# Ambtelijk concept d.d. 04-09-2020
# Nota van toelichting bij het Besluit bevorderen samenwerking en rechtmatige zorg

**Nota van toelichting**

**ALGEMEEN DEEL**

## 1. Inleiding

### 1.1 Algemeen

Fraude met zorggeld is onacceptabel. Geld dat is bestemd voor de zorg, moet ook besteed worden aan zorg. In de zorgsector gaan jaarlijks miljarden om, bedragen die de premie- en belastingbetalers met elkaar moeten opbrengen. Fraude met zorggeld tast de betaalbaarheid van de zorg aan en ondermijnt de bereidheid van mensen om bij te dragen aan de kosten voor het zorgstelsel. Bovendien moeten zorgbehoevenden erop kunnen vertrouwen dat zij de zorg krijgen die ze nodig hebben en waar ze recht op hebben. De persoonlijke, financiële en maatschappelijke gevolgen van fraude in de zorg, vormen een zwaarwegend algemeen belang bij de bestrijding van die fraude.
Met de Wet bevorderen samenwerking en rechtmatige zorg (hierna: 'de wet') is beoogd de bestrijding van fraude in de zorg te verbeteren, door de mogelijkheden tot samenwerking en gegevensuitwisseling tussen in de wet genoemde betrokken instanties in dat kader te verbeteren. In het onderhavige Besluit bevorderen samenwerking en rechtmatige zorg (hierna: 'het besluit') zijn de gegevens aangewezen die op grond van de wet worden verstrekt. Ook bevat het besluit de nadere regels, uitwerking en invulling van de wet en de daarin opgenomen delegatiegrondslagen.

### 1.2 Wet bevorderen samenwerking en rechtmatige zorg

De wet voorziet hoofdzakelijk 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 kort gezegd 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 (AVG), gelden daarbij onverminderd. De verwerking van gegevens, waaronder de gegevensuitwisseling, moet rechtmatig zijn en dient plaats te vinden met oog voor de gevoeligheid van de gegevens en met zorg voor de privacy van betrokkenen. 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. In hoofdstuk 2 wordt dit toegelicht.

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 gegevens aan elkaar te verstrekken via een centraal registratiesysteem. De instanties kunnen elkaar met gebruik van dit systeem waarschuwen voor partijen ten aanzien van wie de gerechtvaardigde overtuiging bestaat dat die hebben gefraudeerd in de zorg. Dit systeem wordt door de betrokken instanties momenteel aangeduid als Waarschuwingsregister zorgfraude (hierna: 'het Waarschuwingsregister'). Het tweede onderdeel van de wet maakt mogelijk dat de in artikel 2.3 van de wet genoemde instanties, in het geval aanleiding tot een vermoeden van fraude in de zorg (een 'signaal') bestaat, gegevens verstrekken aan het Informatieknooppunt zorgfraude (IKZ). Het IKZ heeft een ondersteunende rol in de bestrijding van fraude in de zorg. Het IKZ vult de gegevens aan met gegevens uit de daartoe in de wet aangewezen bronnen en andere noodzakelijke gegevens van betrokken instanties (hierna ook aangeduid als 'verrijken') en verstrekt het resultaat daarvan (een 'verrijkt signaal') 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'). Dit 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 ook een taak om ten behoeve van de Minister van Volksgezondheid, Welzijn en Sport (hierna: 'de Minister van VWS') en de betrokken instanties trends en ontwikkelingen met betrekking tot fraude in de zorg te signaleren en daarover beleidsinformatie en statistische gegevens te ontwikkelen.

## 1.3 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. 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. Onder zorg wordt hier ook maatschappelijke ondersteuning en jeugdhulp verstaan. In het verlengde van het begrip zorg, ligt het begrip zorgaanbieder. Dat begrip heeft eveneens een gevarieerde reikwijdte in diverse wetten. In deze toelichting wordt met de term zorgaanbieder ook de verlener van maatschappelijke ondersteuning en jeugdhulp bedoeld. In artikel 1 van dit besluit wordt gelet op wetgevingssystematiek het begrip 'aanbieder' gebruikt. 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, van de AVG, genoemd, zoals verstrekken, verrijken en uitwisselen van persoonsgegevens. Waar het politiegegevens betreffen, moeten voornoemde begrippen overeenkomstig de invulling daarvan in de Wet politiegegevens worden uitgelegd.

### 1.4 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 politiegegevens. In hoofdstuk 3 wordt ingegaan op de uitwerking van de regels voor verstrekking van gegevens in een centraal registratiesysteem, zoals het Waarschuwingsregister, 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.

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

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 politiegegevens een bijzonder regime. Enerzijds ook in het kader 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 reeds toegelicht 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 hoofdstuk drie en vier.

### 2.1 Privacy

Bij de totstandkoming van de wet is de afweging gemaakt dat het zwaarwegende algemeen belang bij de bestrijding van fraude in de zorg 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 hier 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

CONCEPT

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 er ingevolge artikel 24 van de 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 van de 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 concrete 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 elk specifiek doel van de verwerking, zoals in het algemeen hiervoor beschreven. Het gaat om de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan.

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.

## 2.2 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 de wet is uitwisseling van gegevens waarop het medisch beroepsgeheim rust uitgesloten. In dit besluit is geregeld welke gegevens op grond van de wet verstrekt worden. In dat kader is hier 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 hulpverlener 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

CONCEPT

hieronder vallen. Ook op het enkele feit dat een patiënt een afspraak heeft met een hulpverlener rust het medisch beroepsgeheim.

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), in het onderdeel dat ook wordt aangeduid als Wet inzake de geneeskundige behandelingsovereenkomst (WGBO). Hieronder vallen alle hulpverleners die op grond van een behandelingsovereenkomst met de zorgbehoevende handelingen op het gebied van de geneeskunst verrichten. Een hulpverlener 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 patiënt. Bijvoorbeeld een assistent of secretaresse, maar ook ICT-medewerkers, bewakingspersoneel en schoonmakers.*

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

De gegevensset voor het IKZ bevat 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.

> *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 beroepsbeoefenaar of hulpverlener. Declaratiegegevens en indicatiegegevens zullen dan door instanties geaggregeerd moeten worden voordat de instanties ze aan het IKZ verstrekken.*

## 2.3 Politiegegevens

Persoonsgegevens die door instanties worden verwerkt als onderdeel van het toezicht dat zij op grond van hun wettelijke taak uitvoeren, vallen onder de AVG. Toezicht is erop gericht om mensen en organisaties zich te laten houden aan de norm. Daarnaast zijn er betrokken instanties, de bijzondere opsporingsdiensten (hierna: 'BOD's') FIOD en Inspectie SZW, die zich op grond van hun wettelijke taken bezighouden met de opsporing van

strafbare feiten. Er wordt van opsporing gesproken indien er 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 de Wet politiegegevens (Wpg) en worden aangeduid als ‘politiegegevens’. Vanaf het moment dat politiegegevens door het IKZ zijn ontvangen, is overigens 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 om het verstrekken van politiegegevens door FIOD en Inspectie SZW 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 BOD’s ten behoeve van de uitvoering van de wet politiegegevens aan het IKZ kunnen verstrekken.

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 2.3, 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 Waarschuwingsregister zorgfraude’)

## 3.1 Inleiding

Het eerste onderdeel van de wet biedt een wettelijke grondslag voor gemeenten en ziektekostenverzekeraars om elkaar onderling gegevens, waaronder persoonsgegevens, te verstrekken over partijen ten aanzien van wie een gerechtvaardigde overtuiging bestaat dat zij fraude hebben gepleegd in de zorg. Het uitgangspunt is dat indien sprake is van een gerechtvaardigde overtuiging, betrokken instanties verplicht zijn de gegevens te verstrekken. Of de gerechtvaardigde overtuiging van fraude er in een bepaald geval is, moet worden vastgesteld overeenkomstig een door voornoemde betrokken instanties op te stellen protocol. De verstrekking van gegevens op basis van deze grondslag moet ook noodzakelijk zijn in het kader van bestrijding van de fraude in de zorg. Ook aspecten ten aanzien van die afweging komen terug in het voornoemde protocol.

Deze wettelijke grondslag creëert tevens de mogelijkheid en kaders om deze gegevens uit te wisselen in een gezamenlijk systeem. De wet noch dit besluit schrijft een vorm van het systeem voor. De verstrekking van gegevens bij een gerechtvaardigd vermoeden van fraude is techniekonafhankelijk geregeld. Gedacht wordt aan een centraal registratiesysteem, dat door de hiervoor genoemde betrokken instanties momenteel wordt aangeduid als Waarschuwingsregister zorgfraude, kortweg het Waarschuwingsregister. Omdat betrokken instanties het voornemen hebben de verstrekking op grond van dit deel van de wet uit te voeren in de vorm van een registratie in het Waarschuwingsregister, wordt dit in het vervolg van dit hoofdstuk op die manier aangeduid.

Dit onderdeel van de wet biedt gemeenten en ziektekostenverzekeraars de mogelijkheid elkaar te waarschuwen voor fraudeurs in het zorgdomein. Deze instanties kunnen door het Waarschuwingsregister te raadplegen bijvoorbeeld controleren of een partij met wie ze een contract willen sluiten, in een ander domein fraude gepleegd heeft en maatregelen treffen indien dat het geval is. Zo kan (nieuwe) fraude worden voorkomen of kunnen de gevolgen ervan worden beperkt. Mogelijk gaat van het bestaan van een dergelijk register ook een preventieve werking uit. De persoonlijke, financiële en maatschappelijke gevolgen die het zwaarwegende algemeen belang vormen bij bestrijding van fraude in de zorg, rechtvaardigen de met dit onderdeel van de wet mogelijk gemaakte inmenging in de privacy van betrokkenen. Hiervoor is in paragraaf 2.1 onder verwijzing naar de wet aandacht aan deze afweging besteed.

Gelet op het doel en de werking van het Waarschuwingsregister en de (mogelijke) gevolgen daarvan voor betrokken partijen, zowel persoonlijk als zakelijk, worden hoge eisen gesteld aan de gronden voor opname in dat register en de verwerking van gegevens in dit kader. Ten aanzien van zowel persoonsgegevens als niet-persoonsgegevens gelden dan ook dezelfde waarborgen en maatregelen ten behoeve van een zorgvuldige en rechtmatige verwerking van gegevens. In dit hoofdstuk van de toelichting wordt daarom het begrip ‘gegevens’ gebruikt. Enkel wanneer er aanleiding toe is, wordt specifiek onderscheid gemaakt tussen persoonsgegevens en niet-persoonsgegevens.

Zoals in de memorie van toelichting bij de wet is toegelicht, worden de persoonsgegevens die in het Waarschuwingsregister worden opgenomen, geschaard onder persoonsgegevens van strafrechtelijke aard als bedoeld in artikel 10 van de AVG. Persoonsgegevens van dien aard mogen ingevolge de AVG alleen verwerkt worden als passende waarborgen zijn geboden ter bescherming van de rechten en vrijheden van betrokkenen. Daar wordt met dit besluit en het op te stellen protocol invulling aan gegeven. In dit besluit zijn nadere regels opgenomen over het opstellen van en de eisen aan het protocol. Ook bevat het besluit een uitwerking van regels ten aanzien van de gegevens die moeten worden verstrekt, de beveiliging van de gegevens, de bewaartermijnen en de verwijdering van gegevens en de uitoefening van de rechten van betrokkenen. Die regels worden in dit hoofdstuk toegelicht.

## 3.2. Opstellen protocol

Het protocol wordt ingevolge de wet opgesteld door de in artikel 2.1 van de wet opgenomen betrokken instanties. De wijze waarop de goedkeuring van het protocol door

de Minister van VWS plaatsvindt en de voorschriften die aan deze goedkeuring zijn verbonden, zijn in dit besluit opgenomen.

Het ligt in de rede dat het protocol in de praktijk wordt opgesteld door de Vereniging van Nederlandse Gemeenten (VNG) en Zorgverzekeraars Nederland (ZN). Dit zijn organisaties die de belangen van betrokken instanties, gemeenten respectievelijk ziektekostenverzekeraars, behartigen. Deze organisaties dienen te waarborgen dat voldoende afstemming met de door hen vertegenwoordigde betrokken instanties plaatsvindt, dat er bij die instanties draagvlak is voor het protocol en dat rekening is gehouden met de uitvoerbaarheid ervan.

Het protocol moet volledig zijn alvorens de Autoriteit persoonsgegevens (AP) erover wordt gehoord.

Nadat instanties de AP over het protocol hebben gehoord, moet het worden goedgekeurd door de Minister van VWS. Teneinde goedgekeurd te kunnen worden, moet het protocol voldoen aan wet- en regelgeving in het algemeen en aan de in dit besluit opgenomen eisen in het bijzonder. Het uitgangspunt is dat goedkeuring door de minister pas wordt gegeven nadat de AP een positieve reactie heeft gegeven op het protocol en er geen zwaarwegende bezwaren zijn aangedragen. Het protocol kan echter in afwijking van de reactie van het AP door de Minister van VWS worden goedgekeurd, mits eventuele zwaarwegende bezwaren gemotiveerd worden weerlegd. De goedkeuring van het protocol door de Minister van VWS is een besluit als bedoeld in de Algemene wet bestuursrecht (Awb). Dat besluit moet met het protocol worden gepubliceerd in de Staatscourant.

Met de in dit besluit opgenomen wijze van goedkeuren en daaraan gestelde voorschriften, wordt gewaarborgd dat de in het protocol opgenomen werkwijze en de verwerking van (persoons)gegevens (van strafrechtelijke aard) overeenstemt met de voorwaarden en waarborgen die zijn gesteld in de (U)AVG en de wet en dat voldoet aan de in dit besluit opgenomen voorwaarden, vereisten, maatregelen en waarborgen.

## 3.3 Eisen aan het 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 en passende waarborgen te bieden als bedoeld in artikel 10 van de AVG, is het van belang dat betrokken instanties heldere, objectieve en uniforme criteria hanteren bij de beoordeling of sprake is van een gerechtvaardigde overtuiging van fraude in de zorg (paragraaf 3.3.1) en een noodzaak tot verstrekking van de gegevens (paragraaf 3.3.2). Dit betekent dat vooraf voor betrokkenen duidelijk moet zijn op grond waarvan een partij geregistreerd kan worden en achteraf moet te toetsen zijn of die registratie rechtmatig is. Daarnaast zijn er andere voorwaarden, vereisten, maatregelen en waarborgen die in het protocol moeten terugkomen (3.3.3 en verder). In het protocol moet een weerslag en uitwerking van de eisen, waarborgen en maatregelen uit de (U)AVG, de wet en dit besluit zijn opgenomen. Het is niet de bedoeling dat het een letterlijke herhaling van de in voornoemde regelgeving genoemde waarborgen en eisen bevat. Het uitgangspunt is dat het protocol in de praktijk als zelfstandig document kan worden gebruikt door zowel de instanties die er mee werken als betrokkenen die ermee te maken krijgen. Bij de

CONCEPT

formulering van de eisen aan het protocol is onder andere gebruik gemaakt van de door de AP geformuleerde uitgangspunten.

### 3.3.1 Gerechtvaardigde overtuiging van fraude in de zorg

In de memorie van toelichting bij de wet is opgenomen dat sprake is van een gerechtvaardigde overtuiging van fraude in de zorg, indien er 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. De regels die in acht moeten worden genomen bij het komen tot een voornoemde overtuiging, zijn hierna toegelicht.

In het protocol moet worden opgenomen dat een betrokken instantie slechts tot een gerechtvaardigde overtuiging kan komen nadat het een fraudeonderzoek heeft uitgevoerd. De uitkomst van dat fraudeonderzoek moet de conclusie rechtvaardigen dat ten aanzien van de betreffende partij sprake is van een vastgestelde gedraging die een zwaardere verdenking dan een redelijk vermoeden van fraude in de zorg oplevert. Om die conclusie te kunnen dragen, moet het fraudeonderzoek ondersteund zijn met voldoende bewijsstukken van betrokkenheid van de betreffende partij bij de fraude. Uitgangspunt is dat de betrokken instantie de conclusie moet kunnen onderbouwen en dat geconcretiseerd kan worden waarom tot registratie is overgegaan. Daarbij moet voldoende inzicht kunnen worden gegeven in de gronden daartoe, waarbij wordt ingegaan op de elementen van fraude in de zorg, zoals opzet, misleidend handelen binnen het zorgdomein en dat met eigen of andermans gewin als oogmerk.

Het protocol moet waarborgen bevatten die ervoor zorgen dat fraudeonderzoek, waaronder bijvoorbeeld een feitenonderzoek, zorgvuldig zal plaatsvinden. Bij de uitvoering van het onderzoek moeten beginselen zoals proportionaliteit en subsidiariteit in acht worden genomen, bijvoorbeeld bij het bepalen van de inzet van middelen voor dat onderzoek. Ook kan gedacht worden aan het beginsel van hoor en wederhoor en zouden betrokken instanties de voor hen geldende wet- en regelgeving of (andere) protocollen met betrekking tot uitvoering van onderzoek in acht moeten nemen.

De gerechtvaardigde overtuiging en het bewijs dat daaraan ten grondslag ligt, moeten er zijn op het moment van verstrekking van de gegevens aan andere instanties. Dat is bijvoorbeeld op het moment van registratie in een centraal registratiesysteem zoals het Waarschuwingsregister. Voor een toelichting ten aanzien van de bewaartermijn van de bewijsstukken en de gegevens die zijn verstrekt in het Waarschuwingsregister, wordt hier verwezen naar paragraaf 3.6.

### 3.3.2 Noodzaak tot verstrekking

Als er sprake is van een gerechtvaardigde overtuiging, dan moet voordat tot verstrekking van gegevens wordt overgegaan ook nog worden bepaald of die verwerking noodzakelijk is voor de bestrijding van fraude in de zorg. In de vraag of een verwerking noodzakelijk is, ligt besloten of de verwerking van gegevens proportioneel is en of de verwerking voldoet aan de eis van subsidiariteit. Of de verwerking proportioneel is, betreft de vraag naar effectiviteit en evenredigheid. 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. In het

CONCEPT

protocol moeten waarborgen zijn opgenomen omtrent deze afweging. Daarbij gaat het om de omstandigheden van het geval, zoals 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. Per geval zal deze afweging moeten worden gemaakt en moeten kunnen worden onderbouwd.

In het verlengde hiervan moeten ook regels worden gesteld ten aanzien van de mogelijkheid tot het raadplegen van de in het Waarschuwingsregister opgenomen gegevens. Ook die verwerking van gegevens moet immers noodzakelijk zijn voor de bestrijding van fraude in de zorg. Dit onderdeel komt aan de orde in de volgende paragraaf.

### 3.3.3 Overige eisen aan het protocol

Teneinde een zorgvuldige en rechtmatige verwerking van gegevens te waarborgen, zijn ook andere eisen aan het protocol gesteld. Het gaat dan bijvoorbeeld om eisen ten aanzien van 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. Deze onderdelen zijn nader toegelicht in paragraaf 3.5 tot en met 3.8. Andere onderdelen die in het protocol moeten terugkomen en die hierna worden toegelicht, moeten in samenhang worden bezien met de hiervoor genoemde en elders toegelichte onderdelen.

In het protocol moeten procedurevoorschriften zijn opgenomen ten aanzien van het aan elkaar verstrekken van gegevens, bijvoorbeeld door het in het Waarschuwingsregister registreren en raadplegen van gegevens, en het verwijderen van die gegevens. Ook ten aanzien van de inrichting en het beheer van het te gebruiken systeem, zoals het Waarschuwingsregister, moeten voorschriften in het protocol zijn opgenomen. Hoewel de AP ingevolge de UAVG formeel toezichthouder is op de verwerking van persoonsgegevens, zijn de betrokken instanties verantwoordelijk voor intern toezicht op juiste en zorgvuldige omgang met (persoons)gegevens. Derhalve is voorgeschreven dat elke instantie daartoe een proces heeft ingericht, waarvan de uitgangspunten in het protocol moeten zijn 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.

Ten aanzien van de mogelijkheid tot het raadplegen van het Waarschuwingsregister, moet in het protocol zijn opgenomen dat dit enkel is toegestaan indien dat noodzakelijk is ten behoeve van het doel dat het Waarschuwingsregister dient. Daarbij dient ook, zij het niet limitatief, inzicht te worden gegeven in welke gevallen de gegevens kunnen worden geraadpleegd.

Het uitgangspunt daarbij is dat een betrokken instantie bij het in het kader van zorg aangaan of voortzetten van een relatie met een partij, kan controleren of het nodig is maatregelen te treffen.
Zoals in paragraaf 3.2 van de memorie van toelichting bij de wet aan de orde is gekomen, dienen instanties altijd zelf (nader) onderzoek te doen naar een geregistreerde partij en

CONCEPT

zorgvuldig te bepalen welke beheersmaatregelen worden getroffen. Gedacht kan worden aan het doen van vervolgonderzoek naar fraude en op basis van dat onderzoek besluiten tot het doen van extra controles, het stellen van scherpere voorwaarden of eventueel het niet aangaan dan wel beëindigen van een overeenkomst betreffende zorgverlening. In het protocol moet inzicht worden gegeven in de mogelijke gevolgen die betrokken instanties aan een waarschuwing kunnen geven en welke rechtsmiddelen daar dan tegen open staan. In paragraaf 3.4 van die memorie van toelichting is in algemene zin aandacht besteed aan de bestuursrechtelijke en civielrechtelijke mogelijkheden tot rechtsbescherming tegen mogelijke gevolgen die een waarschuwing voor een partij heeft. Dit moet in samenhang worden gezien met de uitoefening van de rechten van betrokkenen.

Daarnaast moet ook de in artikel 2.8 van de wet opgenomen geheimhoudingsplicht zijn weerslag vinden in het protocol en de afspraken die partijen daaromtrent hebben gemaakt, moeten daarbij zijn opgenomen.

Teneinde een duidelijke en eenduidige werkwijze te waarborgen, wordt voorgeschreven dat betrokken instanties processen concretiseren en invullen door middel van werkinstructies of handreikingen. Ten behoeve van transparantie en rechtszekerheid, dient het protocol beschikbaar te zijn voor partijen. Zoals hiervoor onder 3.2 aan de orde kwam, wordt het protocol met het besluit tot goedkeuring ervan door de Minister van VWS gepubliceerd. In het protocol moet zijn opgenomen dat er een centraal registratiesysteem, zoals het Waarschuwingsregister, is. Instanties moeten hierover ook proactief communiceren. Dat betekent bijvoorbeeld dat zij partijen hierover informeren als zij overeenkomsten met die partijen aangaan en dat op de website van instanties informatie over het register en het protocol wordt gepubliceerd. Dit kan onderdeel uitmaken van een privacy statement.

Het protocol dient ook aan formele vereisten te voldoen. Zo moet het volledig zijn voordat de AP erover wordt gehoord, alvorens het ter goedkeuring aan de Minister van VWS kan worden voorgelegd. Deze volledigheidseis geldt ook voor eventuele bijlagen, zoals formulieren. Het protocol moet een lijst met definities bevatten en het moet een inhoudsopgave, paginanummering en versienummer met datum hebben. Daarnaast moeten ook eventuele bijlagen zijn opgenomen, waarbij gedacht kan worden aan formulieren, machtigingen en verwerkersovereenkomsten.

## 3.4 Gegevensset

### 3.4.1 Inleiding

In de wet is het kader vastgesteld voor verstrekking van gegevens aan betrokken instanties in een centraal registratiesysteem zoals het Waarschuwingsregister. In de memorie van toelichting bij de wet is in hoofdstuk 3 en 5 toegelicht waarom deze verwerking van gegevens noodzakelijk is in het kader van bestrijding van fraude in de zorg. Daarbij is ingegaan op de waarborgen bij die gegevensverwerking. Ook is de gemaakte afweging, tussen het zwaarwegende algemeen belang dat met dit deel van de wet wordt gediend en de mogelijke inmenging in de persoonlijke levenssfeer van betrokkene(n) als gevolg daarvan, toegelicht.

CONCEPT

Ingevolge de wet verstrekken betrokken instanties de bij algemene maatregel van bestuur (hierna: 'amvb') aangewezen gegevens. In onderhavig besluit zijn de betreffende gegevens opgenomen. In deze paragraaf wordt toegelicht welke gegevens door de betrokken instanties moeten worden verstrekt. Conform artikel 5, eerste lid, onderdeel c, van de 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.

Hierna wordt bij de toelichting ten aanzien van de aangewezen gegevensset nader aandacht besteed aan de noodzaak dat specifiek deze gegevens onderdeel uitmaken van die set. Deze gegevensset is gelet op het vorenstaande ook proportioneel gelet op het met de verstrekking van deze gegevens te bereiken doel en het zwaarwegende algemeen belang dat daarmee wordt gediend.

Indien aan de voorwaarden tot verstrekking is voldaan, verstrekken instanties alle gegevens die van deze gegevensset onderdeel uitmaken. Instanties verstrekken 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.

### 3.4.2 Gegevens

Bij verstrekking van gegevens in het kader van dit eerste onderdeel van de wet, wordt aangegeven of het gegevens van een rechtspersoon of een natuurlijk persoon betreft. De verstrekkende instantie verstrekt van een rechtspersoon de administratieve kenmerken. 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.

Gemeenten verstrekken ten behoeve van andere gemeenten ook het burgerservicenummer (BSN). De in het kader van artikel 87 van de AVG en artikel 46 van de UAVG benodigde grondslag voor de verwerking van dit wettelijk identificatienummer

CONCEPT

door gemeenten in het kader van dit onderdeel van de wet, is opgenomen in artikel 10 van de Wet algemene bepalingen burgerservicenummer (Wabb). Voor ziektekostenverzekeraars geldt deze bepaling niet. Er geldt voor hen 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 (in kunnen) zien wanneer zij gebruik maken van het Waarschuwingsregister. Bij de inrichting van het centrale registratiesysteem moet daar dan ook rekening mee worden gehouden, bijvoorbeeld wat betreft beveiliging.

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 het Waarschuwingsregister. Zo kunnen de gegevens gebruikt worden in de zoeksystematiek van het Waarschuwingsregister.

Bij een registratie in het Waarschuwingsregister worden ook de naam, een e-mailadres en een telefoonnummer van de betrokken instantie vermeld die de gegevens heeft geregistreerd. Dit is onder andere noodzakelijk voor het geval dat een partij, van wie persoonsgegevens worden verwerkt, zich voor de uitoefening van zijn rechten uit de AVG wendt tot een van de betrokken instanties. Als de instantie tot wie de partij zich wendt niet zelf de persoonsgegevens in het Waarschuwingsregister heeft geregistreerd, kan de geregistreerde partij worden verwezen naar de instantie die dat wel heeft gedaan. De uitoefening van de rechten van betrokkenen en de verdeling van verantwoordelijkheden tussen betrokken instanties is nader toegelicht in paragraaf 3.7 en 3.8.

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.

Bij een registratie in het Waarschuwingsregister wordt ook de datum van de registratie in het Waarschuwingsregister vastgelegd. De datum van registratie is voor overige raadplegende instanties niet zichtbaar. De datum van de registratie wordt enkel opgenomen voor beheersmatige doeleinden in verband met de termijnen die zijn toegelicht in paragraaf 3.6.

CONCEPT

## 3.5 Beveiliging

Artikel 32 van de 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. Gelet op de gevoeligheid van de gegevens die in een centraal registratiesysteem zoals het Waarschuwingsregister worden verwerkt en de mogelijke gevolgen voor betrokkenen van deze verwerking, zijn naast de hiervoor beschreven hoge eisen aan registratie, ook hoge eisen gesteld aan de beveiliging van het systeem. Dit onder andere ter voorkoming van ongeoorloofde toegang tot of gebruik van de gegevens die worden verwerkt. De instanties dragen gezamenlijk zorg voor een adequate beveiliging en, in het verlengde daarvan, de inrichting en het beheer, van de verwerking van de gegevens in het Waarschuwingsregister. Deze elementen moeten ook terugkomen in het op te stellen protocol. Het vorenstaande geldt onverminderd voor daartoe behorende gegevens niet zijnde persoonsgegevens.

In artikel 2.4, derde lid, van dit besluit is bepaald dat voor de beveiliging van de gegevens nadere 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. 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 geheimhoudingsplicht uit artikel 2.8 van de wet, het loggen van uitgevoerde acties en het classificeren, opslaan en verwijderen van te verwerken gegevens. Er moet worden gedacht aan het scheiden van de verschillende bevoegdheden die er zijn binnen het centraal registratiesysteem en deze moeten bij verschillende afdelingen of personen binnen de betrokken instanties worden belegd. Zo kan voor de verstrekkende 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 Waarschuwingsregister 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 Waarschuwingsregister kan raadplegen. Dit kunnen namelijk alleen medewerkers zijn voor wie het raadplegen van het Waarschuwingsregister noodzakelijk is

voor de uitvoering van hun taak, bijvoorbeeld bij de inkoop van zorg. Zoals in paragraaf 3.4 aan de orde is gekomen, verdient de beveiliging van het BSN daarbij bijzondere aandacht omdat van de betrokken instanties alleen gemeenten dit gegeven in het kader van dit onderdeel van de wet mogen verwerken.

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

CONCEPT

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

### 3.6.1 Termijnen van registreren en bewaren

In artikel 2.2, tweede lid, van de wet is bepaald dat bij amvb regels worden gesteld met betrekking tot de termijn van verstrekken gegevens en de bewaartermijnen van de verstrekte gegevens. In dit besluit is daar invulling aan gegeven. Als uitgangspunt daarbij is genomen artikel 5, eerste lid, onder e, van de AVG, waarin is bepaald dat persoonsgegevens niet langer worden bewaard dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.

Het uitgangspunt is dat gegevens vanaf het moment van verstrekking, gedurende een termijn van vier jaar in het Waarschuwingsregister zijn geregistreerd en raadpleegbaar zijn. In uitzonderlijke gevallen, omdat zwaarwegende omstandigheden dat noodzakelijk maken, kan een termijn van 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 in paragraaf 2.1 en 3.1 beschreven afweging tussen het met de verwerking van gegevens te bereiken doelen, de inbreuk die met die verwerking wordt maakt op de privacy van betrokkene(n) en de mogelijke gevolgen daarvan voor die betrokkene(n) (zowel persoonlijk als zakelijk), 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 in de praktijk. Teneinde met de registratie (de waarschuwing) het met de wet beoogde doel te bereiken, is 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 acht jaar mogelijk. Die termijn kan noodzakelijk en proportioneel zijn gelet op de concrete omstandigheden van het geval.

Of de termijn van acht jaar in een bepaald geval kan worden toegepast, moet door de verstrekkende instantie worden bepaald op basis van door instanties geformuleerd en in het protocol opgenomen criterium. Het criterium moet objectief en helder zijn en in de onderbouwing ervan moet zijn ingegaan op de aspecten van noodzakelijkheid en proportionaliteit. Ook andere aspecten kunnen van invloed zijn op de beoordeling of er noodzaak bestaat tot het toepassen van uitzondering. Bij het formuleren van het criterium kan gedacht worden aan aspecten 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 blijven ontkennen en 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 er 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 direct bekennen van (betrokkenheid bij) fraude in de zorg en 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 kan gedacht worden aan een toets die, na het verstrijken van de eerste vier jaar, periodiek wordt gedaan en waarbij steeds wordt beoordeeld of het toepassen van de termijn van acht jaar nog steeds noodzakelijk is.

Gedurende de verstrekking van de gegevens, dat is de periode waarin de gegevens in een systeem zoals het Waarschuwingsregister zijn opgenomen en raadpleegbaar zijn, worden deze gegevens bewaard door de verstrekkende instantie. De bewijsstukken waarover een verstrekkende 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 gegeven 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 en de gegevens moeten dan verwijderd worden uit het centrale registratiesysteem. De verstrekkende 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 uit het registratiesysteem (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 moet door betrokkeninstanties inzichtelijk worden gemaakt in het protocol.

### 3.6.2 Verwijdering

De betrokken instantie die gegevens in een centraal registratiesysteem aan andere instanties verstrekt, is verantwoordelijk voor die verwerking van gegevens (zie paragraaf 3.8). Die instantie is dan ook verantwoordelijk voor de beëindiging van de verstrekking van die gegevens door middel van verwijdering van de gegevens uit het registratiesysteem. In het protocol dienen procedurevoorschriften ten aanzien van de verwijdering van gegevens zijn 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, moeten die gegevens op dat moment verwijderd worden. Dit kan zich bijvoorbeeld voordoen indien er nieuwe informatie beschikbaar is gekomen. Gedacht kan worden aan een periodieke toets op verstrekte gegevens door de verstrekkende 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 van de AVG, maar zoals toegelicht in paragraaf 3.7 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

CONCEPT

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 blijft uitsluitend voor de betrokken instantie die de gegevens heeft verstrekt zichtbaar dat de verstrekking uit het Waarschuwingsregister is verwijderd. Dit is noodzakelijk om in juridische procedures te kunnen aantonen dat de verstrekking daadwerkelijk is verwijderd.

## 3.7 Uitoefening van de rechten van betrokkenen

Nationaalrechtelijk zijn de rechtsbeschermingsbepalingen uit de AVG nader uitgewerkt en ingevuld in paragraaf 3.3 van de UAVG. Waar nodig zijn deze regels in onderhavig besluit nader uitgewerkt of ingevuld. In artikel 2.5 van dit besluit is bepaald dat de rechten van betrokkenen, zoals geregeld in hoofdstuk 3 van de AVG, van overeenkomstige toepassing zijn op rechtspersonen en de op hen betrekking hebbende gegevens. Dat is nodig gelet op de mogelijke gevolgen van de verwerking van die gegevens, niet zijnde persoonsgegevens. Hoe betrokken instanties de mogelijkheid tot het uitoefenen van de rechten van betrokkenen (verder) regelen en invullen, moet zijn opgenomen in het protocol. Daarbij is het volgende van belang.

De verstrekkende instanties zijn ieder voor zich verantwoordelijk voor de door hen verrichte verwerking van gegevens, bestaande uit het verstrekken van deze gegevens in het kader van het eerste onderdeel van de wet. Ten aanzien van het beheer en de beveiliging van het Waarschuwingsregister en het respecteren en faciliteren van de uitvoering van de rechten van betrokkene(n), zijn zij gezamenlijk verantwoordelijk. Voor zover het de verwerking van persoonsgegevens betreft, zijn instanties gezamenlijke verwerkingsverantwoordelijken als bedoeld in artikel 26 van de AVG. Het is noodzakelijk te regelen waar een betrokken partij, van wie gegevens worden verwerkt, terecht kan voor het uitoefenen van zijn rechten.
Dit komt bijvoorbeeld ook aan de orde bij de beschrijving van een klachtenprocedure. Wat betreft persoonsgegevens gaat het om een klachtenprocedure als bedoeld in artikel 77 van de AVG.

Uitgangspunt daarbij is dat de verstrekkende instantie in beginsel het aanspreekpunt is voor de betrokken partij wiens gegevens geregistreerd zijn in het Waarschuwingsregister. Dit betekent dat de verstrekkende instantie de uitvoering van de rechten van de betrokken partij faciliteert. Wendt de betrokken partij zich tot een van de andere instanties, dan wordt deze partij door deze andere instantie verwezen naar de verstrekkende instantie. Uit de AVG volgt dat de betrokkene zich tot de FG 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.

> *Wanneer bijvoorbeeld gemeente A een registratie in het Waarschuwingsregister opneemt en de partij wiens persoonsgegevens geregistreerd zijn, zich tot gemeente B wendt met een verzoek tot uitoefening van zijn rechten uit de AVG, verwijst gemeente B deze partij naar gemeente A.*

CONCEPT

Als sprake is van de verwerking van gegevens, informeert de verwerkingsverantwoordelijke betrokken instantie de betrokkene wiens gegevens het betreft conform artikel 14 van de 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, van de 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, is het aan betrokken instanties om in het protocol nader te regelen wanneer en inzichtelijk te maken, 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.

### 3.8 Verantwoordelijkheid en samenwerking

De instantie die gegevens in een centraal registratiesysteem aan andere instanties verstrekt, zoals een registratie in het Waarschuwingsregister, is verantwoordelijk voor die verwerking van gegevens. Een raadplegende instantie is verantwoordelijk voor die verwerking (de 'raadpleging'). Indien de verwerking persoonsgegevens betreft, zijn de instanties verwerkingsverantwoordelijke zoals bedoeld in de AVG. Gemeenten en ziektekostenverzekeraars zijn echter gezamenlijk verantwoordelijk, en voor zover het persoonsgegevens raakt gezamenlijke verwerkingsverantwoordelijke (artikel 26 van de AVG), voor de werking, inrichting, beveiliging en het beheer van het Waarschuwingsregister. Het protocol moet de rollen van de verantwoordelijken, verwerkers en betrokken instanties inzichtelijk maken. In dat kader moeten 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 van de 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 moet bijvoorbeeld ten aanzien van rechtspersonen van wie gegevens worden verwerkt een soortgelijke waarborg zijn 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 2.3 van de wet is voorzien in een grondslag voor het door de in dat artikel genoemde betrokken instanties verstrekken van gegevens, waaronder persoonsgegevens, aan het IKZ. Het IKZ ondersteunt die instanties bij de bestrijding van fraude in de zorg. Het gaat om de instanties CIZ, gemeenten, IGJ, Inspectie SZW, NZa, rijksbelastingdienst, FIOD,

SVB en ziektekostenverzekeraars.[1] Indien het verstrekken van in onderhavig besluit aangewezen gegevens voor een of meer van die instanties noodzakelijk is voor de bestrijding van fraude in de zorg in het kader van de aan die instanties opgedragen wettelijke taken, dan is het uitgangspunt dat instanties verplicht zijn tot het verstrekken van die gegevens aan het IKZ. Het IKZ vult de gegevens aan met gegevens uit de daartoe in de wet aangewezen bronnen en andere noodzakelijke gegevens van betrokken instanties. Het resultaat daarvan verstrekt het IKZ 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). Zij hebben zo een betere informatiepositie en worden in staat gesteld efficiënter en, mede met het oog op privacy, zorgvuldig te beoordelen of sprake is van fraude in de zorg. De persoonlijke, financiële en maatschappelijke gevolgen die het zwaarwegende algemeen belang vormen bij bestrijding van fraude in de zorg, rechtvaardigen de met dit onderdeel van de wet mogelijk gemaakte inmenging in de privacy van betrokkenen. Voor een toelichting hierop wordt verwezen naar hoofdstuk 4 en 5 van de memorie van toelichting bij de wet. Dit laat onverlet dat de afweging of de inmenging in de privacy van betrokkenen is toegestaan, in elk specifiek geval moet worden gemaakt. In dit besluit zijn ten aanzien van dit onderdeel van de wet de nadere regels opgenomen en in dit hoofdstuk worden die regels toegelicht.

*Algemeen*
Het verstrekken van gegevens door betrokken instanties en het IKZ, maakt onderdeel uit van hetgeen in de praktijk het uitwisselen van signalen van fraude in de zorg ('signalen') wordt genoemd. Het gaat om signalen, waar ook (persoons)gegevens onderdeel van uitmaken, die aanleiding geven tot een vermoeden van fraude in de zorg. Net als in de memorie van toelichting van de wet, wordt in deze nota van toelichting waar kan bij de terminologie uit de praktijk aangesloten. Daarom wordt bijvoorbeeld het verstrekken van gegevens door betrokken instanties aan het IKZ en andersom aangeduid als 'het uitwisselen van signalen', gaat het om 'het verrijken van signalen door het IKZ' en wordt het resultaat van de verwerking van gegevens door het IKZ 'het verrijkte signaal' genoemd.

De verstrekking van gegevens door betrokken instanties aan het IKZ vindt plaats in twee te onderscheiden onderdelen in het proces. In het eerste onderdeel verstrekt een betrokken instantie gegevens aan het IKZ als die instantie in een bepaald geval een aanleiding tot vermoeden van fraude in de zorg heeft. Dit wordt in deze toelichting aangeduid als het 'verstrekken van een signaal aan het IKZ'. In paragraaf 4.2 worden de regels omtrent de aanleiding tot en de voorwaarden waaronder signalen aan het IKZ worden verstrekt nader toegelicht. Daarbij wordt ook ingegaan op de wijze waarop die verstrekking geschiedt.

De ontvangst van een signaal vormt voor het IKZ het startpunt voor de uitvoering van de taak tot het bijeen brengen van gegevens ten aanzien van dat signaal ('verrijken'). Dat is het tweede onderdeel van het proces. Het IKZ vult het signaal aan met gegevens uit de

[1] 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 Inspectie SZW, de rijksbelastingdienst, waaronder de Fiscale inlichtingen- en opsporingsdienst (FIOD).

daartoe in de wet aangewezen bronnen. Daarnaast vult het IKZ het signaal aan met gegevens die het IKZ noodzakelijk heeft geacht en na uitvraag door de betrokken instanties aan het IKZ zijn verstrekt. Dit wordt in deze toelichting aangeduid als het 'verstrekken van gegevens aan het IKZ in het kader van verrijking'. De regels omtrent deze fase van het proces zijn nader toegelicht in paragraaf 4.3, waarbij ook wordt ingegaan op de inrichting en vormgeving van de werkprocessen van het IKZ.

Het IKZ verstrekt het resultaat van de verrijking (het 'verrijkte signaal') vervolgens indien en voor zover noodzakelijk aan een of meer geëigende instanties. Dit wordt nader toegelicht in paragraaf 4.5.

In dit besluit is opgenomen welke gegevens op grond van de wet worden verstrekt (zie paragraaf 4.4). Van belang daarbij is dat in het kader van dit onderdeel van de wet mogelijk persoonsgegevens als bedoeld in de Wpg worden verwerkt. Het gaat dan om politiegegevens, die verwerkt worden door de FIOD en de Inspectie SZW. 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 van de AVG. Overigens kan tijdens het bijeenbrengen van gegevens door het IKZ 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.

Het IKZ heeft ook de 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 van VWS of betrokken instanties te verstrekken. De regels die daarover in dit besluit zijn opgenomen, zijn toegelicht in paragraaf 4.6.

De in dit besluit opgenomen regels 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, worden toegelicht in paragraaf 4.7. De in dit besluit opgenomen nadere regels moeten in samenhang met elkaar worden bezien 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 gegevens anders dan persoonsgegevens door het IKZ is hoofdstuk 3 van de AVG, over de rechten van betrokkenen, niet van overeenkomstige toepassing verklaard. Voor het IKZ geldt echter dat het onverminderd verantwoordelijk is voor een zorgvuldige en rechtmatige verwerking van die gegevens en de inrichting van een proces daartoe. Ten aanzien van de verwerking van zowel persoonsgegevens als niet-persoonsgegevens geldt als uitgangspunt dat een gelijkwaardig (hoog) niveau aan waarborgen wordt geboden.

CONCEPT

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

### 4.2.1 Aanleiding tot, gevallen waarin en de voorwaarden waaronder gegevens aan het IKZ worden verstrekt

#### *4.2.1.1 Algemeen*

Gelet op de mogelijke (indirecte) gevolgen van een verstrekking van gegevens voor een betrokkene, behoeft het geen nadere uitleg dat het risico op een onjuiste of onzorgvuldige verstrekking van signalen door instanties aan het IKZ zoveel mogelijk moet worden beperkt. Daarnaast zijn de betrokken instanties en het IKZ ook gebaat bij 'goede' signalen, zodat onnodige administratieve belasting wordt voorkomen en de met de wet mogelijk gemaakte gegevensuitwisseling ook daadwerkelijk bijdraagt aan een efficiënte doch zorgvuldige samenwerking ten behoeve van bestrijding van fraude in de zorg.

De nadere regels in dit besluit zijn er daarom op gericht dat wordt gedefinieerd en ingekaderd wanneer sprake is van een aanleiding tot en gevallen of situaties waarin signalen door betrokken instanties aan het IKZ moeten worden verstrekt. 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, hetgeen eveneens bijdraagt aan transparantie voor partijen die hiermee te maken krijgen. Daarnaast zijn ook de voorwaarden bepaald waaronder de verstrekking moet plaatsvinden. In samenhang met de in dit besluit aangewezen gegevensset, waarmee ook nadere regels zijn gegeven ten aanzien van de aard van de te verstrekken gegevens, vormen de hier toegelichte regels een belangrijk onderdeel van de waarborgen in het kader van een zorgvuldige en rechtmatige verwerking van gegevens, de rechtszekerheid voor en rechtsgelijkheid van betrokken partijen en de uitvoerbaarheid voor betrokken instanties.

#### *4.2.1.2 Aanleiding tot, gevallen waarin en voorwaarden waaronder*

*Aanleiding tot een vermoeden van fraude in de zorg*

Als uitgangspunt wordt genomen dat er veel (verschijnings)vormen van signalen van fraude zijn die aanleiding kunnen geven tot een vermoeden van fraude in de zorg. 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 (het signaal), is dan nog onduidelijk. Laat staan dat vastgesteld kan worden dat sprake is van fraude in de zorg. Een betrokken instantie moet dan ook eerst een afweging maken of daadwerkelijk sprake is van een aanleiding tot een vermoeden van fraude in de zorg. In dat kader is vereist dat instanties, voor zover dat in deze fase van het proces mogelijk is gelet op de al dan niet aanwezige gegevens, zelf een zorgvuldig eerste onderzoek doen naar dat signaal. De daarbij geldende voorwaarden en daarmee samenhangende waarborgen worden hierna onder het kopje 'Voorwaarden' verder toegelicht.

*Gevallen waarin gegevens aan het IKZ worden verstrekt*
Indien een betrokken instantie tot het oordeel komt dat sprake is van een aanleiding tot een vermoeden van fraude in de zorg, dan moet het vervolgens afwegen of het noodzakelijk is dat gegevens aan het IKZ worden verstrekt. Indien die vraag bevestigend wordt beantwoord, moet die instantie tot slot afwegen welk gegeven of welke gegevens uit het signaal van fraude in de zorg, passend binnen de in dit besluit aangewezen gegevensset, noodzakelijk is of zijn om aan het IKZ te verstrekken. Daarbij moet ook worden afgewogen of deze verstrekking proportioneel is en voldoet aan de eis van subsidiariteit.[2] De hierna volgende elementen zijn daarbij van belang en de geldende voorwaarden en daarmee samenhangende waarborgen zijn onder het kopje 'Voorwaarden' verder toegelicht.

Een betrokken instantie moet zelf beoordelen of het voor een of meerdere van de betrokken instanties voor de bestrijding van fraude in de zorg in het kader van de aan die instanties opgedragen wettelijke taken noodzakelijk is gegevens aan het IKZ te verstrekken. Van een noodzaak tot verstrekking is kort gezegd sprake indien de bestrijding van (de betreffende) fraude in de zorg zonder de verstrekking niet dan wel onvoldoende kan plaatsvinden. Om dat te kunnen beoordelen moeten instanties dan ook inzicht hebben in voor wie van de betrokken instanties, wanneer, welke gegevens noodzakelijk (kunnen) zijn. Dat is ook nodig omdat voor een verstrekking moet worden afgewogen of een signaal kan worden verstrekt zonder of met minder gegevens. Wanneer het signaal gegevens bevat die niet nodig zijn voor de verdere behandeling ervan, dan mogen deze gegevens niet worden verstrekt. Welke gegevens op grond van de wet worden verstrekt, is ingekaderd door de in dit besluit aangewezen gegevensset. Met het oog op uitvoerbaarheid en effectiviteit moet voorafgaand aan een eventuele verstrekking worden afgewogen of het om al dan niet geloofwaardige en duidelijke signalen gaat. De betrokken instanties en het IKZ moeten zorgvuldig omgaan met de gegevens die worden verstrekt en als het op voorhand overduidelijk is dat het uitwisselen van de gegevens geen kans van slagen heeft of dat het signaal niet plausibel is, moet worden afgezien van het verstrekken van die gegevens.

<u>Voorbeelden</u>
Grofweg kunnen de volgende gevallen zich voordoen.

Als een instantie niet zelf over voldoende gegevens beschikt en niet zelf actie kan ondernemen in het kader van diens wettelijke taak in de zorg, dan ligt gegevensverstrekking aan het IKZ voor de hand. Voor (een goede) bestrijding van fraude in de zorg is het voor een of meer betrokken instanties, dat kan ook de verstrekkende instantie zelf zijn, noodzakelijk dat de gegevens aan het IKZ worden verstrekt en dat verrijking van het signaal plaatsvindt. Dit is de situatie waarop de wet hoofdzakelijk is gericht.

[2] Het kader hiervoor is in algemene zin opgenomen in de wet, in samenhang met de AVG, en is toegelicht in paragraaf 2.1 van deze toelichting. Voor de FIOD en Inspectie SZW geldt het afwijkende regime van de Wpg en dat is in paragraaf 2.3 van deze toelichting aan de orde gekomen.

CONCEPT

*Hierbij gaat het om de situatie van een zorgaanbieder waarvan bekend is dat deze actief is in een groter gebied (in meerdere gemeenten) en in meerdere domeinen. Er zijn signalen dat er sprake is van fraude, maar er is samenwerking en samenvoeging van informatie noodzakelijk teneinde hierover duidelijkheid te krijgen en indien noodzakelijk actie tegen te ondernemen. De verschillende puzzelstukjes moeten dan (mede) door uitwisseling van persoonsgegevens met het IKZ bij elkaar worden gebracht.*

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 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 actief is in één specifiek domein, en waarover voldoende informatie beschikbaar is voor die gemeente om een vervolg te geven aan een signaal (fraudeonderzoek, handhaving, etc.).*

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 (een deel van) de gegevens voor andere betrokken instanties noodzakelijk is voor de bestrijding van fraude in de zorg in het kader van de aan die instanties opgedragen wettelijke taken, moet verstrekking van de gegevens 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 de verstrekkende instantie zelf, maar ook voor de andere instanties noodzakelijk zijn dat het signaal aan het IKZ wordt verstrekt.*

*Voorwaarden*

Door elke betrokken instantie moet een proces zijn ingericht om de hiervoor beschreven afweging tot het al dan niet verstrekken van gegevens 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. Er moet daarbij 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 bij het eerste onderzoek naar en beoordeling van een geval waarin (mogelijk) een aanleiding van fraude in het zorgdomein bestaat. Welke dat zijn, kan bijvoorbeeld worden bepaald op basis van opgedane ervaringen met bekende soorten van fraude in de zorg. Benchmarks, oftewel referentiegegevens, kunnen een belangrijke bijdrage leveren aan het

CONCEPT

maken van een zorgvuldige beoordeling en afweging. Bij de afweging moet worden meegenomen dat juist in deze fase van het proces nog (veel) gegevens ontbreken en aspecten onduidelijk zijn en blijven. Tot slot moet in de inrichting en invulling van het proces de mogelijkheid openblijven dat kan worden bijgestuurd op (nieuwe) ontwikkelingen in de praktijk.

De invulling van de (uitvoerings)processen is aan de betrokken instanties zelf, waarbij onderlinge afstemming gelet op de samenwerking in dit proces specifiek en in de keten in het algemeen nodig is. Betrokken instanties moeten dan ook afspraken met elkaar en met het IKZ maken, die worden vastgelegd in een werkinstructie. 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.
Tot slot moet het proces van instanties zo zijn ingericht, dat het signaal niet aan het IKZ wordt verstrekt als de te verstrekken gegevens onvolledig of onjuist zijn. Wat betreft de juistheid van gegevens gaat het hier om de identificerende gegevens van de partij over wie het signaal gaat.

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. Het ligt in de rede dat over de inrichting van het proces afstemming met andere instanties en het IKZ plaatsvindt.

Voor de verstrekking van politiegegevens door FIOD en Inspectie SZW aan het IKZ geldt de voorwaarde dat dit op grond van en in overeenstemming met de Wpg.

Het hiervoor toegelichte kader moet in samenhang worden bezien met de hierna toegelichte regels ten aanzien van andere voorwaarden, vereisten, maatregelen en waarborgen voor verwerking van gegevens.

### 4.2.2 Wijze van verstrekken aan het IKZ

#### *4.2.2.1 Algemeen*

In artikel 2.7, eerste lid, aanhef en onderdeel a, van de wet is opgenomen dat bij of krachtens amvb regels worden gesteld met betrekking tot de wijze waarop de voor bestrijding van fraude in de zorg noodzakelijke gegevens door de betrokken instanties worden verstrekt aan het IKZ. In artikel 3.25 van dit besluit is hier invulling aan gegeven en daarop wordt hier een toelichting gegeven.

Instanties verstrekken signalen op elektronische wijze aan het IKZ. Achtergrond daarvan is dat de verstrekking efficiënt en met voldoende waarborgen en beveiliging kan plaatsvinden. Ook biedt het de mogelijkheid de verstrekking, voornamelijk in het kader van verrijking, zoveel mogelijk geautomatiseerd te laten plaatsvinden. De systemen van instanties moeten daartoe dan ook zijn aangesloten op de elektronische voorzieningen van het IKZ. Bij die elektronische voorzieningen kan gedacht worden aan een systeem

CONCEPT

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 in dit besluit opgenomen regels met betrekking tot de inrichting, het beheer en de beveiliging van de elektronische voorzieningen voor de verwerking van gegevens en beveiliging van gegevens worden in paragraaf 4.7.1 toegelicht.

Wat betreft de wijze van verstrekken van signalen door gemeenten (met tussenkomst van het Inlichtingenbureau) en de rijksbelastingdienst (fiscale gegevens) zijn er bijzonderheden dan wel afwijkende regels. Die worden hierna toegelicht.

##### *4.2.2.2 Verstrekking door gemeenten aan het IKZ: rol Inlichtingenbureau*

De verstrekking van signalen door gemeenten aan het IKZ, als bedoeld in artikel 2.3 van de wet, geschiedt door tussenkomst van het Inlichtingenbureau (IB). Het IB is uitsluitend een koppeling tussen de gemeenten en het IKZ en dus niet tussen het IKZ en de andere in dit wetsvoorstel genoemde instanties. In paragraaf 4.8 van de memorie van toelichting van de wet is ingegaan op de positie en rol van het IB in dit kader, waarbij ook aandacht is besteed aan hoe de diverse verwerkingen door het IB er uitzien en aan de verwerkingsverantwoordelijkheid van het IB.

##### *4.2.2.3 Wijze van verstrekking van fiscale de gegevens door de rijksbelastingdienst*

De rijksbelastingdienst heeft geen specifieke taak in het zorgdomein. De rijksbelastingdienst houdt toezicht op de naleving van fiscale wet- en regelgeving door, voor zover hier van belang, partijen in het zorgdomein. Ook die partijen moeten voldoen aan fiscale verplichtingen. 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 van de 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 met het elektronische systeem van het IKZ 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 Verwerking van gegevens door het IKZ en verrijking van signalen

### 4.3.1 Algemeen

Nadat de in paragraaf 4.2.1 van deze toelichting beschreven afweging door een betrokken instantie heeft plaatsgevonden en een signaal aan het IKZ is verstrekt, start het IKZ met diens taak tot het verrijken van signalen. Het IKZ raadpleegt de daartoe in de wet aangewezen bronnen en beoordeelt welke gegevens noodzakelijk zijn voor de verrijking en vraagt die gegevens uit bij de betrokken instanties. Het uitgangspunt is dat de bevraagde instanties de betreffende gegevens aan het IKZ verstrekken voor zover zij daarover beschikken. De BOD's verstrekken de gevraagde politiegegevens indien dat mogelijk is op grond van en met inachtneming van de Wpg. In de daaropvolgende fase

CONCEPT

verstrekt het IKZ, indien en voor zover dat noodzakelijk is, het resultaat van de verrijking (het 'verrijkte signaal') aan de daartoe geëigende instantie(s).

Voor al deze verwerkingen geldt onverminderd het belang van zorgvuldigheid. Ook deze fases in het proces moeten daarom plaatsvinden tegen de achtergrond van de bij elke verwerking van gegevens terugkerende afweging of (verdere) verwerking van de betreffende gegevens noodzakelijk en proportioneel is en voldoet aan de eis van subsidiariteit. Niet alleen gelet op het belang van betrokken partijen van wie gegevens worden verwerkt, maar ook gelet op de uitvoerbaarheid voor het IKZ en betrokken instanties.

Teneinde te waarborgen dat voornoemde verwerkingen zorgvuldig en tegen voornoemde achtergrond plaatsvindt, is in dit besluit bepaald dat het IKZ daartoe een proces moet hebben ingericht. Hoewel de invulling en inrichting van het proces aan het IKZ is, in afstemming met betrokken instanties, is in dit besluit bepaald welke onderdelen in elk geval in het proces terug moeten komen.

Hierna wordt een aantal specifieke nadere regels ten aanzien van de inrichting van het proces van verrijken, nader toegelicht. De specifieke nadere regels ten aanzien van het verstrekken van gegevens door het IKZ aan geëigende instantie(s) komen in paragraaf 4.5 aan de orde.

### 4.3.2 Verrijking

In de eerste plaats dient te worden aangesloten bij, dan wel voortgebouwd op, het proces dat en de afspraken die instanties hanteren bij de afweging of sprake is van een signaal dat aan het IKZ moet worden verstrekt. In de verrijkingsfase is het aan het IKZ gegevens bij betrokken instanties uit te vragen. In dat kader moet het IKZ beoordelen welke gegevens al dan niet noodzakelijk en proportioneel zijn. Ook hier is het essentieel dat te doen op basis van heldere, objectieve en uniforme criteria en te handelen op basis van indicatoren, (bewijs)stukken en aanwijzingen. Ervaring en kennis uit de praktijk zijn daarvoor leidend. Benchmarks kunnen ook in deze fase van het proces een belangrijke bijdrage leveren aan het maken van een zorgvuldige beoordeling en afweging. In acht moet worden genomen dat kan worden bijgestuurd op (nieuwe) ontwikkelingen in de praktijk. Het ligt op de weg van het IKZ in het kader van het proces van verrijken ook een werkinstructie te hebben. Met het in achtneming van het vorenstaande wordt dan ook voldaan aan de vereiste passende waarborgen voor het verwerken van persoonsgegevens van strafrechtelijke aard, voor zover er sprake is van verwerking van die gegevens.
Met welke gegevens een signaal door het IKZ wordt verrijkt en welke gegevens betrokken instanties in dat kader desgevraagd aan het IKZ verstrekken, is ingekaderd door de in dit besluit aangewezen gegevensset. Met inachtneming van de geformuleerde criteria en indicatoren moet, mede op basis van aard en herkomst van gegevens, zorgvuldig worden afgewogen met welke gegevens uit die set een specifiek signaal moet worden verrijkt met het oog op de bestrijding van de betreffende vorm van fraude. Het goed vastleggen van de aard en herkomst van de te verwerken gegevens is ook noodzakelijk voor een goede taakuitoefening van de geëigende instantie aan wie het verrijkte signaal (mogelijk) verstrekt wordt. Dit is ook van belang voor de verantwoording van verrichtingen in het kader van strafrechtelijke vervolging. Het gebruik en de vastlegging van de aard en

herkomst van de te verwerken gegevens moet ingevolge dit besluit dan ook zijn geborgd in het verrijkingsproces.

Het proces van het IKZ moet onder andere gelet op beperking van de administratieve lasten zo zijn ingericht, dat het geen uitvraag doet van gegevens die in het kader van behandeling van het signaal reeds bij het IKZ bekend zijn. Dat kan bijvoorbeeld het geval zijn als het gaat om gegevens die duidelijk maken welke partij het betreft. Uitgangspunt bij de uitvraag is dat het IKZ gegevens zoveel mogelijk bij de bron ophaalt. Dit ten behoeve van een zorgvuldige gegevensverwerking. Het is een waarborg dat het actuele en juiste gegevens betreft. Voor zover het persoonsgegevens betreft, is het ook een waarborg dat de verwerking ervan door de betreffende betrokken instantie rechtmatig plaatsvindt. Teneinde het verstrekken van juiste informatie door de bevraagde instanties te waarborgen, is het op grond van artikel 2.3, vierde lid, van de wet ook mogelijk dat het IKZ (persoons)gegevens aan de bevraagde instantie verstrekt in het kader van die uitvraag. Het betreft slechts die gegevens die het voor de bevraagde instantie mogelijk maken zo zorgvuldig mogelijk aan de uitvraag te voldoen en gegevens aan het IKZ te verstrekken. De bevraagde instanties mogen de in dit kader van het IKZ verkregen gegevens dan ook voor geen enkel ander doel gebruiken. De gegevensverstrekking door het IKZ aan instanties in het kader van verrijking vindt plaats met de elektronische voorzieningen die ook voor de overige aspecten van verrijking worden gebruikt.

In dit besluit is ook bepaald dat het verrijkingsproces getrapt moet plaatsvinden. Met deze maatregel is eens te meer gewaarborgd dat gegevens niet of niet verder worden verwerkt indien dat niet noodzakelijk is voor de bestrijding van fraude in de zorg. Een aantal treden van verrijking die het IKZ bij de inrichting van het verrijkingsproces moet hanteren, is opgenomen in onderhavig besluit. De mogelijkheid is voor het IKZ opengelaten om in afstemming met de betrokken instanties treden toe te voegen of binnen treden een nadere onderverdeling aan te brengen. Hierna worden eerst de in dit besluit voorgeschreven treden toegelicht. Daaropvolgend wordt toegelicht welke elementen bij de inrichting van het verrijkingsproces moeten terugkomen en waarom.

Teneinde een zorgvuldig verrijkingsproces bij het IKZ te waarborgen, is bepaald dat de eerste treden van verrijking in het teken staat 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 onnodige inbreuk op privacy van een betreffende betrokkene en onnodige uitvoeringslasten voor het IKZ worden voorkomen. Het IKZ en betrokken instanties moeten in dit kader daarom ook hebben vastgelegd welke (basis)set aan gegevens onderdeel uitmaakt van de verstrekking van een signaal. Met juistheid wordt hier gedoeld op de identificerende gegevens van de betrokken partij en niet op de aanleiding tot het vermoeden van fraude in de zorg. 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, zal de verstrekkende instantie door het IKZ in staat worden gesteld het signaal aan te vullen. Bij het uitblijven van een (juiste) aanvulling van gegevens, zal signaal eveneens niet in het voor verrijking gebruikte systeem terecht komen. De inrichting van het systeem, waarover

meer in de volgende paragraaf, moet zo zijn vormgegeven, dat het risico op onjuiste of onvolledige 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 juiste en volledige gegevens. Het tweede element, de reikwijdte van het signaal, betreft het domein waarop het signaal betrekking heeft en met welke domeinen en betrokken instanties het raakvlakken heeft. Dit wordt gezien als de eerste noodzakelijk stap in het bepalen van het vervolg van het verrijkingsproces. 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 verrijkingsproces, 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 al dan niet bijeengebracht worden en gezamenlijk verder worden verwerkt. In een werkproces moet zijn vastgelegd wanneer signalen wel of niet gezamenlijk verder worden behandeld.

In artikel 2.3, tweede lid, van de wet zijn de openbare bronnen aangewezen die het IKZ mag raadplegen in het kader van de verrijking van signalen. Het gaat om het Handelsregister en het Jaardocument Maatschappelijke Verantwoording (JMV). Deze bronnen worden door het IKZ in beginsel geraadpleegd in het kader van de eerste trede van verrijking. De gegevens uit het Handelsregister zijn in de eerste plaats van belang bij het beoordelen van de juistheid van de ontvangen gegevens. Andere openbare gegevens uit het Handelsregister en de gegevens uit het JMV, dragen bij aan een zorgvuldig en rechtmatig vervolg van het verrijkingsproces. Met de beschikking over de betreffende openbare gegevens, kan het IKZ een betere beoordeling en afweging maken van de noodzakelijkheid tot het verwerken van gegevens (uit de gegevensset) gedurende het proces van verrijking.

Ten aanzien van het vervolg van het verrijkingsproces is bepaald dat het IKZ, voordat een signaal met bepaalde gevoelige gegevens mag worden verrijkt, eerst een of meerdere treden moet doorlopen waarbij het signaal met niet zodanige gevoelige gegevens is verrijkt. Pas als daarna noodzaak tot verrijking met de gevoelige gegevens bestaat, kan verrijking met die gegevens plaatsvinden. Onder gevoelige gegevens worden in deze toelichting verstaan politiegegevens, gegevens over de gezondheid, persoonsgegevens van strafrechtelijke aard en fiscale gegevens.
Dit is slechts anders indien en voor zover de aard van het signaal en de reeds bij het IKZ aanwezige gegevens het noodzakelijk maken, dat de eerstvolgende verrijking plaatsvindt met (specifieke) gevoelige gegevens.
De reden voor deze bepaling ten aanzien van het moment van het verwerken van deze gegevens, is daarin gelegen dat extra wordt gewaarborgd dat de (mogelijk) gevoelige gegevens niet worden verwerkt in een te vroeg stadium van verrijking en onderbouwing van het vermoeden van fraude in de zorg en dat ze als gevolg daarvan mogelijk onnodig zouden worden verwerkt.

CONCEPT

Door het IKZ moet, in afstemming met betrokken instanties, zijn vastgelegd op basis waarvan de stap naar een volgende trede in het verrijkingsproces 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 invulling en inrichting van het verrijkingsproces. Andere elementen die hier bijvoorbeeld ook bij kunnen worden betrokken, zijn 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.

### 4.3.3 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 in paragraaf 4.2.2 is beschreven, kan worden gedacht 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. 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, 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 in de geldende normen daar aanleiding toe geven, worden normen in 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. De 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 van de 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. Ook de verstrekking van bepaalde gegevens door het IKZ aan bevraagde instanties in het kader van de uitvraag voor verrijking draagt bij aan dataminimalisatie, omdat de bevraagde

instantie in staat wordt gesteld zorgvuldig en gericht de specifieke gevraagde gegevens kan verstrekken.

Voor het in het kader van verrijking raadplegen van de daartoe in de wet aangewezen bronnen, gebruiken de betreffende 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 FIOD en Inspectie SZW 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.

De toelichting ten aanzien van waarborgen voor het opslaan en bewaren van het signaal en de gegevens waarmee dat signaal is verrijkt, zoals beveiligingseisen, komen hierna aan de orde in paragraaf 4.7.

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

Andere elementen die bij de inrichting en vormgeving van de werkprocessen van het IKZ onder andere aan de orde moeten komen, betreffen het resultaat waartoe de verrijking van een signaal moet leiden en het eind van het verrijkingsproces. Bij het resultaat kan gedacht worden aan termijnen waarbinnen bepaalde acties in het verrijkingsproces moeten worden ondernomen en hoe het op te leveren ‘product’ wordt vormgegeven. Wat betreft het eind van het verrijkingsproces gaat het er met name om dat het proces zo is ingeregeld dat het tijdig wordt beëindigd zodra niet (langer) aan de voorwaarden voor (verdere) verrijking wordt voldaan. De in dit besluit bepaalde regels ten aanzien van bewaartermijnen en het verwijderen van gegevens, worden hierna toegelicht in paragraaf 4.7.

Hierna worden in paragraaf 4.5 de in dit besluit opgenomen regels voor deze fase van het proces toegelicht.

## 4.4 Gegevensset

In de wet is het kader vastgesteld voor de verstrekking van gegevens door de in de wet opgenomen instanties aan het IKZ en de verwerking van die gegevens door het IKZ. In de memorie van toelichting bij de wet is in hoofdstuk 3 en 5 toegelicht waarom deze verwerking van gegevens noodzakelijk is in het kader van bestrijding van fraude in de zorg. Daarbij is ingegaan op de waarborgen bij die gegevensverwerking en is de gemaakte afweging, tussen het zwaarwegende algemeen belang dat met dit deel van de wet wordt gediend en de mogelijke inmenging in de persoonlijke levenssfeer van betrokkene(n) als gevolg daarvan, toegelicht.

CONCEPT

Ingevolge de wet verstrekken betrokken instanties de bij amvb bepaalde gegevens aan het IKZ. In onderhavig besluit is daar invulling aan gegeven en is een set aan gegevens aangewezen. Elk gegeven uit deze gegevensset kan noodzakelijk zijn voor de bestrijding van fraude in de zorg en per geval en per fase van verwerking moet worden beoordeeld welk gegeven of welke gegevens uit deze set daadwerkelijk verstrekt 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 lopende en afgeronde onderzoeken, dat instanties zelf een afweging maken welke gegevens daaruit op het signaal betrekking hebben en noodzakelijk zijn om te verstrekken.
Hoe dan ook geldt dat een instantie alleen die gegevens verstrekt die in de voor die instantie aangewezen gegevensset in dit besluit zijn opgenomen, indien en voor zover het over de betreffende gegevens beschikt. De gegevensset is tot stand gekomen in afstemming met betrokken instanties.

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, van de AVG en het beginsel van privacy by design. Het is niet mogelijk met een beperktere set aan gegevens 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. Zo is geborgd dat de verwerking plaatsvindt ten aanzien van de juiste betrokkene en met de juiste gegevens. Indien een kleinere set aan gegevens zou worden aangewezen, zou dat leiden tot een (groter) risico op het onnodig en 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 deze 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 verwerking op grond van de wet, de afweging maken of deze verwerking van de in dit besluit aangewezen gegevens past binnen het kader van de wet 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 buiten de aangewezen gegevensset vallen, 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 of door het IKZ worden verwerkt en door verstrekt aan de geëigende instantie(s).

Politiegegevens, dat zijn persoonsgegevens die worden verwerkt door de FIOD en Inspectie SZW, 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 wordt aangepast om verstrekking van politiegegevens aan het IKZ mogelijk te maken. In dit besluit is wat deze gegevens betreft volstaan met een generieke duiding van de onder de Wpg vallende gegevens. De FIOD en Inspectie SZW komen op basis van deze generieke aanduiding tot een lijst van politiegegevens die zij verstrekken aan IKZ en leggen dit vast in een werkdocument.

### 4.4.1 Het signaal

In de memorie van toelichting bij de wet is toegelicht dat het bij gegevensuitwisseling tussen het IKZ en betrokken instanties gaat om “signalen, waar ook (persoons)gegevens onderdeel van uitmaken, die aanleiding geven tot een vermoeden van fraude in de zorg.” Een (verrijkt) 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. Daarbij dient ook te worden 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 signaal gemaakte afweging in het (verrijkte) signaal zijn opgenomen. De omschrijving bevat geen gegevens die geen onderdeel uitmaken van de gegevensset. Bij het verstrekken van een signaal aan het IKZ kunnen instanties jaarrekeningen of bepaalde gegevens uit het Handelsregister toevoegen ter toelichting en onderbouwing van het signaal. Hoewel het IKZ zelfstandig het Handelsregister en JMV kan raadplegen, is het denkbaar dat er situaties zijn waarbij instanties bepaalde momentopnamen uit deze bronnen 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 geen uitvraag van gegevens die het in het kader van de behandeling van het signaal al heeft en vraagt 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.

CONCEPT

### 4.4.2 Administratieve kenmerken en identificerende gegevens

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).
Onder identificerende gegevens van een natuurlijk persoon worden in dit besluit verstaan: naam, adres, woonplaats, geboortedatum, geslacht, BIG-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.

Voornoemde administratieve kenmerken van een rechtspersoon respectievelijk identificerende gegevens van een natuurlijk persoon zijn noodzakelijk, omdat het IKZ daarmee in staat wordt gesteld zorgvuldig en met voldoende zekerheid vast te stellen dat het om de juiste (rechts)persoon gaat. Het KvK-nummer stelt het IKZ in staat zelfstandig het Handelsregister te raadplegen

Deze 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.

In bepaalde gevallen is het noodzakelijk om de identificerende gegevens van bestuurders van een rechtspersoon te controleren. Dat is bijvoorbeeld het geval als er een signaal is over een bepaalde partij, waarvan een bestuurder betrokken is bij de vermoedelijke fraude. Het IKZ controleert de identificerende gegevens van die bestuurder en daaruit kan blijken dat de betreffende bestuurder ook al bij een eerder signaal betrokken was. 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. De meest geëigende instantie die het verrijkte signaal verder onderzoekt, kan dan ook gerichter onderzoek doen naar deze verbanden en netwerken. Indien noodzakelijk kan ook een duiding van de relatie tussen verschillende natuurlijke en rechtspersonen die betrokken zijn bij het signaal worden verstrekt.

### 4.4.3 Handelsgegevens

Onder handelsgegevens worden in dit besluit de volgende gegevens verstaan: omvang van het personeelsbestand, informatie over het cliëntenbestand (namelijk het aantal zorgbehoevenden en de plaats waar de zorgbehoevende de zorg ontvangt), informatie over dochterondernemingen en concernrelaties en bestuurder(s).

Handelsgegevens zijn noodzakelijk om een inschatting te maken van de aard en omvang van de vermoedelijke fraude waarop het signaal betrekking heeft. Informatie over het personeelsbestand en cliëntenbestand kan noodzakelijke aanwijzingen bevatten ten aanzien 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.

> *Een voorbeeld van een signaal waarbij verwerking van handelsgegevens noodzakelijk kan zijn, betreft een geval waarin de zorgbehoevende zorg ontvangt*

CONCEPT

*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 of zorgverlener zorg levert, dan wel de zorgbehoevende zorg ontvangt, en gegevens over de soort zorg die wordt geleverd of ontvangen. Het is noodzakelijk te beschikken over gegevens waaruit het zorgdomein en de soort zorg blijken, bijvoorbeeld om het proces van verrijken zorgvuldig te kunnen laten plaatsvinden en de meest geëigende instantie(s) te bepalen. Als duidelijk is om welk domein het gaat, kan gericht met specifiek voor dat domein relevante gegevens worden verrijkt. De meest geëigende instantie die het signaal verder oppakt, heeft de gegevens over het zorgdomein en de soort zorg op haar beurt nodig om te kunnen onderzoeken of de bepalingen die gelden voor dat domein en die soort zorg, overtreden worden.

In het geval van verstrekking van gegevens van een zorgbehoevende, is het mogelijk dat gegevens over de gezondheid als bedoeld in artikel 9 van de AVG worden verstrekt. Het gaat om gegevens waarop geen medisch beroepsgeheim rust. Dit kan zich voordoen indien ten aanzien van een specifieke 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 zorgdomein en de soort zorg, kan bijvoorbeeld dan blijken dat de betreffende 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. In paragraaf 2.2 is toegelicht waarop het 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 Benchmarks

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 de sector 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 kenmerken zoals de aard van de verleende zorg, de regio waarin zij actief zijn en de omvang van hun praktijk, vergelijkbaar zijn met de partij op wie het signaal betrekking heeft. Die referentiegegevens worden in dit besluit als benchmarks aangeduid. Het gaat om conclusies uit analyses die zijn

CONCEPT

uitgevoerd op een of meerdere verzamelingen van gegevens van andere partijen. De benchmarks die instanties aan het IKZ verstrekken, mogen geen gegevens bevatten die te herleiden zijn tot individuele (rechts)personen.

Instanties die over benchmarks beschikken, moeten deze dan ook aan het IKZ verstrekken. Dat kan bijvoorbeeld het geval zijn als zij een signaal verstrekken en zij de benchmark bij de afweging tot verstrekking hebben gebruikt. Ook kan het IKZ in het kader van verrijking benchmarks bij instanties opvragen, als het IKZ die benchmarks 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 er een lopend onderzoek is, kan bilateraal of multilateraal mogelijk afstemming plaatsvinden teneinde te voorkomen dat dat 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. In het geval van afgeronde onderzoeken gaat het om noodzakelijke inhoudelijke informatie met betrekking tot het signaal. Het kan ook informatie over de afdoening en de opgelegde maatregelen bevatten.

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 verstrekkende 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 wegen 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 toezichtrapport bij de IGJ dat waardevolle 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 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*

CONCEPT

*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 er sprake was van fraude, zal de meest geëigende instantie naar aanleiding van het signaal verder moeten onderzoeken of er opnieuw sprake is van fraude. Bleek uit het fraude- of rechtmatigheidsonderzoek juist dat er 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.*

Evenals bij het verstrekken van een signaal aan het IKZ, kunnen instanties als onderdeel van afgeronde onderzoeken, jaarrekeningen of bepaalde gegevens uit het Handelsregister aan het IKZ verstrekken. Hoewel het IKZ zelfstandig het Handelsregister en JMV kan raadplegen, is het denkbaar dat er situaties zijn waarbij instanties bepaalde momentopnamen uit deze bronnen als onderdeel van een afgerond onderzoek aan het IKZ verstrekken.

### 4.4.7 Gegevens rijksbelastingdienst

De rijksbelastingdienst verstrekt noodzakelijke en voor het signaal relevante 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 er 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. Evenals bij het gegeven over lopende en afgeronde onderzoeken, geldt hier dat een afweging nodig is door de verstrekkende instantie, in dit geval 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 in zorg.*

*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 natuurlijk geen bewijs voor fraude in de zorg, maar kan wel een deel van de noodzakelijke gegevens zijn dat nader onderzoek vraagt om vast te stellen of er 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 personen kunnen worden geïdentificeerd door welke partij dan ook, met inzet van (voor het doel) redelijke middelen.

Declaratiegegevens betreffen informatie over de overeengekomen 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, tarieven van de prestaties in relatie tot betaling van de prestaties, de periode waarover is uitgekeerd, de omzet per ziektekostenverzekeraar of verstrekker over het lopende jaar en de drie voorgaande jaren. Ook gegevens over betalingen en bankrekeningnummers maken onderdeel uit van de categorie declaratiegegevens. Omdat er 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 er sprake is van fraude in de zorg, is inzicht nodig in wat er is overeengekomen, wat er is gedeclareerd en wat er is vergoed of uitgekeerd. Uit de declaratiegegevens kan, in combinatie met andere gegevens of nader onderzoek door de geëigende instantie die het signaal opvolgt, onderzocht worden of de gemaakte afspraken zijn nagekomen en of de zorg is geleverd die in rekening werd gebracht. Er kan worden onderzocht of duurdere behandelingen zijn gedeclareerd dan er daadwerkelijk overeengekomen zijn of dat er 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 er 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 bezien. Gegevens over de aard van de zorgzwaartepakketten kunnen bijvoorbeeld worden afgezet tegen declaratiegegevens van de ziektekostenverzekeraars, gemeenten en de SVB. Hieruit kan blijken dat de bedragen die gedeclareerd zijn, (niet) overeenkomen met de zorg waarvoor geïndiceerd is.

### 4.4.10 Gegevens van bijzondere opsporingsdiensten

Gelet op de wet- en regelgeving systematiek van de Wpg, is de gegevensset, voor zover het politiegegevens betreft, voor FIOD en Inspectie SZW generieker in dit besluit opgenomen dan de overige gegevens. Het is aan deze BOD's om op basis van deze generieke aanduiding te komen tot een lijst van politiegegevens 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, zullen doorgaans gegevens betreffen 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 Inspectie SZW en de FIOD worden verwerkt op grond van artikel 8 respectievelijk artikel 9 van de Wpg. 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 FIOD en Inspectie SZW 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 FIOD respectievelijk Inspectie SZW 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.

Vanaf het moment dat deze BOD's de politiegegevens hebben verstrekt aan het IKZ, zijn het voor verdere verwerking door IKZ persoonsgegevens waarop de AVG van toepassing is. Het zijn dan gegevens van strafrechtelijke aard als bedoelding in artikel 10 van de AVG, waarvoor passende waarborgen en maatregelen zijn getroffen.

Voor zover het niet-persoonsgegevens betreft, geldt het Wpg regime niet en verstrekken de BOD's de volgende gegevens aan het IKZ. Het signaal van fraude in de zorg**,** administratieve kenmerken van een rechtspersoon, handelsgegevens, gegevens over het zorgdomein en de soort zorg waarin de aanbieder zorg levert. Tevens betreft het informatie over afgeronde onderzoeken voor zover noodzakelijk in verband met het betreffende signaal. Ten aanzien van lopende onderzoeken wordt enkel het gegeven verstrekt dát er een onderzoek gaande is.

CONCEPT

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

*Wijze waarop*
Aansluitend op 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 eveneens elektronisch plaats. De mogelijkheden waaraan kan worden gedacht wat betreft de inrichting van deze verstrekking, zoals een portaalfunctie of een berichtenverkeerfunctie, zijn hiervoor in paragraaf 4.2.2 beschreven. 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. In paragraaf 4.7 zijn de regels met betrekking de inrichting, het beheer en de beveiliging van de elektronische voorzieningen en beveiliging van gegevens beschreven.

Ook voor deze verstrekking gelden afwijkende regels ten aanzien van gemeenten en de rijksbelastingdienst. De verstrekking van verrijkte signalen door het IKZ aan gemeenten, geschiedt door tussenkomst van het IB. 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.

Wat betreft de verstrekking van een verrijkt signaal door het IKZ aan geëigende instanties, moet onder andere worden gewaarborgd dat zorgvuldig wordt bepaald welke instanties geëigend zijn en dat elk van die instanties niet meer verrijkte gegevens ontvangt dan noodzakelijk voor de uitvoering van de wettelijke taak. In het geval fiscale gegevens van de rijksbelastingdienst en de FIOD onderdeel uitmaken van het verrijkte signaal, neemt het IKZ de in dit besluit opgenomen regels in acht voordat verstrekking van dat signaal aan ziektekostenverzekeraars plaatsvindt.

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

<u>Resultaat van verrijking</u>
In het geval het resultaat van de verrijking van gegevens 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 instantie(s) 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

CONCEPT

verwachting dat de IGJ met regelmaat als een van de geëigende instanties wordt aangemerkt. Ook voor de rijksbelastingdienst geldt dat het domein mogelijk niet relevant is. Fiscale fraude kan zich immers in ieder domein in de zorg voordoen en als daarvan sprak 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. In paragraaf 4.2.1 is beschreven hoe instanties beoordelen of verstrekking van gegevens aan het IKZ noodzakelijk is. 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). In paragraaf 4.3 is reeds toegelicht welke elementen van belang zijn voor het proces dat voor het maken van voornoemde afweging door het IKZ moet worden ingericht en hier wordt volstaan daarnaar te verwijzen.

<u>Gerichte verstrekking (om de meest geëigende instantie(s) te bepalen)</u>
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 er 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 2.3, vierde lid, van de wet is daarom bepaald dat het IKZ en instanties elkaar in dat geval en voor dit doel bij amvb aangewezen gegevens, waaronder persoonsgegevens, gericht kunnen verstrekken. Deze set aan gegevens is opgenomen in artikel 3.12 van dit besluit en beperkter dan de gegevensset voor verstrekkingen op grond van artikel 2.3, 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 er is gemaakt ten aanzien van de meest geëigende instantie(s).

De voor het specifieke geval bij het overleg betrokken instanties kunnen ook onderling afspraken maken over de vervolgaanpak, bijvoorbeeld welk 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 meerdere instanties onnodig tegelijkertijd

actie ondernemen op een signaal en dit is noodzakelijk voor de effectieve en zorgvuldige bestrijding van fraude in de zorg.

Wat betreft de wijze van verstrekking in dit kader wordt hier verwezen naar hetgeen hierover is toegelicht eerder in deze paragraaf en in paragraaf 4.2.2.

*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 zorgvuldig te kunnen maken. Wat betreft de voorwaarden die voor deze verstrekkingen gelden, wordt hier voor de uitgangspunten verwezen naar hetgeen daarover is beschreven in paragrafen 4.2 en 4.3.
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 (persoons)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.

*Voorwaarden voor verstrekking van fiscale gegevens door het IKZ aan ziektekostenverzekeraars*
Voor de verstrekking van gegevens van de rijksbelastingdienst en de FIOD, voor zover het gegevens uit een fiscaal strafrechtelijk onderzoek betreft, geldt 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.

## 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 van VWS en betrokken instanties.

De wet bepaalt dat persoonsgegevens die het IKZ voor het verrijken van gegevens heeft ontvangen, 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 partijen 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 toezichthoudende, handhavende en opsporende taken beter uit te voeren. Op het moment dat ontwikkelingen zichtbaar worden, kunnen de instanties zelf doelgerichter 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 2.5 van de wet is echter uitgesloten dat het IKZ profileert zoals bedoeld in artikel 4, onder 4, van de 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

CONCEPT

voorspellen, mag plaatsvinden. Er worden door het IKZ 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 van de AVG.

De Minister van VWS 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, die zijn toegelicht in paragraaf 4.7. 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

In deze paragraaf worden de regels toegelicht die gelden voor de gehele gegevensverwerking door het IKZ. Deze regels moeten in samenhang worden gelezen met de hiervoor toegelichte regels ten aanzien van specifieke onderdelen van het proces van gegevensverwerking in het kader van de wet. Tezamen vormen deze regels 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.

Hoewel ook gegevens niet zijnde persoonsgegevens worden verwerkt, zijn gelet op de gevoeligheid van alle in dit kader te verwerken gegevens de principes uit de AVG, zoals privacy by design en privacy by default, gegevensbescherming door ontwerp en standaardinstellingen, leidend.

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

*Algemeen*

In artikel 2.6 van de wet is bepaald dat het IKZ zorg draagt 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 2.7 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

CONCEPT

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 Baseline Informatiebeveiliging Overheid (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 bewoording 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 (persoons)gegevens verstrekken en zelf de gegevens (blijven) verwerken.

Bij de nadere regels die in dit besluit zijn opgenomen, is ten aanzien van de inrichting, het beheer en de beveilig van de elektronische voorzieningen en de beveiliging van gegevens aangesloten bij de AVG. In artikel 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. Ook moeten 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 er 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 sprak 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

CONCEPT

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 kan er onderscheid in autorisatie worden gemaakt tussen medewerkers van het IKZ. 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 daar om 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 van VWS in dit besluit nader geregeld. In dit besluit zijn regels opgenomen ten aanzien van vaststellen van het jaarplan van het IKZ. De Minister van VWS 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 2.8 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 zorg gedragen 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 van VWS 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 2.7, eerste lid, aanhef en 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 het ministerie van VWS. De Minister van VWS 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, 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.

<u>Verrijking</u>
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. 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 er 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. Dit geldt ook voor de gegevens die het IKZ toevoegt uit de bronnen die het zelfstandig raadpleegt.

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 er 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

CONCEPT

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 zaaksinformatiesysteem. De startdatum van de termijn is daarmee gelijk aan die voor het verrijken van signalen. Gegevens die het IKZ 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 voornoemd 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 er 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 weggevallen. Tot slot meldt het IKZ bij de betrokken instantie die het signaal heeft verstrekt, dat het signaal verwijderd is omdat er niet langer een aanleiding tot een vermoeden van fraude bestaat. Andersom kan het ook

CONCEPT

voorkomen dat een van de betrokken instanties tot de conclusie komt dat er 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. 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 verstrekkende 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 (zie hierna) op grond van de AVG, zoals het recht op gegevenswisseling in artikel 17, aanleiding vormen tot verwijdering van gegevens.

### 4.7.5 Uitoefening van de rechten van betrokkenen

In artikel 2.7, tweede lid, 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. 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. Het IKZ richt daartoe een proces in en draagt zorg voor de kenbaarheid van openstaande rechtsmiddelen. Daarbij kan bijvoorbeeld gedacht worden aan een klachtenprocedure.

De betrokkene richt een verzoek tot effectuering van zijn rechten uit de (U)AVG in beginsel tot het IKZ. Conform artikel 14 van de 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, van de 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, is het aan het IKZ te regelen dat mogelijk wordt gemaakt 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 2.7, aanhef en 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 als bedoeld in Boek 2 van het Burgerlijk Wetboek. Er moet bij de aanwijzing rekening worden gehouden met de brede schakering van betrokken instanties, zowel publiek als privaat en zowel centraal als decentraal, zoveel mogelijk recht 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 verantwoordelijk van de Minister van VWS 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 berust bij de Minister van VWS.

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). In overweging moet worden of de instelling het maken van winst al dan niet tot doel mag hebben. 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 van VWS 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 van VWS.

CONCEPT

# 5 Gegevensbeschermingseffectbeoordeling

Voor dit besluit is conform artikel 35 van de 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

PM

## 6.1 Autoriteit persoonsgegevens

PM

## 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.

PM

## 6.3 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, het Waarschuwingsregister, brengt beperkte regeldrukgevolgen met zich mee voor de betrokken instanties, genoemd in artikel 2.1,

CONCEPT

eerste lid, van de wet. Ingevolge artikel 2.1, tweede lid stellen instanties een protocol op. Het besluit bevat nadere vereisten waaraan dit protocol moet voldoen. Het opstellen van het protocol conform de vereisten uit het besluit brengt eenmalig uitvoeringslasten met zich mee. Nadat het protocol is goedgekeurd dient het actueel gehouden te worden, wat slechts een beperkte lastenverzwaring met zich mee zal brengen. 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 2.3, 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 (zie paragraaf 2.2 van de memorie van toelichting). In het kader van de uitvoering van hun wettelijke taken beschikken de betrokken instanties reeds over de (persoons)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 (persoons)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 (persoons)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.

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

CONCEPT

**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 de hele opsomming "zorg of overige dienst als omschreven bij of krachtens de Zorgverzekeringwet, 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" moet worden gebruikt, is die opsomming samengevat in het begrip 'zorg, hulp of ondersteuning'. Het begrip 'aanbieder' is daaraan gekoppeld en betreft dus iemand die "zorg of overige dienst als omschreven bij of krachtens de Zorgverzekeringwet, 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" levert.
Het begrip 'instantie' wordt in deze regeling gedefinieerd als een van de instanties die worden genoemd in artikel 2.3, eerste lid, van de wet, met uitzondering van het IKZ. Dat komt dus neer op het CIZ, (een van de) college(s) van burgemeester en wethouders van een gemeente, de IGJ, de ISZW, 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 IKZ gaat, wordt de term in de tekst van deze algemene maatregel van bestuur ('amvb') alleen gehanteerd in artikelen die op dat deel zien. In het deel dat ziet op het Waarschuwingsregister zorgfraude ('het Waarschuwingsregister'), wordt in deze amvb 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 amvb dat ziet op het Waarschuwingsregister zijn immers alleen de colleges en ziektekostenverzekeraars betrokken, bij het deel van de wet en deze amvb dat ziet op het IKZ 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 deze amvb relevant is.

*Artikel 2.1*
Dit artikel 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 verstrekkende 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 verstrekkende 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

CONCEPT

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. Colleges verstrekken elkaar onderling ook het burgerservicenummer (hierna: BSN) van natuurlijke personen, 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*
In het eerste lid van artikel 2.2 wordt de wijze waarop de goedkeuring van het protocol plaatsvindt doorgedelegeerd naar de Minister van VWS. Gedacht moet worden aan de manier waarop instanties het protocol bij de minister moeten aanleveren, het proces dat vervolgens doorlopen wordt en de wijze waarop de minister instanties informeert over de voortgang. Aan deze vaststelling worden in deze amvb geen verdere vormvoorschriften verbonden.
In het tweede lid wordt de termijn bepaald waarbinnen de minister een besluit moet nemen op de aanvraag tot goedkeuring van het protocol. Voorgeschreven wordt dat ziektekostenverzekeraars en colleges gezamenlijk het protocol ter goedkeuring aanbieden, maar niet is uitgesloten dat zij één of enkele partijen, uit hun midden of daarbuiten, aanwijzen die deze aanvraag namens hen allen indient of indienen. De reactietermijn van de minister is gesteld op drie maanden, om instanties en de minister de kans te geven gedurende de procedure nader met elkaar te corresponderen en instanties de ruimte te geven eventuele wijzigingen in te dienen. Het ligt overigens in de rede dat instanties al in een vroeg stadium met de minister en de AP corresponderen over het concept-protocol om daarover overeenstemming te bereiken. Wanneer de minister het protocol goedkeurt, moet dit besluit en het protocol worden gepubliceerd in de Staatscourant. Hiermee wordt geborgd dat voor een ieder kenbaar is in welke gevallen instanties elkaar gegevens verstrekken op grond van de wet en wat daarvoor de kaders zijn. Zie paragraaf 3.2 van het algemene deel van deze toelichting voor meer informatie over de procedure voor het opstellen van het protocol.

*Artikel 2.3*
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 deze amvb 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 het schrijven van deze amvb. Artikel 2.3 stelt eisen aan het protocol dat instanties moeten opstellen. Daarbij is inspiratie geput uit de eisen die de AP stelt aan protocollen voor privaatrechtelijke zwarte lijsten. Bij het invullen van die eisen zal ook inspiratie kunnen worden geput uit de protocollen van zwarte lijsten die reeds door de AP zijn goed gekeurd. Het Waarschuwingsregister verschilt echter van andere zwarte lijsten in de zin dat de grondslag van dit Waarschuwingsregister publiekrechtelijk van aard is. Dit, tezamen met het feit dat de wet en de amvb niet het

Waarschuwingsregister zelf regelen, heeft gevolgen voor de wijze van formulering van het artikel. Zoals in de toelichting bij het vorige artikel valt te lezen, is de verwachting dat instanties al in een vroeg stadium met de minister en de AP corresponderen over het concept-protocol. Dit biedt ook de mogelijkheid om overeenstemming te bereiken over de interpretatie van de in dit artikel gestelde eisen.
Indien het (reeds vastgestelde) protocol in een later stadium wordt gewijzigd, dient hiervoor, op grond van onderdeel r, dezelfde procedure te worden gevolgd.

*Artikel 2.4*
In het eerste lid van artikel 2.4 wordt in invulling gegeven aan het feit dat de colleges en ziektekostenverzekeraars ingevolge artikel 26 van de AVG gezamenlijke 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 3.8 van het algemene deel van deze toelichting voor meer informatie hierover.
In het tweede lid wordt het eerste 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 3.7 van het algemene deel van deze toelichting.
In het derde lid is bepaald dat concrete beveiligingseisen in een ministeriële regeling worden opgenomen. Het voornemen bestaat om de Baseline Informatiebeveiliging (Stcrt. 2019, 26526) (hierna: BIO) voor te schrijven. De BIO stelt beveiligingsnormen voor publieke en semipublieke organisaties, waar colleges en ziektekostenverzekeraars onder vallen. 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.

*Artikel 2.5*
Naast de gezamenlijke verantwoordelijkheid die colleges en ziektekostenverzekeraars hebben, zoals uitgewerkt in het vorige artikel, 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 verstrekkende instantie ervoor zorg draagt 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 3.7 van het algemene deel van deze toelichting voor meer informatie over de uitoefening van de rechten van betrokkenen.

*Artikel 2.6*

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, van de AVG. Indien echter sprake is van voldoende verzwarende omstandigheden, kan ook worden besloten dat een registratie voor een periode van 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 3.6.1 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 2.3, tweede lid, onderdeel e, een instructie in het protocol worden opgenomen. Zie paragraaf 3.6 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 Inspectie SZW, de rijksbelastingdienst, de FIOD, de Sociale verzekeringsbank, ziektekostenverzekeraars en de zorgautoriteit op grond van artikel 2.3, 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.
Voor de bijzondere opsporingsdiensten wordt in deze artikelen slechts bepaald welke gegevens, niet zijnde politiegegevens, zij verstrekken. Zoals is bepaald in artikel 2.3, eerste lid, van de wet, vindt verstrekking van politiegegevens door de FIOD en de ISZW immers plaats op grond van en met inachtneming van de Wpg. In deze amvb wordt daarom verder niets over politiegegevens geregeld. Zie paragraaf 2.3 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 ISZW of FIOD over die naam beschikt, daarmee een politiegegeven. Het telefoonnummer van de rechtspersoon is geen persoonsgegeven en daarom geen politiegegeven. Het onderhavige artikel regelt daarom welke van deze laatste gegevens over rechtspersonen door de ISZW en de FIOD worden verstrekt. Voor de verstrekking van politiegegevens wordt in artikel 4.1 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 benchmarks 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 benchmarks 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. Zie paragraaf 4.4 van het algemene deel van deze toelichting voor meer informatie over de gegevensset.

*Artikel 3.10*
In artikel 2.3, tweede lid, van de wet worden enkele bronnen genoemd waaruit het IKZ eigenstandig de bij amvb 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 3.11*

In de tweede zin van artikel 2.3, 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 de laatste alinea van paragraaf 4.5 van het algemene deel van deze toelichting. Aan het slot van dat artikellid is echter bepaald dat bij amvb uitzonderingen zijn te stellen op deze regels. Dit artikel stelt 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). Zie paragraaf 4.5 van het algemene deel van deze toelichting voor meer informatie over het verstrekken van gegevens door het IKZ. 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 3.12*
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 2.3, 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 artikel 3.12 van deze amvb is bepaald om welke gegevens dat gaat. Het gaat in om dezelfde gegevens als bedoeld in het vorige artikel, met de aanvulling dat dit ook kan gaan om gegevens over de aard en soort van de vermoede fraude. Deze laatste gegevens hebben de instanties immers 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 2.3, 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 2.3, 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 ISZW 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 ISZW of de FIOD in dit kader met het IKZ uitwisselen.
Zie paragraaf 4.5, onder het kopje ‘Gerichte verstrekking (om de meest geëigende instantie(s) te bepalen)’ voor meer informatie over dit onderwerp.

*Artikel 3.13*

Artikel 3.13 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 3.14*
Artikel 3.14 geeft een invulling aan het noodzakelijkheidsvereiste voor de gegevensverwerking door het IKZ en de uitvoering van het verrijkingsproces. 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 de wijze waarop het IKZ gegevens verwerkt en verrijkt.

*Artikel 3.15*
Om verder te waarborgen dat het verrijkingsproces proportioneel, zorgvuldig en rechtmatig verloopt, is in het eerste lid van artikel 3.15 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 verrijkingsproces 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 de laatste drie alinea's van paragraaf 4.3.2 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 het tweede, derde en vierde lid zijn enkele verplichte treden opgenomen.
In het tweede lid is bepaald dat de eerste fase van het verrijkingsproces 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 het derde lid, 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 3.18.
Het vierde lid 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 het vijfde lid 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 4.3.2 van het algemene deel van deze toelichting voor meer informatie over de getrapte verrijking.

*Artikel 3.16*
Nadat het IKZ de verrijking heeft afgerond, moet het IKZ nagaan wie de geëigende instantie(s) is of zijn en in hoeverre het verrijkte signaal aan de betreffende instantie(s) moet worden verstrekt. Dit artikel regelt dat die beoordeling (mede) in het licht van de gemaakte afspraken en de verkregen toestemming plaatsvindt.
Zie paragraaf 4.5 van het algemene deel van deze toelichting voor meer informatie over het vertrekken van gegevens door het IKZ aan geëigende instanties.

*Artikel 3.17*
In dit artikel is bepaald dat de FIOD en de ISZW, wanneer ze in reactie op een uitvraag van het IKZ geen politiegegevens verstrekken, daarbij niet aan het IKZ bekend maken waarom ze de verstrekking weigeren. Uit het enkele feit dát een bijzondere opsporingsdienst beschikt over politiegegevens, zou immers al strafrechtelijke informatie afgeleid kunnen worden over de persoon wiens gegevens het betreft. Dit betekent niet dat de FIOD en de ISZW nooit beperkte gegevens over een onderzoek naar een persoon mogen delen, maar daaraan moet, net als bij elke andere verstrekking van politiegegevens aan het IKZ, op

grond van en met inachtneming van de Wpg, wel een bewuste noodzakelijkheidsafweging vooraf gaan.
Zie paragraaf 4.4.10 van het algemene deel van deze toelichting voor meer informatie hierover.

*Artikel 3.18*
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 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 dit 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.
In het tweede 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 derde 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 3.19*
De rechten uit hoofdstuk III van de AVG zijn onverkort van toepassing op natuurlijke personen van wie gegevens worden verwerkt. In artikel 3.19 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 3.20*
In de artikelen 3.20 tot en met 3.23 worden enkele zaken geregeld omtrent de financiering en het beheer van het IKZ. Het IKZ is geen zelfstandig bestuursorgaan, maar er wordt wel een bepaalde invloed vanuit de minister geregeld die in veel opzichten lijkt op de invloed die een minister doorgaans op een zelfstandig bestuursorgaan heeft. In artikel 3.20 wordt de financiering, het jaarplan en de verslaglegging van en door het IKZ geregeld. De Minister van VWS wordt in het eerste lid verantwoordelijk gesteld voor de financiering van het IKZ. Deze amvb 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 IZK 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. Te denken valt aan nadere voorschriften aan de subsidie of de wijze en het tijdstip waarop de stukken aan de minister moeten worden gezonden. Dat wordt geregeld in het vierde lid.
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 artikel 3.21 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 3.22*
In het eerste lid van artikel 3.22 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’.
Het vierde lid schrijft voor dat herleidbare gegevens die eenmaal worden verwerkt in de analyseomgeving, daarna niet terug mogen vloeien naar het zaaksinformatiesysteem. Hiermee wordt niet bedoeld dat onderzoek en analyse pas mag plaatsvinden nadat de verwerking/verrijking in het zaaksinformatiesysteem is beëindigd, maar slechts dat gegevens vanuit de analyseomgeving niet mogen vloeien naar het zaaksinformatiesysteem. De gegevens van een persoon mogen dus wel in het zaaksinformatiesysteem en de analyseomgeving tegelijkertijd verwerkt worden en gegevens mogen van het zaaksinformatiesysteem naar de analyseomgeving vloeien, maar niet andersom.
Zie paragraaf 4.7 van het algemene deel van deze toelichting voor meer informatie over gestelde waarborgen.

*Artikel 3.23*
Dit artikel is gebaseerd op artikel 20 van de Kaderwet zelfstandige bestuursorganen en stelt de minister in staat om inlichtingen van het IKZ te verkrijgen. Het derde lid voegt hieraan echter wel een beperking toe, het IKZ verstrekt aan de minister geen persoonsgegevens of gegevens die te herleiden zijn tot individuele rechtspersonen.

*Artikel 3.24*
In artikel 3.24 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.

CONCEPT

In paragraaf 4.5 van het algemene deel van deze toelichting wordt meer uitgelegd over de afspraken die instanties samen moeten maken.

*Artikel 3.25*
In artikel 3.25, eerste lid, is bepaald dat alle gegevensuitwisselingen die op basis van artikel 2.3 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 deze amvb, 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 derde lid van dit artikel 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 paragrafen 4.2.2, 4.3.3, 4.5 van het algemene deel van deze toelichting voor meer informatie over elektronische en geautomatiseerde gegevensuitwisseling.

*Artikel 3.26*
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 3.27*
In artikel 3.27 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 2.3, 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, waar alle bij het IKZ betrokken instanties onder vallen. 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). De Wpg kent een eigen systeem van gegevensverwerking. De wet en deze amvb 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 5.1*
In artikel 5.1 wordt voor de inwerkingtreding van deze amvb aangesloten bij de inwerkingtredingsbepaling 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 amvb 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 deze amvb is gekozen om aan te sluiten bij de citeertitel van de wet.

De Minister van Volksgezondheid,
Welzijn en Sport,

CONCEPT