanzien van de wijziging van het Besluit BRP (artikel 4.2 van het besluit) zijn in de internetconsultatie voornamelijk zorgen geuit ten aanzien van de werking van de wet en de mogelijke gevolgen daarvan voor betrokkenen. Het betreft onder andere het zwaarwegend belang dat de inbreuk op privacy rechtvaardigt, de rechtsbescherming en waarborgen en de onderbouwing van de noodzaak en proportionaliteit. Ten aanzien van de toegang tot BRP-gegevens zijn eveneens zorgen over noodzaak en waarborgen naar voren gebracht. De regering verwijst voor een reactie hierop naar de memorie van toelichting bij de wet alsmede hetgeen in de toelichting bij dit besluit over deze aspecten is opgenomen. Ten aanzien van het gebruik van gegevens uit de BRP wordt benadrukt dat dit alleen gegevens betreft van de betrokkene op wie het signaal van fraude betrekking heeft en dat de hiermee voor het IKZ mogelijk gemaakte controle juist een waarborg tegen onrechtmatige gegevensverwerking betreft. Hetgeen in reactie op het AP-advies en in de artikelsgewijze toelichting is opgenomen, verduidelijkt dit. De gegevens mogen niet voor een ander doel dan controle worden geraadpleegd en gegevens van anderen, zoals familieleden, mogen in geen geval worden geraadpleegd.

#### 6.4 Adviescollege Toetsing Regeldruk

Regeldruk is een verzamelnaam voor kosten die samenhangen met administratieve lasten (kosten om te voldoen aan informatieverplichtingen aan de overheid vanuit regelgeving), inhoudelijke nalevingskosten (kosten om te voldoen aan inhoudelijke eisen uit wet- en regelgeving) en toezichtlasten. Bij de totstandkoming van de wet is aandacht besteed aan de regeldrukaspecten. Geconcludeerd is dat de wet geen consequenties heeft op het gebied van regeldruk voor burgers, zorgondernemingen en zorgprofessionals. Het onderhavige besluit vormt een uitwerking van de in de wet opgenomen delegatiegrondslagen. Evenals de wet zelf, kent dit besluit geen consequenties op het gebied van regeldruk voor burgers, zorgondernemingen en zorgprofessionals. De uitvoeringslasten die het besluit met zich mee brengt gelden enkel voor de betrokken instanties aan wie verplichtingen worden opgelegd en voor het IKZ dat een wettelijke taak heeft.

Het eerste onderdeel van het besluit, betreffende onderlinge gegevensverstrekking tussen gemeenten en ziektekostenverzekeraars in het geval van een gerechtvaardigde overtuiging van fraude in de zorg, brengt beperkte regeldrukgevolgen met zich mee voor deze instanties. De betrokkenheid bij het opstellen van het protocol en de inrichting van het Waarschuwingsregister brengt eenmalig uitvoeringslasten met zich mee. Over het geheel genomen is de lastenverzwaring die dit onderdeel van het besluit met zich meebrengt voor betrokken instanties beperkt.

Ook het tweede onderdeel van dit besluit, betreffende de gegevensuitwisseling met het IKZ, brengt slechts een beperkte hoeveelheid extra uitvoeringslasten met zich mee voor de betrokken instanties genoemd in artikel 2.4, eerste lid, van de wet. Instanties zullen voor de verstrekking van signalen aan het IKZ een uitvoeringsproces moeten inrichten conform de vereisten in dit besluit. Ook zullen instanties met elkaar moeten samenwerken en het IKZ voorzien van heldere instructies ten aanzien van de gegevens die zij nodig hebben voor de uitvoering van hun wettelijke taken. Zoals in het kader van de regeldruktoets bij de wet reeds is opgemerkt, neemt de wet de knelpunten in de huidige samenwerking weg. In het kader van de uitvoering van hun wettelijke taken beschikken de betrokken instanties reeds over de gegevens die in dit besluit zijn aangewezen. De wet en het besluit maken het mogelijk dat de samenwerking tussen betrokken instanties en de uitwisseling van gegevens die daarbij noodzakelijk is, efficiënter en zorgvuldig kan plaatsvinden. Het belang bij een zorgvuldige gegevensverwerking, het verrijken van

signalen door het IKZ en het verstrekken daarvan aan de geëigende instantie(s), weegt voor betrokken instanties op tegen de regeldrukgevolgen die voortvloeien uit de verplichting tot het verstrekken van gegevens.

Daarnaast dienen betrokken instanties kennis te nemen van de inhoud van dit besluit. De daarmee gemoeide kennisnamekosten zijn echter vanwege de geringe omvang van het voorstel, de beperkte doelgroep en hun actieve betrokkenheid in het proces van totstandkoming van dit besluit, verwaarloosbaar.

Ten aanzien van de wijziging van het Besluit BRP in artikel 4.2 geldt dat met het opnemen van nieuwe werkzaamheden met een gewichtig maatschappelijk belang geen verplichtingen voor burgers gecreëerd. Van een lastenverzwaring voor de burger is derhalve geen sprake.

Verstrekingen aan het IKZ hebben naar verwachting geen lastenreductie voor de burger tot gevolg. Het betreft hier de verstrekking van gegevens ten behoeve van het controleren van gegevens die reeds bij het IKZ bekend zijn.

Het Adviescollege toetsing regeldruk heeft VWS laten weten de analyse en beschrijving van de gevolgen voor de regeldruk te delen.

## **ARTIKELSGEWIJS DEEL**

### *Artikel 1*

In dit artikel worden enkele begrippen gedefinieerd. Deze begrippen sluiten waar mogelijk aan bij reeds bestaande begrippen in andere regelgeving. Om te voorkomen dat vaak hele opsommingen moeten worden herhaald, zijn ook diverse opsommingen samengevat in een begrip.

De opsomming "zorg of overige dienst als omschreven bij of krachtens de Zorgverzekeringswet of aanvullende ziektekostenverzekering, zorg als omschreven bij of krachtens de Wet langdurige zorg, maatschappelijke ondersteuning als omschreven bij of krachtens de Wet maatschappelijke ondersteuning 2015 of jeugdhulp als omschreven bij of krachtens de Jeugdwet" is samengevat in het begrip 'zorg, hulp of ondersteuning'. Hiermee is niet beoogd enige inkadering aan te brengen ten opzichte van wat in de wet is geregeld, het is slechts de bedoeling om de leesbaarheid te bevorderen. Het begrip 'aanbieder' is aan het begrip 'zorg, hulp of ondersteuning' gekoppeld en betreft dus iemand die "zorg of overige dienst als omschreven bij of krachtens de Zorgverzekeringswet, zorg als omschreven bij of krachtens de Wet langdurige zorg, maatschappelijke ondersteuning als omschreven bij of krachtens de Wet maatschappelijke ondersteuning 2015 of jeugdhulp als omschreven bij of krachtens de Jeugdwet" aanbiedt. Het werkwoord 'aanbieden' moet in deze definitie niet beperkend worden opgevat. Net als het begrip 'fraude in de zorg', moet de term 'aanbieden' worden ingevuld aan de hand van wat gebruikelijk is binnen het rechtsgebied waarbinnen de handelingen plaatsvinden en waarbinnen de instanties opereren. De NZa zal zich dus in principe baseren op het begrip 'zorgaanbieder' uit de Wet marktwerking gezondheidszorg (Wmg), terwijl de IGJ bijvoorbeeld uit zal gaan van het begrip 'zorgaanbieder' uit de Wkkgz of 'jeugdhulpaanbieder' uit de Jeugdwet. Gegeven het op samenwerking gerichte karakter van de wet en dit besluit, ligt het ook voor de hand dat instanties rekening houden met elkaars invulling van de begrippen. Het enige beperkende element zit daarmee in de vraag of iets valt onder "zorg of overige dienst als omschreven bij of krachtens de Zorgverzekeringswet of aanvullende ziektekostenverzekering, zorg als omschreven bij of krachtens de Wet langdurige zorg, maatschappelijke ondersteuning als omschreven bij of krachtens de Wet maatschappelijke ondersteuning 2015 of jeugdhulp als omschreven bij of krachtens de Jeugdwet".

Ook de begrippen 'administratieve kenmerken van een rechtspersoon', 'declaratiegegevens', 'handelsgegevens' en 'identificerende gegevens van een natuurlijke persoon' zijn samenvattingen van opsommingen. Deze opsommingen zijn voornamelijk van belang voor de gegevensset. Voor een inhoudelijke toelichting op die begrippen, wordt daarom verwezen naar paragraaf 4.4 van het algemene deel van deze toelichting, die uitleg geeft over de gegevensset.

Het begrip 'instantie' wordt in deze regeling gedefinieerd als een van de instanties die worden genoemd in artikel 2.4, eerste lid, van de wet, met uitzondering van het Informatieknooppunt zorgfraude. Dat komt dus neer op het CIZ, (een van de) college(s) van burgemeester en wethouders van een gemeente, de IGJ, de NLA de rijksbelastingdienst, de FIOD, de SVB, (een van de) ziektekostenverzekeraars of de zorgautoriteit. Omdat het om een verwijzing gaat naar het deel van de wet dat over het Informatieknooppunt zorgfraude gaat, wordt de term in de tekst van dit besluit alleen gehanteerd in artikelen die op dat deel zien. In het deel dat ziet op het Waarschuwingsregister, wordt in dit besluit telkens verwezen naar 'colleges' en 'ziektekostenverzekeraars', om verwarring te voorkomen. In deze toelichting wordt dat onderscheid niet strikt aangehouden, maar kan uit de context worden afgeleid welke instanties worden bedoeld. Bij het deel van de wet en deze besluit dat ziet op het Waarschuwingsregister zijn immers alleen de colleges en ziektekostenverzekeraars betrokken, bij het deel van de wet en dit besluit dat ziet op het Informatieknooppunt zorgfraude zijn ook de overige instanties betrokken.

Het begrip 'KVK-nummer' duidt aan wat in het normale spraakgebruik ook met een KVK-nummer wordt bedoeld, voor zover dat voor dit besluit relevant is.

Met betrekking tot gerechtvaardigde overtuiging geldt dat hiervoor een verkorte aanduiding is opgenomen. Wat onder gerechtvaardigde inhoud moet worden verstaan is opgenomen in artikel 2.1.

#### *Artikel 2.1*

Het eerste lid van dit artikel geeft aan wat onder gerechtvaardigde overtuiging wordt verstaan. Het geeft vooral aan dat deze overtuiging gebaseerd dient te zijn op bewijsmiddelen en dat de overtuiging gebaseerd is op meer dan een vermoeden. In het protocol zal nog nader ingegaan worden op hoe tot deze overtuiging dient te worden gekomen. Zie ook paragraaf 3.2 van algemeen deel van deze nota van toelichting.

Het tweede lid vormt een uitwerking van artikel 2.1, eerste lid, van de wet. In dit artikel wordt bepaald welke gegevens colleges en ziektekostenverzekeraars op grond van dat artikel aan elkaar verstrekken. Voor rechtspersonen betreft het alleen administratieve gegevens, voor natuurlijke personen alleen identificerende gegevens. Er worden in dit kader geen gegevens verstrekt over de aard van de (gerechtvaardigde overtuiging van) fraude in de zorg. Wel worden de contactgegevens van de verstreckende instantie aan de verstrekking toegevoegd, zodat tijdens de gehele termijn waarbinnen de gegevens kunnen worden verstrekt (vier tot acht jaar) contact kan worden opgenomen met de verstreckende instantie. Dit contact is niet bedoeld om inhoudelijke informatie over de aard van de (gerechtvaardigde overtuiging) van fraude in de zorg uit te wisselen, maar kan bijvoorbeeld gebruikt worden om kennelijke onjuistheden door te geven. Tevens kan de ontvangende instantie op basis van die contactgegevens een betrokkene die gebruik wil maken van zijn rechten, verwijzen naar de juiste instantie. Onder de term 'door ziektekostenverzekeraars gehanteerde administratieve codes' valt in het bijzonder de AGB-code van de natuurlijke persoon of rechtspersoon wiens gegevens worden verstrekt, maar dit begrip is daartoe niet beperkt. Mogelijk gebruiken instanties nu of in de toekomst ook andere administratieve codes die hieronder vallen. Weliswaar is er sprake van een limitatieve opsomming die op grond van deze wet verstrekt worden, maar dat laat onverlet dat colleges elkaar onderling ook het BSN van natuurlijke personen verstrekken,

omdat dit een hogere mate van zekerheid oplevert over de identiteit van de persoon wiens gegevens worden verstrekt. Colleges zijn hiertoe bevoegd op grond van artikel 10 van de Wet algemene bepalingen burgerservicenummer. Ziektekostenverzekeraars hebben deze bevoegdheid in dit kader echter niet, dus door hen en aan hen wordt geen BSN verstrekt. Zie voor meer informatie over de gegevensset van het Waarschuwingsregister paragraaf 3.4 van het algemene deel van deze toelichting.

#### *Artikel 2.2*

Zoals te lezen valt in paragraaf 3 van het algemene deel van deze toelichting, is artikel 2.1, eerste lid, van de wet een grondslag voor de gegevensverstrekking die noodzakelijk is om een centraal registratiesysteem (aangeduid als 'het Waarschuwingsregister') te kunnen opzetten. Het Waarschuwingsregister zelf wordt niet in de wet en dit besluit geregeld, maar het voornemen om een centraal registratiesysteem zoals het Waarschuwingsregister in gebruik te nemen voor de verstrekking van gegevens, is, net als bij de wet, wel als uitgangspunt genomen bij dit besluit. Artikel 2.2 stelt eisen aan het protocol dat instanties moeten gebruiken om te komen tot de gerechtvaardigde overtuiging dat er sprake is van fraude in de zorg. Het protocol zelf wordt vastgesteld bij ministeriële regeling.

#### *Artikel 2.3*

In het eerste lid is een grondslag opgenomen om bij amvb regels te stellen aan de beveiliging van gegevens. Het voornemen bestaat om de Baseline Informatiebeveiliging (Stcrt. 2019, 26526) (hierna: BIO) voor te schrijven. De BIO stelt beveiligingsnormen voor die goed toepasbaar zijn bij de hier beoogde samenwerking tussen publieke instanties en ziektekostenverzekeraars. De BIO zelf verwijst via een 'pas toe of leg uit'-systematiek weer naar op de internationaal geaccepteerde normalisatienormen ISO 27001 en ISO 27002. Omdat deze verwijzing op niet dwingende wijze plaatsvindt, wordt voldaan aan aanwijzing 3.48 van de Aanwijzingen voor de regelgeving. Omdat het echter normen zijn van niet-publiekrechtelijke aard, moet de verwijzing daarnaar ingevolge aanwijzing 3.47 van die Aanwijzingen op statische wijze plaatsvinden. Informatiebeveiliging is echter een vakgebied dat zich snel ontwikkelt en om informatie ook in de toekomst veilig te houden, is noodzakelijk dat de beveiligingsvoorschriften met enige regelmaat worden herzien. Om die reden is gekozen voor verdere delegatie naar een ministeriële regeling. Een ministeriële regeling kan immers veel gemakkelijker en sneller worden aangepast dan een amvb. Zie voor meer informatie over de beveiliging van deze gegevens paragraaf 3.5 van het algemene deel van deze toelichting.

In het tweede lid wordt invulling gegeven aan het feit dat de colleges en ziektekostenverzekeraars ingevolge artikel 26 AVG gezamenlijk verwerkingsverantwoordelijkheid dragen voor persoonsgegevens die zij in het kader van artikel 2.1 van de wet verstrekken. Om die reden moeten zij gezamenlijk afspraken maken over hoe deze gegevens worden beveiligd en over de rechten die betrokkenen op grond van hoofdstuk III van de AVG hebben. Zie paragraaf 3.7 van het algemene deel van deze toelichting voor meer informatie hierover.

In het derde lid wordt het tweede lid van overeenkomstige toepassing verklaard op rechtspersonen over wie gegevens worden verwerkt. Dit betekent dat de rechten en verplichtingen die voortvloeien uit de AVG, mutatis mutandis, ook gelden voor rechtspersonen en de gegevens, waaronder niet-persoonsgegevens, die van hen worden verwerkt. Zie hiervoor paragraaf 3.6 van het algemene deel van deze toelichting. Omdat de AP niet kan fungeren als toezichthouder op de verwerking van niet-persoonsgegevens of daarin een rol als 'klachteninstantie' kan spelen, zijn artikel 13, tweede lid, onderdeel d, AVG en artikel 36 UAVG niet van overeenkomstige toepassing verklaard.

#### *Artikel 2.4*

Naast de gezamenlijke verantwoordelijkheid die colleges en ziektekostenverzekeraars hebben, zoals uitgewerkt in artikel 2.3, hebben zij ook allen een eigen individuele verantwoordelijkheid. Deze individuele verantwoordelijkheid is uitgewerkt in het onderhavige artikel. Specifiek wordt in het eerste lid geregeld dat de verstreckende instantie ervoor zorgdraagt dat een betrokkene bij hem zijn rechten als bedoeld in hoofdstuk III van de AVG tot uitoefening kan brengen. Tevens wordt in het tweede lid geregeld dat wanneer een betrokkene de verkeerde instantie benadert om zijn rechten in te roepen, de instantie het verzoek van de betrokkene doorstuurt aan de instantie die de gegevens van de betrokkene heeft verstrekt en de betrokkene daarover informeert. Net als het vorige artikel, is ook dit artikel van overeenkomstige toepassing op rechtspersonen en de gegevens, waaronder ook niet-persoonsgegevens, van hen die worden verwerkt. Dit wordt geregeld in het derde lid. Zie paragraaf 3.6 van het algemene deel van deze toelichting voor meer informatie over de uitoefening van de rechten van betrokkenen.

#### *Artikel 2.5*

Om proportionaliteit van de verstrekking door middel van het Waarschuwingsregister (ook wel 'registratie' genoemd) en de periode waarbinnen deze gegevens kunnen worden geraadpleegd te waarborgen, moet de termijn hiervan worden gelimiteerd. Onverminderd de plicht om ingevolge artikel 2.1, vierde lid, van de wet een registratie te beëindigen wanneer niet langer de gerechtvaardigde overtuiging bestaat dat de geregistreerde fraude in de zorg heeft gepleegd, worden in dit artikel daarom algemene maximumtermijnen gesteld. Het uitgangspunt is dat een registratie na verloop van vier jaren wordt verwijderd. Deze termijn wordt aan het begin van de registratie aan de geregistreerde medegedeeld, tenzij sprake is van een uitzonderingssituatie van de informatieplicht als bedoeld in artikel 14, vijfde lid, AVG. Als een andere instantie, nadat de registratie is aangevangen, op een later moment eveneens een gerechtvaardigde overtuiging heeft, dan kan deze instantie ook verstrekken en daarvoor geldt dan weer een 'nieuwe' termijn. De betreffende andere instantie moet dan uiteraard wel zelf de gerechtvaardigde overtuiging kunnen onderbouwen met voldoende bewijsstukken.

Indien echter sprake is van voldoende verzwarende omstandigheden, kan ook worden besloten dat een registratie voor een periode van maximaal acht jaar geldt. Ook deze termijn wordt aan het begin van de periode bepaald en, onder dezelfde voorwaarden, medegedeeld aan de geregistreerde, met als verschil dat in de laatste vier jaar jaarlijks wordt heroverwogen of deze langere termijn nog proportioneel is. Het eventuele gevolg van die heroverweging is dat de registratie eerder dan na acht jaar wordt verwijderd. Zie paragraaf 3.5 van het algemene deel van deze toelichting voor een nadere uitleg van wat onder verzwarende omstandigheden wordt verstaan. Uiteraard moeten bij de overweging om een registratie voor acht jaar aan te gaan ook verlichtende omstandigheden worden meegewogen. Om willekeur in de door verschillende instanties toegepaste termijnen te voorkomen, moet over de afweging van verzwarende en verzachtende omstandigheden ingevolge artikel 2.2, tweede lid, onderdeel d, van dit besluit een instructie in het protocol worden opgenomen. Zie paragraaf 3.5 van het algemene deel van deze toelichting voor meer informatie over bewaartermijnen en termijnen van verstrekking.

In het derde lid wordt bepaald dat gegevens die noodzakelijk zouden zijn om (eventueel achteraf) de rechtmatigheid van de registratie te kunnen aantonen, langer mogen worden bewaard. Deze termijn is variabel en hangt af van de mate waarin nog rechtsmiddelen open staan tegen de registratie, waarvoor de registrerende instantie bewijs van de rechtmatigheid daarvan zou moeten kunnen leveren. De geregistreerde zou bijvoorbeeld een rechtszaak wegens (vermeende) onrechtmatige daad kunnen starten, aangifte kunnen doen wegens (vermeende) smaad of laster, of, in het geval van de verwerking van persoonsgegevens, een klacht kunnen indienen bij de AP. Zolang de mogelijkheid tot het starten van dergelijke procedures nog niet is verjaard en/of reeds gestarte procedures nog niet tot een definitief einde zijn gekomen, moet de betreffende instantie in staat

worden gesteld om (persoons)gegevens te bewaren die de rechtmatigheid van die registratie kunnen aantonen. De gegevens mogen echter niet voor een ander doel worden gebruikt. Denkbaar is dus dat een registratie reeds wegens het verlopen van de termijn is verwijderd, maar dat tegen die registratie nog een rechtszaak loopt, waarvoor de instantie gegevens bewaart en inbrengt in de rechtszaak.

#### *Artikelen 3.1 tot en met 3.9*

In de artikelen 3.1 tot en met 3.9 is vastgelegd welke gegevens het CIZ, de colleges, de Inspectie gezondheidszorg en jeugd, de NLA, de rijksbelastingdienst, de FIOD, de Sociale verzekeringsbank, ziektekostenverzekeraars en de zorgautoriteit op grond van artikel 2.4, eerste lid, van de wet aan het IKZ moeten verstrekken. Op deze gegevensset is nader ingegaan in paragraaf 4.4 van het algemene deel van deze toelichting. Het begrip 'aanleiding tot een vermoeden' geeft in deze artikelen een minimumniveau van vermoeden van fraude in de zorg aan. De artikelen zijn echter ook van toepassing op sterkere vermoedens. Zoals is uitgelegd in paragraaf 4.2.1.2, is de term 'vermoeden' hier niet bedoeld zoals in artikel 27 van het Wetboek van Strafvordering, maar gaat het om de betekenis die het in het normale spraakgebruik heeft.

Voor de bijzondere opsporingsdiensten wordt in deze artikelen slechts bepaald welke gegevens, niet zijnde politiegegevens, zij verstrekken. Zoals is bepaald in artikel 2.4, eerste lid, van de wet, vindt verstrekking van politiegegevens door de FIOD en de NLA immers plaats op grond van en met inachtneming van de Wpg. In dit besluit wordt daarom verder niets over politiegegevens geregeld. Zie hoofdstuk 2 van het algemene deel van deze toelichting voor meer informatie over politiegegevens. BOD's beschikken ook over gegevens die niet onder het begrip 'politiegegeven' vallen. Dat betreft, voor zover relevant voor deze artikelen, gegevens over rechtspersonen waarin geen persoonsgegevens voorkomen. De naam van de bestuurder van een rechtspersoon is bijvoorbeeld een persoonsgegeven en, als de FIOD of NLA over die naam beschikt, daarmee een politiegegeven. Het telefoonnummer van de rechtspersoon is geen persoonsgegeven en daarom geen politiegegeven. Het eerste lid van de artikelen 3.4 en 3.6 regelt daarom welke van deze laatste gegevens over rechtspersonen door de FIOD en NLA worden verstrekt.

In de praktijk is het echter vaak zo dat de niet-politiegegevens nauw verbonden zijn met politiegegevens. Wanneer gegevens gaan over een rechtspersoon, gaat een deel van de gegevens vaak over personen, bijvoorbeeld bestuurders, van die rechtspersoon. Het is daardoor voor de bijzondere opsporingsdiensten moeilijk, zo niet onmogelijk, om deze typen gegevens strikt van elkaar te scheiden en volgens verschillende regimes te verstrekken. Daarom is in het tweede lid van de artikelen 3.4 en 3.6 een uitzondering gemaakt. Niet-politiegegevens die nauw zijn verbonden aan politiegegevens worden door de FIOD en NLA slechts verstrekt indien ook deze verbonden politiegegevens worden verstrekt. In de praktijk betekent dit dus dat de verstrekking van deze niet-politiegegevens afhankelijk is van de beoordeling van de vraag of de politiegegevens verstrekt zullen worden. Het is aan de betreffende bijzondere opsporingsdienst om te beoordelen welke gegevens inderdaad dusdanig nauw met elkaar zijn verbonden dat verbonden verstrekking noodzakelijk is.

Voor de verstrekking van politiegegevens is in artikel 4.1 van dit besluit een wijziging opgenomen van artikel 4.3, eerste lid, van het Besluit politiegegevens.

Uit het feit dat een soort gegeven is opgenomen in de gegevensset, volgt niet de verplichting om dit gegeven te verkrijgen of te genereren. Een instantie die bijvoorbeeld op grond van de gegevensset conclusies uit benchmarkgegevens moet aanleveren, hoeft dat alleen te doen als deze reeds beschikking heeft over de relevante benchmarks. De instantie hoeft deze benchmarks echter niet te maken indien zij die nog niet bezit. Dit betekent echter niet dat instanties nooit bewerkingen op hun gegevens hoeven uit te voeren om gegevens aan het IKZ te leveren. In veel gevallen zal het immers nodig zijn om gegevens (deels) te aggregeren, pseudonimiseren of op andere wijze bepaalde

gegevens uit de tot hen ter beschikking staande gegevens te schrappen, alvorens de gegevens aan het IKZ kunnen worden verstrekt. Immers, alleen gegevens die voor instanties noodzakelijk zijn voor de bestrijding van fraude in de zorg worden aan het IKZ verstrekt.

#### *Artikel 3.10*

Sommige van de gegevens die op grond van artikel 2.4, eerste lid, van de wet worden verwerkt, vallen onder het begrip 'justitiële gegevens' of het begrip 'strafvorderlijke gegevens' van de Wet justitiële en strafvorderlijke gegevens (hierna: Wjsg). Er is niet beoogd om enige wijziging aan te brengen in het regime van die wet, dergelijke gegevens kunnen alleen verstrekt worden indien de Wjsg dat toestaat. In artikel 3.10 is daarom voor de duidelijkheid opgenomen dat de Wjsg in acht wordt genomen bij verstrekkingen van gegevens onder die artikelen.

#### *Artikel 3.11*

In artikel 2.4, tweede lid, van de wet worden enkele bronnen genoemd waaruit het IKZ eigenstandig de bij dit besluit aangewezen gegevens kan verwerken. In dit artikel worden die gegevens aangewezen. Kortgezegd worden alle gegevens in die bronnen aangewezen die openbaar beschikbaar zijn. De jaarverantwoordingen op grond van de Wet marktwerking gezondheidszorg en de Jeugdwet zijn in hun geheel openbaar. Daarom worden alle gegevens die daarin voorkomen aangewezen. Het Handelsregister is slechts deels openbaar, daarom wordt alleen dat openbare deel aangewezen. Zie ook voor meer informatie over deze gegevens paragraaf 4.4 van het algemene deel van deze toelichting.

#### *Artikel 3.12*

In de tweede zin van artikel 2.4, derde lid, van de wet is bepaald dat het IKZ in beginsel geen gegevens uit een verrijkt signaal verstrekt aan ziektekostenverzekeraars, wanneer die gegevens afkomstig zijn van de rijksbelastingdienst of van de FIOD voor zover de FIOD taken uitvoert op grond van de AWR. Zie voor een inhoudelijk toelichting paragraaf 4.5 van het algemene deel van deze toelichting. Aan het slot van dat artikellid is echter bepaald dat bij amvb een uitzondering kan worden gemaakt op dat uitgangspunt. Artikel 3.12 regelt die uitzondering. De uitzondering komt er kortweg op neer dat het IKZ de betreffende gegevens wel aan ziektekostenverzekeraars kan verstrekken, wanneer het IKZ daartoe toestemming heeft verkregen van de rijksbelastingdienst of de FIOD (afhankelijk van welke instantie de gegevens heeft verstrekt). Het ligt in de rede dat het IKZ met de rijksbelastingdienst en de FIOD voor zover mogelijk algemene afspraken maakt over het soort gegevens en situaties waarin die toestemming wordt verleend, om willekeur zoveel mogelijk te voorkomen.

#### *Artikel 3.13*

Om te faciliteren dat het IKZ kan beoordelen welke instantie(s) het meest geëigend is of zijn om het verrijkte signaal in ontvangst te nemen, is in artikel 2.4, vierde lid, bepaald dat het daartoe gegevens aan instanties kan verstrekken en dat instanties dezelfde soort gegevens aan het IKZ kunnen verstrekken. Zie voor meer informatie over deze zogenaamde 'gerichte verstrekking' paragraaf 4.5, onder het kopje 'Gerichte verstrekking (om de meest geëigende instantie(s) te bepalen)'. In dit artikel is bepaald om welke gegevens dat gaat. De gegevens hebben de instanties nodig om te kunnen inschatten of zij het verrijkte signaal nodig hebben voor de aan hen opgedragen wettelijke taken op het gebied van de bestrijding van fraude in de zorg. Artikel 2.4, vierde lid, van de wet is bedoeld om dataminimalisatie te waarborgen, door te voorkomen dat direct het volledige verrijkte signaal aan een of meer instanties wordt verstuurd, terwijl niet duidelijk is of zij deze gegevens nodig hebben. Het is daarom ook expliciet niet mogelijk om op basis van



dit artikel het volledige verrijkte signaal te versturen. Dat moet plaatsvinden op grond van het derde lid van artikel 2.4, van de wet.

In het tweede lid is bepaald dat het eerste lid niet van toepassing is op politiegegevens. Ook politiegegevens die worden uitgewisseld ten behoeve van het bepalen van de meest geëigende instantie, worden uitgewisseld op grond van en met inachtneming van de Wpg. Persoonsgegevens die zich bij de NLA of de FIOD bevinden, vallen onder dit begrip 'politiegegeven'. Uitwisseling van deze gegevens ten behoeve van het bepalen van de meest geëigende instantie vindt dus plaats op grond van de Wpg. Het vereiste van noodzakelijkheid geldt onverminderd voor politiegegevens en het ligt daarom in de lijn der verwachting dat het soort politiegegeven dat wordt uitgewisseld ten behoeve van de gerichte verstrekking, inhoudelijk vergelijkbaar zal zijn met de gegevensset uit het eerste lid. Het eerste lid van het onderhavige artikel is wel van toepassing op andere gegevens dan politiegegevens die de NLA of de FIOD in dit kader met het IKZ uitwisselen.

#### *Artikel 3.14*

Artikel 3.14 ziet alleen op de situatie waarin instanties een aanleiding tot een vermoeden van fraude in de zorg ('signaal') aan het IKZ moeten verstrekken, niet op de situatie dat het IKZ verzoekt om gegevens ter verrijking. Zie voor meer informatie over het signaal paragraaf 4.2 van het algemene deel van deze toelichting. Het is vrijwel onmogelijk om vooraf in regelgeving exact vast te leggen wat een signaal precies is en onder welke omstandigheden deze naar het IKZ verzonden moet worden, zonder daarmee de werking van het IKZ zover wordt ingeperkt dat vele vormen van fraude in de zorg het IKZ nooit halen en het kerndoel van het IKZ wordt aangetast. Een exacte beschrijving van de bewijsmiddelen die noodzakelijk zijn om een signaal voldoende te kunnen onderbouwen, zal noodzakelijkerwijze erg lang en waarschijnlijk nooit volledig zijn, waardoor ook dat ertoe zou leiden dat veel signalen van fraude in de zorg niet aan het IKZ worden gemeld. Aan de andere kant moet voor partijen voldoende voorzienbaar zijn wanneer onder de wet gegevens van hen worden verwerkt en moet worden voorkomen dat met al te ruime mogelijkheden te lichtzinnig wordt omgegaan met gegevens en de verstrekking daarvan aan het IKZ.

Dit artikel is bedoeld om tussen die afwegingen een balans te vinden, door nader in te kaderen hoe een signaal van fraude in de zorg moet worden opgebouwd. Het artikel komt er grofweg op neer dat een instantie goed moet onderbouwen waarom er sprake is van een aanleiding tot een vermoeden van fraude in de zorg, wat daarvoor de (feitelijke) onderbouwing is, waarom het noodzakelijk is om dit signaal te verstrekken aan het IKZ en welke gegevens, die via het IKZ zouden kunnen worden verkregen, het signaal verder zouden kunnen onderbouwen.

#### *Artikel 3.15*

Artikel 3.15 geeft een invulling aan het noodzakelijkheidsvereiste voor de gegevensverwerking door het IKZ en de uitvoering van het verrijkingproces. Zoals uit het artikel blijkt, doet het niet af aan het algemene vereiste dat het IKZ in alle gevallen slechts gegevens mag verwerken indien dit noodzakelijk is voor de bestrijding van fraude in de zorg, maar kadert het dit vereiste wel ten dele nader in. In het eerste onderdeel is bepaald dat het IKZ slechts een gegevensuitvraag doet naar aanleiding van een signaal dat het van instanties heeft verkregen. Hiermee wordt beoogd om uit te sluiten dat het IKZ op eigen initiatief een uitvraag zou doen. Een uitvraag moet immers altijd verband houden met een signaal dat het van een instantie heeft verkregen. Het IKZ heeft op grond van de wet enkel de taak instanties te ondersteunen bij het bijeenbrengen van gegevens ten aanzien van signalen van die instanties. Het IKZ heeft geen taak of bevoegdheid zelf het onderzoek naar signalen van fraude te initiëren. Vervolgens moet het IKZ voordat het een uitvraag doet, kortgezegd, afwegen of die uitvraag wettelijk en praktisch tot een nuttig resultaat zou kunnen leiden. Indien het IKZ bijvoorbeeld bij voorbaat al weet dat het soort gegevens dat het nodig heeft, niet het type gegevens betreft waarover de

instanties beschikken, dan is het zinloos om een uitvraag te doen. Daarmee zou de uitvraag niet noodzakelijk zijn en dus niet toegestaan. Zie paragraaf 4.3 van het algemene deel van deze toelichting voor meer informatie over het verrijgingsproces.

#### *Artikel 3.16*

Om verder te waarborgen dat het verrijgingsproces proportioneel, zorgvuldig en rechtmatig verloopt, is in het eerste lid een bepaling opgenomen over de zogenaamde getrapte verrijking. Dit houdt in dat het IKZ bij het verrijken van een signaal niet direct een uitvraag doet naar alle in dit besluit aangewezen gegevens van betrokken instanties, maar het verrijgingsproces en daarmee ook de uitvraag waar mogelijk opdeelt in verschillende treden. Per trede doet het IKZ dan een beperkte uitvraag en aan de hand van de verkregen gegevens bepaalt het vervolgens of een volgende uitvraag trede van verrijking nog gerechtvaardigd is. Daarmee wordt onnodige gegevensverwerking voorkomen. Zie hierover ook paragraaf 4.3.1 van het algemene deel van deze toelichting. Het IKZ kan, eventueel in overleg met betrokken instanties, besluiten een of meer treden aan het proces toe te voegen, maar in de onderdelen a tot en met d van het eerste lid zijn enkele verplichte treden opgenomen.

In onderdeel a is bepaald dat de eerste fase van het verrijgingsproces altijd bestaat uit een controle van de identificerende gegevens die in het signaal zitten en een beoordeling van de reikwijdte van het signaal. Indien de identificerende gegevens incompleet of niet volledig juist zijn, verzoekt het IKZ de instantie het signaal te corrigeren, respectievelijk opnieuw, correct, in te dienen. Indien de gegevens wel juist en volledig zijn, of deze zijn gecorrigeerd of aangevuld, beziet het IKZ, conform onderdeel b, of dit signaal ziet op een (rechts)persoon van wie op dat moment al gegevens in het zaakinformatiesysteem staan. Als dat het geval is, moeten beide zaken mogelijk worden samengevoegd. In dat geval gaat de bewaartermijn van de oude gegevens ook gelden voor de gegevens van het nieuwe signaal die hieraan worden toegevoegd. Zie hiervoor de toelichting bij artikel 3.17. Onderdeel c schrijft voor dat het IKZ vervolgens aan de hand van de reikwijdte van het signaal bepaalt wat de reikwijdte van de volgende trede moet zijn. Indien bijvoorbeeld direct duidelijk is dat een bepaalde zorgaanbieder slechts in een bepaalde regio of bepaald domein actief is, is het waarschijnlijk niet noodzakelijk om gegevens te vragen van instanties in andere regio's of domeinen. Maar de conclusie uit de overweging kan ook zijn dat er onvoldoende grond is om de reikwijdte in te kaderen. In dat geval zal het IKZ in de volgende trede(n), met inachtneming van het uitgangspunt van proportionaliteit, een brede gegevensuitvraag moeten doen. In onderdeel d is bepaald dat voordat een uitvraag wordt gedaan om specifieke, extra gevoelige, gegevens te ontvangen, eerst wordt bekeken of er nog andere treden kunnen worden genomen waarin niet om deze gegevens wordt gevraagd.

Zie paragraaf 4.3.1 van het algemene deel van deze toelichting voor meer informatie over de getrapte verrijking.

#### *Artikel 3.17*

In dit artikel worden de bewaartermijnen bepaald voor de gegevens die het IKZ op grond van de wet verwerkt. In het eerste lid wordt bepaald dat de bewaartermijn voor gegevens die het IKZ verwerkt in het kader van het verrijken en gerichte verstrekking van signalen in principe vijf jaar betreft. Uiteraard worden gegevens eerder verwijderd wanneer niet langer (ten minste) een aanleiding tot een vermoeden van fraude in de zorg bestaat. Gegevens waarmee een signaal wordt verrijkt, worden gebundeld met het initiële signaal en worden daarmee gekoppeld aan de bewaartermijn van dat signaal. Deze gegevens moeten dus worden verwijderd wanneer het betreffende signaal wordt verwijderd. Dat wordt geregeld in het tweede lid.

In het derde lid is de bewaartermijn bepaald voor de andere taak van het IKZ, te weten onderzoek en analyse. Deze termijn is gesteld op tien jaar. Deze termijn is noodzakelijk om over meerdere jaren trends en ontwikkelingen te kunnen waarnemen. De termijn is

ook proportioneel, omdat deze gegevens nooit zullen worden gedeeld met andere instanties, slechts worden gebruikt voor onderzoek en analyse en de resultaten van dat onderzoek en die analyses niet herleidbaar zijn tot individuele (rechts)personen. De termijn is alleen van toepassing op persoonsgegevens en gegevens die herleidbaar zijn tot individuele rechtspersonen en dus niet op (volledig) geanonimiseerde gegevens. Voor geanonimiseerde gegevens geldt geen uiterste bewaartermijn.

Het vierde lid van dit artikel regelt dat gegevens die noodzakelijk zouden zijn om (eventueel achteraf) de rechtmatigheid van de verwerkingen te kunnen aantonen, langer mogen worden bewaard. Deze termijn is variabel en hangt af van de mate waarin nog rechtsmiddelen open staan tegen de registratie, waartegen de registrerende instantie zich moet kunnen verdedigen. De geregistreerde zou bijvoorbeeld een rechtszaak wegens (vermeende) onrechtmatige daad kunnen starten of, voor zover het over persoonsgegevens gaat, een klacht kunnen indienen bij de AP met mogelijke rechtsgevolgen. Zolang de mogelijkheid tot het starten van dergelijke procedures nog niet is verjaard en/of reeds gestarte procedures nog niet tot een definitief einde zijn gekomen, moet de betreffende instantie in staat worden gesteld om (persoons)gegevens te bewaren die de rechtmatigheid van die registratie kunnen aantonen. De gegevens mogen echter niet voor een ander doel worden gebruikt.

Zie paragraaf 4.7.4 van het algemene deel van deze toelichting voor meer informatie over de bewaartermijnen en de verwijdering van gegevens.

#### *Artikel 3.18*

De rechten uit hoofdstuk III van de AVG zijn onverkort van toepassing op natuurlijke personen van wie gegevens worden verwerkt. In dit artikel wordt bepaald dat het IKZ moet zorgen effectieve en kenbare processen voor de effectuering daarvan. Te denken valt aan duidelijke uitleg en contactgegevens op de website van het IKZ en, wanneer een persoon wordt geïnformeerd over het feit dat van diegene gegevens worden verwerkt, informatie over de wijze waarop diegene zijn rechten kan effectueren. Hoewel de AVG niet van toepassing is op niet-persoonsgegevens, maakt dat niet dat verwerken van de gegevens van rechtspersonen zonder waarborgen moet zijn. Temeer omdat in het kader van deze wet elke verwerking plaats vindt in het licht van de bestrijding van fraude in de zorg en de gevolgen voor betrokkenen groot kunnen zijn, hebben ook rechtspersonen bepaalde rechten. Om ook voor die rechtspersonen een hoog niveau van rechtsbescherming te garanderen en om de methode van rechtsbescherming met betrekking tot alle soorten gegevens zoveel mogelijk te uniformeren, wordt in dit artikel bepaald dat het IKZ voor rechtspersonen en de op hen betrekking hebbende gegevens, voor zover deze dus niet reeds zijn gedekt door de AVG, zorgdraagt voor een soortgelijke bescherming.

Zie paragraaf 4.7.5 van het algemene deel van deze toelichting voor meer informatie over de uitoefening van de rechten van betrokkenen.

#### *Artikel 3.19*

In dit artikel worden enkele zaken geregeld over bestuurders en medewerkers van het IKZ. Deze bepalingen zijn grotendeels overgenomen uit de Kaderwet zelfstandige bestuursorganen, in het bijzonder de artikelen 12, 13 en 14, en bevatten bijvoorbeeld regels over de wijze waarop bestuurders van het IKZ worden benoemd, geschorst of ontslagen, de bezoldiging van bestuurders, regels over nevenfuncties en tegenstrijdige belangen en regels over verantwoording. Indien nodig kunnen hierover bij ministeriële regeling nadere regels worden gesteld.

Zie ook voor een toelichting op de inhoud van dit artikel paragraaf 4.7.2 van het algemene deel van deze toelichting.

### *Artikel 3.20*

In dit artikel wordt de financiering, het jaarplan en de verslaglegging van en door het IKZ geregeld. De Minister voor LZS wordt in het eerste lid verantwoordelijk gesteld voor de financiering van het IKZ. Dit besluit regelt niet op welke wijze die financiering wordt vastgesteld, maar gedacht wordt aan een instellingssubsidie op grond van de Kaderwet VWS-subsidies. In het tweede lid wordt bepaald dat het IKZ jaarlijks een jaarplan moet vaststellen, waarin tenminste een begroting en een werkprogramma zijn opgenomen. In dat werkprogramma moet onder andere worden bepaald welke onderzoeken het IKZ in het kader van zijn taak op het gebied van onderzoek en analyse van plan is uit te voeren. De minister moet het jaarplan goedkeuren, zo is sturing op het IKZ geborgd. In het derde lid is bepaald dat het IKZ jaarlijks ook een jaarrekening en een bestuursverslag opstelt, zoals dat in titel 9 van Boek 2 van het Burgerlijk Wetboek omschreven is. Deze jaarrekening en dit bestuursverslag worden aan de minister gezonden. Indien nodig kunnen hierover bij ministeriële regeling nadere regels worden gesteld (vierde lid). Te denken valt aan nadere voorschriften aan de subsidie of de wijze en het tijdstip waarop de stukken aan de minister moeten worden gezonden. Zie paragraaf 4.7.2 van het algemene deel van deze toelichting voor meer informatie over het beheer van en de verantwoording door het IKZ.

### *Artikel 3.21*

In het eerste lid wordt bepaald dat medewerkers van het IKZ in het kader van hun werkzaamheden slechts toegang hebben tot de gegevens die zij in het kader van hun taken nodig hebben. Dit kan bijvoorbeeld mogelijk worden gemaakt door gegevens van verschillende betrokkenen of rechtspersonen gescheiden en beveiligd op te slaan en medewerkers alleen toegang te geven tot de gegevens van betrokkenen of rechtspersonen wiens zaak zij behandelen. De achterliggende reden is dat bij het IKZ een hoop gevoelige gegevens worden verwerkt en dat de principes van privacy by default en privacy by design vereisen dat toegang tot die gegevens zoveel mogelijk wordt beperkt. Uiteraard moet het werk van het IKZ daarbij wel redelijkerwijze uitvoerbaar blijven en is niet beoogd om deze scheidingen zo strikt aan te houden dat het IKZ daardoor elke flexibiliteit verliest en de processen ernstig vertraagd worden. In het tweede lid is een inspanningsverplichting opgenomen voor het IKZ om zijn processen, kortgezegd, zo privacyproof mogelijk in te richten. Het derde lid schrijft voor dat persoonsgegevens die worden gebruikt voor onderzoek en analyse, worden gepseudonimiseerd, zoals bedoeld in de AVG. Dat houdt in dat de persoonsgegevens die zich in de analyseomgeving bevinden, niet direct te herleiden zijn tot individuele betrokkenen, tenzij men beschikt over de juiste aanvullende gegevens (sleutel) om die informatie te ontsluiten. Voor veel verwerkingen in onderzoek en analyse is die informatie immers niet nodig. Het is echter niet uit te sluiten dat die gegevens soms wel nodig zullen zijn, daarom mogen de gegevens voor dergelijke verwerkingen worden ontsleuteld. Het IKZ zal dus moeten blijven beschikken over de sleutel, maar het ligt in de rede om het aantal medewerkers met toegang tot die sleutel te beperken. Dit lid is van overeenkomstige toepassing op gegevens die herleidbaar zijn tot individuele rechtspersonen. In het geval van die gegevens moet dus telkens in plaats van 'betrokkene' of 'natuurlijke persoon' worden gelezen 'rechtspersoon' en in plaats van 'persoonsgegevens' worden gelezen 'gegevens die herleidbaar zijn tot individuele rechtspersonen'.

### *Artikel 3.22*

Dit artikel is geformuleerd naar analogie van artikel 20 van de Kaderwet zelfstandige bestuursorganen en stelt de minister in staat om inlichtingen van het IKZ te verkrijgen. Dat is nodig omdat de minister in het algemeen verantwoordelijk is voor het zorgdomein en de inrichting en het functioneren van het zorgstelsel. Gelet op het doel van het IKZ, het ondersteunen van betrokken instanties bij het bestrijden van fraude in de zorg, valt

het IKZ beleidsmatig onder zijn verantwoordelijkheid. De verantwoording door het IKZ jegens de minister strekt zich niet uit tot casuïstiek. Het derde lid bepaalt dat het IKZ aan de minister geen persoonsgegevens of gegevens verstrekt die te herleiden zijn tot individuele rechtspersonen.

#### *Artikel 3.23*

In het eerste lid is bepaald dat alle gegevensuitwisselingen die op basis van artikel 2.4 van de wet tussen het IKZ en de in het eerste lid van dat artikel genoemde instanties elektronisch plaatsvindt. Het IKZ is verantwoordelijk voor de instandhouding van de voorzieningen daartoe.

In het tweede lid is bepaald dat het IKZ en de instanties gezamenlijk toe werken naar een geautomatiseerde uitwisseling van deze gegevens. Wanneer geautomatiseerde gegevensuitwisseling goed geïmplementeerd wordt, kan dit ertoe leiden dat minder personen toegang hoeven te hebben tot te verwerken (persoons)gegevens, wat een bijdrage levert aan dataminimalisatie. Tevens kan dit zorgen voor een sneller en efficiënter proces en een beperking van de administratieve lasten. Ten tijde van het schrijven van dit besluit, is deze automatisering echter nog niet gerealiseerd. Daarom regelt dit lid een inspanningsverplichting voor het IKZ en de betrokken instanties om te werken aan deze automatisering. De verwachting is dat deze automatisering in de toekomst, al dan niet stapsgewijs, gerealiseerd wordt. De wens is dat op dat moment geautomatiseerde gegevensuitwisseling de norm wordt. Om mogelijk te maken dat de automatisering op enig moment verplicht wordt voltooid en de gegevensuitwisseling geautomatiseerd plaatsvindt, kan bij ministeriële regeling ook een resultaatsverplichting worden opgelegd aan het IKZ en/of de instanties. Deze verplichting kan zien op de mate waarin het ontwikkelen van een geautomatiseerd systeem voor uitwisseling voltooid moet zijn en de mate waarin de gegevensuitwisseling geautomatiseerd moet plaatsvinden. De verplichtingen hoeven niet direct te zien op een volledige automatisering, denkbaar is dat op enig moment een deel van de gegevens geautomatiseerd kunnen worden uitgewisseld en dat deel dan verplicht wordt gesteld. Tevens kan worden gedifferentieerd tussen de verschillende instanties en het IKZ. Denkbaar is immers ook dat automatisering tussen bepaalde instanties en het IKZ al (geheel of gedeeltelijk) mogelijk is en tussen andere instanties en het IKZ (geheel of gedeeltelijk) nog niet.

In het vierde lid is bepaald dat de vorige leden niet van toepassing is op gegevensuitwisseling met de rijksbelastingdienst. Dit betekent dat voor die gegevensuitwisseling niet de inspanningsverplichting geldt om te werken automatisering hiervan of het bijbehorende systeem en niet de mogelijkheid geldt om deze automatisering op enig moment bij ministeriële regeling verplicht te stellen. Het bovenstaande sluit overigens niet uit dat (een deel van) de bovengenoemde gegevensuitwisseling op enig moment in de toekomst alsnog geautomatiseerd zal plaatsvinden, maar daartoe is dan de vrijwillige samenwerking van het IKZ en de rijksbelastingdienst noodzakelijk.

Zie het algemene deel van deze toelichting voor meer informatie over elektronische en geautomatiseerde gegevensuitwisseling.

#### *Artikel 3.24*

Het IKZ vervult een belangrijke ondersteunende rol in de uitwisseling van gegevens tussen de instanties. Om die uitwisseling op een zorgvuldige, efficiënte en veilige manier te laten plaatsvinden, houdt het IKZ daartoe elektronische voorzieningen in stand. Het IKZ helpt de instanties bij het gebruik van deze elektronische voorzieningen. Dat wordt in dit artikel geregeld.

Zie paragraaf 4.7 van het algemene deel van deze toelichting voor meer informatie over het beheer en de inrichting van de elektronische voorzieningen.

### *Artikel 3.25*

In het eerste lid is opgenomen dat het IKZ en de andere instanties afspraken maken over hun samenwerking en de termijn waarbinnen gegevensverstrekking normaal gesproken plaatsvindt. Deze afspraken zullen nodig zijn om het proces goed te laten verlopen en om uniformiteit aan te brengen in de wijze waarop alle partijen met de gegevensuitwisseling omgaan.

In het algemene deel van deze toelichting wordt meer uitgelegd over de afspraken die instanties samen moeten maken.

Het is niet de bedoeling dat het IKZ als een soort zwarte doos te werk gaat. Voor personen en rechtspersonen moet redelijkerwijze voorzienbaar zijn onder wat voor omstandigheden hun gegevens bij het IKZ zullen worden verwerkt. Daarom wordt in het tweede lid van dit artikel bepaald dat het IKZ op hoofdlijnen de op grond van het eerste lid gemaakte afspraken moet publiceren, samen met de hoofdlijnen van zijn eigen werkprocessen. Daarbij wordt beoogd om een redelijk inzicht te geven in de manier van werken, zonder dat daarmee het werk van het IKZ in gevaar komt. Een te grote mate van inzicht in die werkprocessen kan het voor potentiële fraudeurs immers weer te makkelijk maken om buiten het zicht van het IKZ te blijven. Daartussen moet een redelijke balans worden gevonden. Bij ministeriële regeling zal worden bepaald hoe de publicatie moet plaatsvinden. Te denken valt aan publicatie op de website van het IKZ.

### *Artikel 3.26*

In dit artikel wordt geregeld dat over bepaalde zaken bij ministeriële regeling nadere regels kunnen worden gesteld. Dit gaat in de eerste plaats om praktische zaken met betrekking tot de wijze waarop verstrekking van gegevens op grond van artikel 2.4, eerste en tweede lid, van de wet, plaatsvindt. Te denken valt aan het aanwijzen van de software die hiervoor gebruikt moet worden.

In de tweede plaats gaat het om de wijze waarop de in de wet genoemde elektronische voorzieningen worden ingericht en het beheer daarvan. Hierbij valt te denken aan eisen over toegankelijkheid en interoperabiliteit van die voorzieningen.

In de derde plaats gaat het om de beveiliging van gegevens. Het voornemen bestaat om de Baseline Informatiebeveiliging (Stcrt. 2019, 26526) (hierna: BIO) voor te schrijven. De BIO stelt beveiligingsnormen voor publieke en semipublieke organisaties. De BIO zelf verwijst via een 'pas toe of leg uit'-systematiek weer naar op de internationaal geaccepteerde normalisatienormen ISO 27001 en ISO 27002. Omdat deze verwijzing op niet dwingende wijze plaatsvindt, wordt voldaan aan aanwijzing 3.48 van de Aanwijzingen voor de regelgeving. Omdat het echter normen zijn van niet-publiekrechtelijke aard, moet de verwijzing daarnaar ingevolge aanwijzing 3.47 van die Aanwijzingen op statische wijze plaatsvinden. Informatiebeveiliging is echter een vakgebied dat zich snel ontwikkelt en om informatie ook in de toekomst veilig te houden, is noodzakelijk dat de beveiligingsvoorschriften met enige regelmaat worden bijgewerkt. Om die reden is gekozen voor verdere delegatie naar een ministeriële regeling, een ministeriële regeling kan immers veel gemakkelijker en sneller worden aangepast dan een amvb.

Zie paragraaf 4.7 van het algemene deel van deze toelichting voor meer informatie over de beveiliging van de elektronische voorzieningen.

### *Artikel 4.1*

Bij het IKZ zijn twee instanties aangesloten die gegevens verstrekken op grond van de Wet politiegegevens (Wpg), namelijk de FIOD en de NLA. De Wpg kent een eigen systeem van gegevensverwerking. De wet en dit besluit beogen niet dat systeem te doorbreken, maar aan te sluiten bij de Wpg. Daartoe wordt een wijziging aangebracht in artikel 4.3, eerste lid, van het Besluit politiegegevens. Kortweg voegt deze wijziging het IKZ toe aan de lijst met instanties aan wie in principe politiegegevens kunnen worden verstrekt die worden verwerkt overeenkomstig de artikelen 8, 9, 10, eerste lid, onderdelen a en c en 13

van de Wpg. Dit wordt echter verder ingekaderd door het vereiste van noodzakelijkheid. Het Bpg kent een eigen regime om te beoordelen welke gegevens in een individueel geval mogen worden verstrekt, waarbij ook andere opsporingsbelangen worden meegewogen. Voor de verstrekking van politiegegevens geldt voor instanties dus niet een algemene verplichting tot verstrekking aan het IKZ, zoals voor de niet-politiegegevens uit de gegevensset wel het geval is. Het ligt overigens in de lijn der verwachting dat het type gegeven dat op grond van de Wpg aan het IKZ zal worden verstrekt, inhoudelijk vergelijkbaar zal zijn met de gegevens die zijn opgenomen in de gegevensset. Zie paragraaf 4.4.10 van het algemene deel van deze toelichting voor meer informatie over politiegegevens.

#### *Artikel 4.2*

Dit artikel wijzigt het Besluit BRP. Hiermee zijn nieuwe werkzaamheden aangewezen als werkzaamheden met een gewichtig maatschappelijk belang ten behoeve waarvan systematisch gegevens uit de basisregistratie kunnen worden verstrekt. Bij de aanwijzing is tevens bepaald welke categorieën van derden voor de verstrekking in aanmerking komen en worden de werkzaamheden geclausuleerd. De werkzaamheden betreffen: het uitvoeren van de taken, bedoeld in artikel 2.4, derde lid, van de Wet bevorderen samenwerking en rechtmatige zorg ten behoeve van de bestrijding van fraude in de zorg (het Informatieknooppunt zorgfraude). Hiervoor dient bijlage 4 bij het Besluit BRP te worden aangevuld wat met bijgaande wijziging is geschied. In de aanwijzing is een beperking opgenomen ten aanzien van de gegevens die ten hoogste uit de BRP aan het IKZ verstrekt worden. Het betreft gegevens over de naam, de geboorte, het geslacht, het overlijden, het adres en het naamgebruik van degene op wie het signaal van fraude in de zorg betrekking heeft. Gegevens over gerelateerden (zoals ouder, partner en kind) kunnen op grond van dit besluit aldus niet verstrekt worden aan het IKZ. De gegevensset (derdenverstrekking) is daarmee beperkt tot de identificerende gegevens die het IKZ op grond van hoofdstuk 3, paragraaf 1, van dit Besluit verwerkt. Door verstrekking vanuit de BRP kan het IKZ de juistheid van deze gegevens controleren.

#### *Artikel 5.1*

In artikel 5.1 wordt voor de inwerkingtreding van dit besluit aangesloten bij de inwerkingtreddingsbepaling van de wet, in de zin dat de inwerkingtreding voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld. Immers moeten delen van de dit besluit in werking treden op het moment dat hun grondslag in werking treedt. Met dit artikel wordt dat mogelijk gemaakt.

#### *Artikel 5.2*

Ook de citeertitel van dit besluit is gekozen om aan te sluiten bij de citeertitel van de wet.

De Minister voor Langdurige Zorg  
en Sport,

Conny Helder