



Handreiking – Versie 1.0

Uniforme werkwijze voor ontsluiten van gegevens benodigd voor aanpak wachttijden jeugdzorg

Versie 1.0 oktober 2023

Inhoud

Nr.	Onderwerp
0.	Leeswijzer
1.	Schets van urgentie
2.	Rechtsgrondslag
3.	Noodzakelijkheid
4.	Zorgvuldigheid
5.	Conclusie en aanbevelingen

Bijlage 1: Tabel noodzakelijke persoonsgegevens

Leeswijzer

Wat staat er in deze handreiking?

Deze handreiking maakt inzichtelijk op welke gestandaardiseerde wijze gemeenten of jeugdzorgorganisaties persoonsgegevens en zorginhoudelijke informatie van zorgaanbieders kunnen ontvangen in overeenstemming met de privacyregels.

De handreiking is een levend document en zal regelmatig worden geactualiseerd op basis van veranderende wet- en regelgeving. De handreiking zal in de volgende versie worden aangevuld met best practice-voorbeelden en de toevoeging van standaard formats en modellen als bijlagen. Denk aan een model DPIA-format en verwerkingsovereenkomst.

Voor wie is deze handreiking?

Deze handreiking is bestemd en geschreven voor gemeenten en jeugdzorgorganisaties. De handreiking kan ook benut worden voor samenwerkingsverbanden van gemeenten, waarin de jeugdzorg gezamenlijk wordt ingekocht. Dit kan indien de individuele gemeente rechtmatig het samenwerkingsverband heeft gemandateerd om jeugdzorg in te kopen. In dat geval kan overal waar in dit document 'gemeente' staat, 'samenwerkingsverband van gemeenten' ('inkooporganisatie jeugd') worden gelezen.

De uitwerking van de (juridische) werkwijze is gestructureerd met (4) hoofd paragrafen:



1. **Schets van urgentie** als fundament voor het creëren van draagvlak, zodat voor alle betrokken stakeholders de noodzaak van een structurele aanpak helder is.



2. **Rechtsgrondslag** voor het verwerken van persoonsgegevens en gezondheidsinformatie.

- *Is er een legitieme rechtsgrondslag voor de verwerking van (bijzondere) persoonsgegevens door de gemeente?*



3. **Noodzakelijkheid** van de gegevensverwerking op grond van de beginselen van doelbinding en doelspecificatie (minimale gegevensverwerking).

- *Worden uitsluitend die gegevens verwerkt die noodzakelijk zijn voor het vastgestelde doel van de verwerking?*

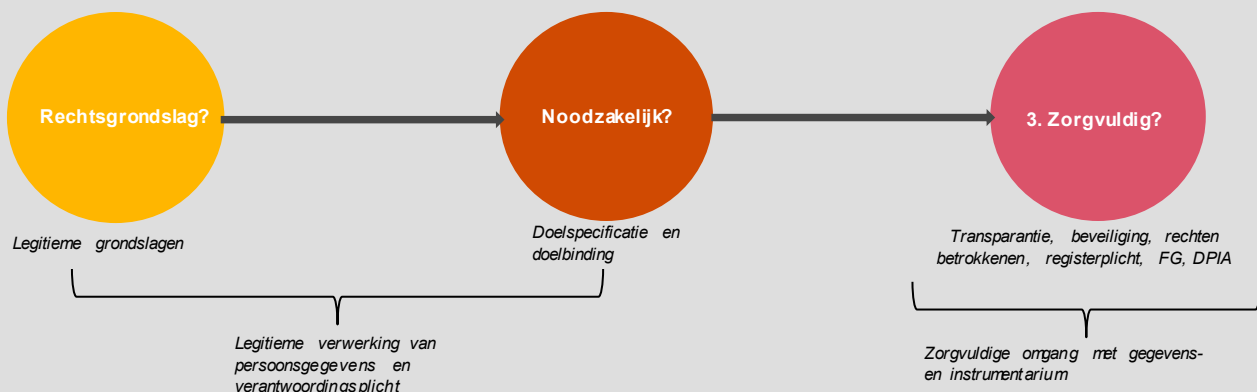


4. **Zorgvuldigheid** van de gegevensverwerking aan de hand van verplichtingen die rusten op de verwerkingsverantwoordelijke en de verplichting tot het treffen van een onderlinge regeling tussen de gemeente of jeugdzorgorganisatie enerzijds en de zorgaanbieders anderzijds.

- *Worden de gegevens op een zorgvuldige wijze verwerkt?*

Bij iedere paragraaf wordt ook besproken wat er nodig is voor praktische implementatie.

Visuele weergave juridisch kader



Schets van urgentie

De maatschappelijke noodzaak is helder: de toegang tot jeugdzorg binnen het Nederlandse jeugdhulpstelsel staat onder druk. De (schaduw)wachtlijsten tot jeugdzorg binnen de regio's lopen op en de toeleiding naar voldoende en passende jeugdzorg wordt steeds complexer. Om de beschikbaarheid van zorg voor jeugdigen te verbeteren, zullen gemeenten en zorgorganisaties binnen de jeugdzorgregio de handen ineen moeten slaan om (beter) grip te krijgen op de wachtlijsten problematiek om zo (kwetsbare) jeugdigen tijdig en dichterbij de zorg te brengen die zij nodig hebben.

Noodzaak voor structurele aanpak

Lange wachtlijsten

De Nederlandse jeugdzorg kampt al jaren met lange wachtlijsten door verschillende factoren als de stijgende zorgvraag, lange behandelingsduur, een krappe arbeidsmarkt en het ontbreken van eigenaarschap in situaties van multiproblematiek. Jeugdigen ontvangen door deze wachtlijsten te laat passende zorg, waardoor in wachttijd de problematiek vaak verergerd en steeds vaker een beroep moet worden gedaan op (schaarse) specialistische jeugdzorg.

Gemeenten hebben in het systeem van decentrale inkoop onvoldoende goede en tijdige data om zelfstandig te kunnen sturen op deze wachtlijstenproblematiek. Hierdoor ontbreekt op zowel regionaal als landelijk niveau inzicht en overzicht van wachtlijsten in de jeugdzorg. Om de wachttijden effectiever te kunnen verbeteren is een structurele aanpak nodig waarin de noodzakelijke data voor gemeenten beschikbaar komt. Door een goede, structurele en privacy bestendige gegevensuitwisseling tussen de gemeenten en zorgaanbieders op te zetten, kunnen de Nederlandse regio's zelf een duurzaam wachttijdbeleid opstellen en de wachttijden binnen de regio monitoren en beheersen.

Data voor monitoring wachtlijsten

Monitoring

Middels monitoring kan de gemeente effectief inzicht en overzicht van de wachttijden bij zorgaanbieders in de regio verkrijgen. Voor effectieve monitoring is nagedacht over de minimale informatiebehoefte van gegevens over jeugdigen (*Bijlage 1*):

- Burgerservicenummer (BSN): om vanuit kwantitatief perspectief het aantal wachtenden te kunnen monitoren en dubbele registraties op wachtlijsten op te sporen (en op te schonen);

- Zorginhoudelijke gegevens: om hulpvragen te identificeren en vanuit kwalitatief perspectief na te gaan of er vanuit de regio alternatieven kunnen worden aangeboden indien een jeugdige niet direct geplaatst kan worden bij een gewenste zorgaanbieder.

Uiteraard is voorafgaand aan de vaststelling van de minimale basisset aan (bijzondere) persoonsgegevens – als opgenomen in Bijlage 1 – onderzocht in hoeverre de noodzakelijke data al direct uit het bestaande (administratieve/ financiële) berichtenverkeer tussen zorgaanbieders en de gemeente kon worden gehaald. Dit bleek niet het geval, omdat uit het huidige iJw berichtenverkeer niet een volledig beeld kan worden verkregen van het zorgproces van de jeugdige. Dit komt omdat bijvoorbeeld een toewijzingsbericht vanuit de gemeente met terugwerkende kracht kan worden afgegeven, waardoor een onjuist beeld ontstaat dat de toewijzing van zorg overeenkomt met de daadwerkelijke startdatum van de zorg. Dit maakt dat de ontsluiting van aanvullende (minimale) basisset aan (bijzondere) persoonsgegevens noodzakelijk is.

Borgen van vertrouwen

Vertrouwen

Het is van belang dat gemeenten aan zorgaanbieders duidelijkheid kunnen bieden dat de aanvullende (bijzondere) persoonsgegevens in overeenstemming met de privacywetgeving op een zorgvuldige wijze zullen worden uitgewisseld. Hiermee zal de gemeente het vertrouwen moeten geven dat met de aanvullende gegevens op een zorgvuldige en integere manier zal worden omgegaan. Dit omvat tevens de betrouwbaarheid van de systemen/dashboards waarop de data zal worden opgeslagen.

Voor het creëren van draagvlak onder alle betrokkenen is het bovendien van belang dat een evenwicht wordt behouden tussen het medisch beroepsgeheim van de zorgaanbieders en beschikbaarheid van data aan gemeenten. Zo wordt toegewerkt naar een structurele aanpak waarin sprake is van datasolidariteit en data-altruïsme: de bereidheid van zorgaanbieders om (zorg-)data te delen voor een groter belang, namelijk om de wachttijden in de jeugdzorg te reduceren.

Rechtsgrondslag

Is er een legitieme rechtsgrondslag voor de verwerking van (bijzondere) persoonsgegevens door de gemeente?

Juridisch kader

- Artikel 6, 7 en 9 Algemene verordening gegevensbescherming ("AVG")
- Uitvoeringswet Algemene verordening gegevensbescherming ("UAVG")
- Wet op de Geneeskundige Behandelingsovereenkomst ("WGBO")
- Jeugdwet

Waarom mag een zorgaanbieder de gegevens niet zomaar delen met de gemeente?

De AVG strekt ter bescherming van persoonsgegevens. Dit zijn alle gegevens die herleidbaar zijn naar een individu. Daarbij is er onderscheid in twee typen persoonsgegevens, die beiden relevant zijn in het kader van deze werkwijze.



Burgerservicenummer (BSN) en andere niet-bijzondere persoonsgegevens

Een ander gegeven kan een geboortejaar of postcode zijn, maar er is alleen sprake van een persoonsgegeven indien deze postcode of geboortejaar aan de naam of BSN van de cliënt is gekoppeld. Hierdoor is het herleidbaar tot de persoon.

- Voor een rechtmatige verwerking van deze 'gewone' persoonsgegevens is op grond van de AVG een gerechtvaardigde *wettelijke grondslag* vereist.



Bijzondere persoonsgegevens, betreffende de gezondheid

Gegevens over zorginhoudelijke aspecten zijn een voorbeeld van bijzondere persoonsgegevens onder de AVG. Gegevens kwalificeren als bijzondere persoonsgegevens indien deze gekoppeld zijn aan het BSN of de naam van de cliënt, omdat deze gegevens dan herleidbaar zijn naar een persoon.

- Voor bijzondere persoonsgegevens geldt het verwerkingsverbod. In beginsel is de verwerking van bijzondere persoonsgegevens verboden, tenzij een uitzondering van toepassing is. De (U)AVG maakt een uitzondering op het verwerkingsverbod indien verwerking noodzakelijk is voor 'de goede uitvoering van een wettelijk voorschrift'.



Medisch beroepsgeheim

De WGBO beschermt de toegang van de patiënt tot zorg, en zijn veiligheid en die van de samenleving door het medisch beroepsgeheim. De gegevens die de gemeente bij de zorgaanbieder wil uitvragen, vallen *onder de reikwijdte van het medisch beroepsgeheim*.

Door het plaatsen van een cliënt op de wachtlijst ontstaat een geneeskundige behandelingsovereenkomst waardoor het beroepsgeheim van toepassing is.

- Om dit te mogen doorbreken, moet er een gegronde reden zijn.

Waarom is er in dit geval toch een wettelijke grondslag om gegevens te delen?

Waarom voldoet de wettelijke grondslag van individuele toestemming niet?

Als een deel van de patiënten geen toestemming verleent, verleende toestemming later wordt ingetrokken of een deel van de patiënten niet in staat is om toestemming te verlenen, dan heeft dat als consequentie dat onvoldoende gegevens beschikbaar zijn voor de gemeente om efficiënt aan wachtlijstmonitoring te kunnen doen. Dit geldt ook wanneer een zorgaanbieder afziet van het vragen van individuele toestemming aan de patiënt, bijvoorbeeld indien het vragen van deze toestemming te veel (kostbare) tijd kost. Indien niet door alle zorgaanbieders de relevante gegevens worden aangeleverd, kan dit bovendien leiden tot selectieve bias. Dit betekent dat de gemeente beschikt over een dataset die geen juiste afspiegeling en niet representatief is voor de volledige groep aan (wachtende) patiënten. De conclusies over de wachtlijsten zijn dan niet of minder betrouwbaar.

Waarom is het volledig anonimiseren niet mogelijk?

Bij anonimiseren van patiëntgegevens is het niet langer mogelijk dat de patiëntgegevens van de zorgaanbieder op persoon gekoppeld kunnen worden. Dit vormt een probleem bij het identificeren van de hulpvraag en vanuit kwalitatief perspectief na te gaan of er vanuit de regio alternatieven kunnen worden aangeboden (door middel van zorgbemiddeling) indien een jeugdige niet direct geplaatst kan worden bij een gewenste zorgaanbieder.

Omdat zowel het werken met individuele toestemming, als het werken met (volledig) anonimiseren niet werkbaar is voor het goed laten functioneren van wachtlijstmonitoring is een wettelijke grondslag nodig voor een rechtmatige verwerking van (bijzondere) persoonsgegevens door de gemeente.

Wettelijke verplichting t.a.v. verstrekken van gegevens door jeugdzorgaanbieders

- ✓ Op grond van artikel 7.4.0 lid 1 Jeugdwet *mogen gemeenten* persoonsgegevens, waaronder bijzondere persoonsgegevens, verwerken voor zover dat noodzakelijk is voor onder andere de toeleiding naar jeugdhulp.
- ✓ Artikel 7.4.0 lid 2 en 3 Jeugdwet *verplicht zorgaanbieders* om de gegevenste verstrekken die voor de gemeente noodzakelijk zijn om haar bij en krachtens de Jeugdwet geregelde taken uit artikel 7.4.0 lid 1 goed te kunnen vervullen.
- ✓ De verstrekking kan op grond van artikel 7.3.11 lid 1 Jeugdwet geschieden *zonder inachtneming* van de beperkingen die voortvloeien uit de (medische) geheimhoudingsplicht.

Wettelijke verplichting t.a.v. gegevensverwerking door gemeente ten behoeve van de uitvoering van de Jeugdwet

- ✓ De gemeente kan zowel het BSN als andere (bijzondere) persoonsgegevens van cliënten bij zorgaanbieders opvragen, indien deze noodzakelijk zijn voor het uitvoeren van de wettelijke toeleidingstaak.
- ✓ Daarbij geldt echter wel dat de gemeente deze persoonsgegevens op grond van de wet niet zomaar verder mag verwerken (waaronder het verstrekken aan anderen, zowel binnen- als buiten de organisatie).

Kernpunten

Wettelijke grondslag

- De gemeente kan op grond van haar wettelijke toeleidingstaak naar jeugdhulp zowel het BSN als zorginhoudelijke informatie opvragen bij zorgaanbieders indien deze gegevens noodzakelijk zijn in het kader van de uitvoering van deze wettelijke taak. Zie voor de verdere invulling van het vereiste van noodzakelijkheid de volgende paragraaf.

Toepasselijke gegevens

- Deze wettelijke toeleidingstaak geldt als rechtsgrondslag voor alle persoonsgegevens (zowel gewone als bijzondere persoonsgegevens) die in *Bijlage 1* zijn opgenomen.

Zorgaanbieders

- De zorgaanbieders zijn op basis van deze wettelijke taak verplicht deze gegevens aan de jeugdzorgorganisatie te verstrekken. De medische geheimhoudingsplicht staat hieraan niet in de weg.

Noodzakelijkheid

Worden uitsluitend die gegevens verwerkt die noodzakelijk zijn voor het vastgestelde doel van de verwerking?

Juridisch kader

- Artikel 5 Algemene verordening gegevensbescherming ("AVG"): basisbeginselen voor verwerking persoonsgegevens

Aan welke noodzakelijkheidsbeginselen moet de gemeente voldoen?

Doelbinding

- ✓ Persoonsgegevens mogen alleen worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt.
- ✓ De specifieke doeleinden waarvoor persoonsgegevens worden verwerkt moeten zijn vastgesteld op het moment dat de persoonsgegevens worden verzameld.
- ✓ De gemeente mag als verwerkingsverantwoordelijke alleen (bijzondere) persoonsgegevens verwerken voor het doel waarvoor ze zijn verkregen. Dit wil zeggen dat de gemeente alleen het BSN en zorginhoudelijke informatie mag gebruiken voor de monitoring van wachttijden voor het *doel* om de toeleiding naar jeugdhulp te waarborgen.

Doelspecificatie en opslagbeperking (minimale gegevensverwerking)

- ✓ De persoonsgegevens dienen toereikend en terzake dienend te zijn en beperkt te blijven tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Het principe van dataminimalisatie vereist dat de gemeente vaststelt *welke gegevens* noodzakelijk zijn voor het doel. De gegevens zoals opgenomen in Bijlage 1 zijn hierbij richtinggevend.

Kernpunten

Voldoen aan beginselen doelbinding en doelspecificatie

- Het vastgestelde doel is het inzichtelijk maken van de wachttijden om de toeleiding naar jeugdhulp te kunnen waarborgen. In *Bijlage 1* is per persoonsgegeven beargumenteerd hoe er aan doelbinding en doelspecificatie wordt voldaan. Hiermee voldoet de gemeente aan deze beginselen.

Aanvullende aandachtspunten

- Aandachtspunt is dat de gemeente ervoor dient te zorgen dat de persoonsgegevens niet langer bewaard worden dan noodzakelijk is voor het aanpakken van de wachttijden. Ook mag er niet méér informatie worden uitgevraagd of ontvangen dan nodig, en waar nodig dienen gegevens geanonimiseerd of gepseudonimiseerd te worden (denk aan het gebruiken van een hash van het BSN). Verder dient de gemeente zich te vergewissen welke medewerkers toegang hebben tot de data en of deze toegang tot een minimum is beperkt.

Zorgvuldigheid

Worden de gegevens op een zorgvuldige wijze verwerkt? (I)

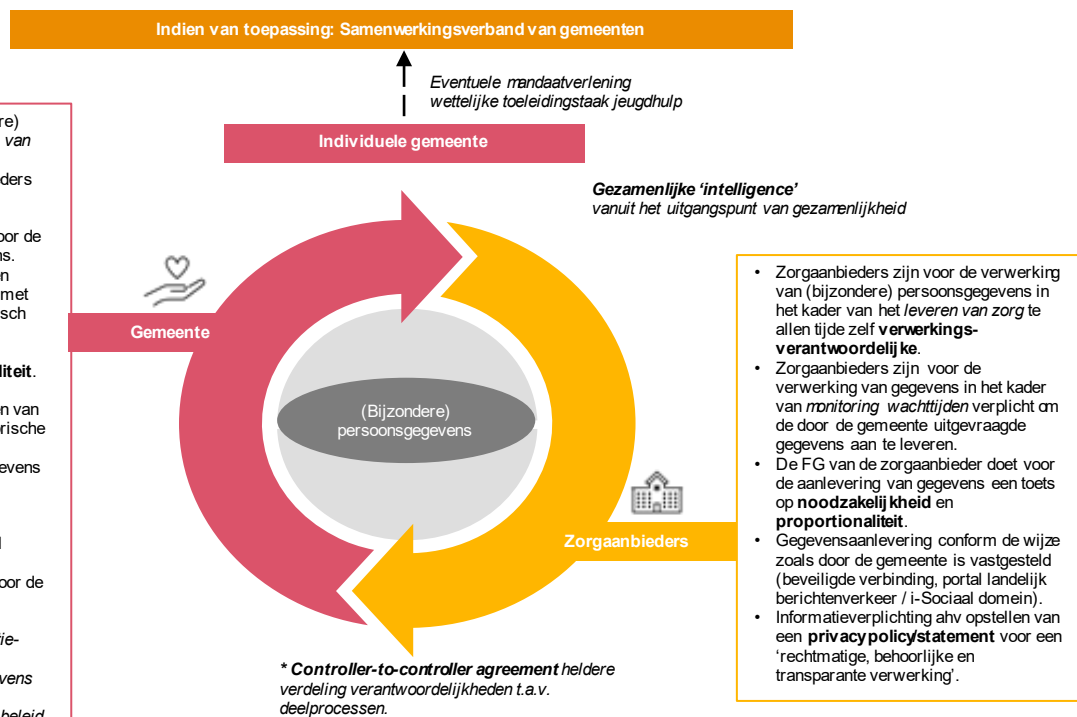
Juridisch kader

- Artikel 24 Algemene verordening gegevensbescherming ("AVG")
- KNMG-richtlijn 'Omgaan met medische gegevens'

Verwerkingsverantwoordelijkheden

- ✓ De **gemeente** kwalificeert als **verwerkingsverantwoordelijke** volgens de AVG, en is daarmee verplicht om passende en effectieve maatregelen uit te voeren en moet kunnen aantonen dat elke verwerkingsactiviteit in overeenstemming is met de AVG.
- ✓ De **zorgaanbieders** zijn op grond van deze wettelijke taak alleen verantwoordelijk voor de **aanlevering van de gevraagde gegevens**.

Procesoverzicht verwerkingsverantwoordelijkheden



- Vanaf het moment dat de (bijzondere) persoonsgegevens voor **monitoring van wachttijden** zijn ontvangen door de gemeente, verliezen de zorgaanbieders controle over de gegevens en is de gemeente **verwerkingsverantwoordelijke** voor de verwerking en beheer van gegevens.
- Aangeleverde informatie mag alleen worden verwerkt door ambtenaren met een **geheimhoudingsplicht** (medisch beroepsgeheim / art. 2:5 Awb).
- De FG van de gemeente toetst op **noodzakelijkheid en proportionaliteit**.
- **Privacy by Design** voor elke verwerkingsactiviteit door het treffen van passende technische en organisatorische maatregelen (t.a.v. (o.a.) deling, archivering en vernietiging van gegevens en borgen rechten van (betrokken) cliënten).
- Gegevens die reeds volgen uit het landelijk berichtenverkeer/i-Sociaal domein, worden niet uitgevraagd.
- De gemeente is verantwoordelijk voor de wijze van gegevensaanlevering overeenkomstig **NEN: 7510, ISO:27001, Baseline informatiebeveiliging Overheid**.
- NB. Voor **ontsluiting van BSN gegevens** gelden aanvullende voorwaarden. Gemeenten hebben hierop (eigen) beleid gemaakt, zoals bv. het toepassen van hashing.

- Zorgaanbieders zijn voor de verwerking van (bijzondere) persoonsgegevens in het kader van het **leveren van zorg** te allen tijde zelf **verwerkingsverantwoordelijke**.
- Zorgaanbieders zijn voor de verwerking van gegevens in het kader van **monitoring wachttijden** verplicht om de door de gemeente uitgevraagde gegevens aan te leveren.
- De FG van de zorgaanbieder doet voor de aanlevering van gegevens een toets op **noodzakelijkheid en proportionaliteit**.
- Gegevensaanlevering conform de wijze zoals door de gemeente is vastgesteld (beveiligde verbinding, portal landelijk berichtenverkeer / i-Sociaal domein).
- Informatieverplichting ahv opstellen van een **privacy policy statement** voor een 'rechtmatige, behoorlijke en transparante verwerking'.

Praktische tips voor de uitvoering

Voorbeelden van technische en organisatorische maatregelen (check ook NEN:7510, ISO:27001, Baseline informatiebeveiliging Overheid)



- ✓ Logische (netwerk, domein of applicatie) en fysieke (toegangs)beveiliging
- ✓ Technisch beheer van de (zo beperkt mogelijke) autorisaties
- ✓ Automatisch verwijderen van verouderde gegevens
- ✓ Versleuteling van gegevens
- ✓ Hashing/pseudonimiseren
- ✓ Verantwoordelijkheden voor informatiebeveiliging



Andere verplichtingen als verwerkingsverantwoordelijke

- ✓ Bijhouden van een verwerkingsregister (bij meer dan 250 medewerkers)
- ✓ Uitvoeren van een Data Protection Impact Assessment ("DPIA") voor gegevensverwerkingen met een hoog privacyrisico
- ✓ Bijhouden van een register van datalekken die zijn opgetreden en het aanstellen van een functionaris gegevensbescherming



Extra (niet verplichte) maatregelen als verwerkingsverantwoordelijke:

- ✓ Aansluiten bij een gedragscode
- ✓ Behalen van een certificaat
- ✓ Hanteren van een specifiek ICT-beveiligingsbeleid
- ✓ Aflleggen van verantwoording over de verwerking van persoonsgegevens in het (privacy)jaarrapport

Kernpunten

Verwerkingsverantwoordelijkheden

- De gemeente is als **verwerkingsverantwoordelijke** verantwoordelijk voor de wijze waarop de gegevens door zorgaanbieders moeten worden aangeleverd. Zie ook bovenstaand procesoverzicht.

Technische en organisatorische maatregelen vereist

- De gemeente dient als **verwerkingsverantwoordelijke** passende **technische en organisatorische maatregelen** te treffen om zodoende een passend gegevensbeschermingsbeleid te kunnen waarborgen. Dit wordt ook wel 'Privacy by Design' genoemd.

Zorgvuldigheid

Worden de gegevens op een zorgvuldige wijze verwerkt? (II)

Juridisch kader

- Artikelen 12-14 Algemene verordening gegevensbescherming ("AVG")

Rechten van betrokkenen jeugdigen

- ✓ Volgens het **transparantiebeginsel** moet het voor *betrokken jeugdigen* transparant zijn dat hun persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt en in hoeverre dat het geval is.
- ✓ De informatie en communicatie hierover moet eenvoudig en begrijpelijk zijn, en gaan over:
 - Identiteit van de verwerkingsverantwoordelijke;
 - Doeleinden van de verwerking;
 - Risico's, regels, waarborgen en (uitoefening van) rechten door de betrokkene;
 - Overige informatie die leidt tot transparante verwerking, zoals een mededeling over welke gegevens zijn verwerkt.

Praktische tips voor de uitvoering



De rechten van betrokkenen die de gemeente dient te waarborgen zijn de volgende:

- ✓ recht op inzage (en ontvangen van kopie gegevens);
- ✓ recht op vergetelheid;
- ✓ recht op rectificatie en aanvulling;
- ✓ recht op dataportabiliteit;
- ✓ recht op beperking van de verwerking;
- ✓ recht met betrekking tot geautomatiseerde besluitvorming en profilering (besluiten van een menselijke blik);
- ✓ recht om bezwaar te maken tegen de gegevensverwerking;
- ✓ recht op duidelijke informatie over wat met de persoonsgegevens wordt gedaan.



Vormgeven controller-to-controller agreement:

- ✓ Vaststellen van ieders verantwoordelijkheid voor de naleving van de verplichtingen die voortvloeien uit de AVG;
- ✓ Optioneel: nadere afspraken maken over (zelfstandige) verantwoordelijkheid ten aanzien van de verwerking van bijzondere persoonsgegevens;
- ✓ Beschrijven omgang met de rechten van betrokken jeugdigen (Wie beantwoordt klachten of vragen van betrokkenen en hoe wordt er omgegaan met een eventueel datalek?).

Kernpunten

Borging rechten betrokkenen

- De gemeente zal als verwerkingsverantwoordelijke de rechten van betrokkenen na moeten leven en zal daarom moeten onderzoeken op welke wijze deze rechten worden geborgd.

Controller-to-controller agreement

- De gemeente en de zorgaanbieders kunnen in een gezamenlijke regeling (een *controller-to-controller agreement*) onderling afspraken maken over de verschillende deelprocessen.

Conclusie en aanbevelingen

Op basis van haar wettelijke (toeleidings)taak mag een gemeente* zowel het BSN als zorginhoudelijke gegevens opvragen bij zorgaanbieders en zullen zorgaanbieders mee moeten werken aan dit verzoek.



*Voor samenwerkingsverbanden van gemeenten geldt hetzelfde indien er sprake is van een aan dit verband gemandateerde taak. Deze bevoegdheid is **niet** onbepaald. De gemeente mag nooit méér gegevens opvragen en ontvangen dan strikt noodzakelijk zijn voor de uitvoering van haar wettelijke taak. Zie *Bijlage 1* als 'guidance' van de mogelijk uit te vragen gegevens.

Checklist voor uitvoering

I De gemeente zal als verwerkingsverantwoordelijke passende **technische en organisatorische maatregelen** moeten treffen en zal moeten onderzoeken op welke wijze de rechten van betrokkenen worden geborgd.

II De gemeente zal in een **onderlinge regeling** met de zorgaanbieders nader invulling dienen te geven aan ieders verantwoordelijkheden voor de naleving van de verplichtingen die voortvloeien uit de AVG.

Aanvullende aanbevelingen voor uitvoering



Opstellen en publiceren privacy statement, zodat voor betrokkenen duidelijk is welke persoonsgegevens met welk doel worden verzameld, wie voor welke taken verantwoordelijk is en hoe betrokkenen hun rechten kunnen uitoefenen.



Geen uitvraag van gegevens die reeds uit het berichtenverkeer kunnen worden afgeleid, om onnodige administratieve last van zorgaanbieders te voorkomen.



Zorgaanbieders inzicht verschaffen in de wijze waarop de gegevens worden verwerkt, zodat er gezamenlijk wordt gewerkt aan een oplossing voor de wachtlijsten. Dit kan worden opgenomen in de onderlinge regeling.

Bijlage 1: Tabel noodzakelijke persoonsgegevens

- ✓ Onderstaand is een uitwerking opgenomen van zowel de 'gewone' als **bijzondere persoonsgegevens** die noodzakelijk zijn voor het efficiënt kunnen monitoren van de wachttijden door gemeenten, en daarmee de invulling van de wettelijke taak.
- ✓ Deze uitwerking is **richtinggevend** voor de persoonsgegevens die een gemeente kan en mag opvragen, hierbij is maatwerk per gemeente mogelijk en wordt zo veel mogelijk aansluiting gezocht bij de datastromen uit het elektronisch berichtenverkeer vanuit het uitgangspunt van efficiëntie en dataminimalisatie. Indien de noodzaak zorgvuldig onderbouwd kan worden en er hierover in de regio overeenstemming kan worden bereikt, kan het ook mogelijk zijn om meer of andere gegevens op te vragen.

Gegeven	Onderbouwing noodzakelijkheid
AGB-code	De AGB-code is de unieke code van de zorgaanbieder. Met deze code wordt binnen het iJw berichtenverkeer de zorgaanbieder geïdentificeerd in de jeugdzorgketen. Met deze AGB-code ontstaat er tot op het niveau van zorgaanbieder inzicht in de wachttijden.
BSN (one-way hash)	Het BSN is de unieke identifier om de cliënt te identificeren. Het BSN is noodzakelijk om verschillende databronnen te kunnen koppelen. Hierdoor kunnen cliënten die op meerdere wachtlijsten voorkomen inzichtelijk gemaakt worden, zodat ze niet dubbel meegeteld worden en kan een cliënt op een (eerdere) wachtlijst gekoppeld worden aan het iJw berichtenverkeer.
Toewijzingsnummer	Het toewijzingsnummer is noodzakelijk om een koppeling met de productie te maken en daarmee de wachtlijst op te schonen. Als een jeugdige meerdere toewijzingen heeft openstaan (dus op meerdere producten wacht) dan moeten we hier onderscheid in kunnen maken. Enkel het BSN volstaat dan niet.
Geboortejaar	Op basis van geboortejaar wordt inzichtelijk gemaakt hoe de wachttijden zich verhouden naar leeftijd (categorie).
Postcode client	Op basis van de postcode van de cliënt wordt inzichtelijk gemaakt hoe de wachttijden zich verhouden naar postcode.
Gemeentecode verantwoordelijke gemeente	Op basis van gemeentecode wordt inzichtelijk gemaakt welke gemeente verantwoordelijk is voor de jeugdige, aangezien naar verwachting de meeste wachtlijsten cliënten bevatten uit meerdere gemeenten in de regio. Het gaat hier om de verantwoordelijke gemeente, niet om de woonplaats van de cliënt. Vanwege het Woonplaatsbeginsel kan dit van elkaar afwijken.
Datum eerste aanmelding zorgaanbieder (na verwijzing)	De datum eerste aanmelding bij zorgaanbieder is het meest concrete en noodzakelijk meetmoment om aan te duiden wanneer een wachttijd start en om wachttijden bij zorgaanbieder te bepalen. Om wachttijden tussen fasen in het jeugdzorgproces inzichtelijk te maken is dit het startpunt. Het gaat hier om de datum aanmelding vanuit een verwijzer en dus de datum dat een jeugdige op de aanmeldlijst komt bij een zorgaanbieder.
Datum start behandeling	De datum start behandeling is meestal gelijk aan een 305-bericht, maar er is niet altijd een toewijzing bij start behandeling. Indien de toewijzing ontbreekt, is de datum start behandeling noodzakelijk.
Productcode	De productcode is noodzakelijk om te weten om welk type hulp het gaat.
Datum start multidisciplinair overleg (of vergelijkbaar overleg tussen verschillende zorgaanbieders)	Het multidisciplinair overleg heeft betrekking op cliënten die niet direct in zorg genomen kunnen worden door de Zorgaanbieder waar de cliënt naar verwezen is. Dit kan bijvoorbeeld een gevolg zijn van capaciteit, expertise of voorkeuren van de cliënt. Tijdens het multidisciplinair overleg wordt vervolgens door verschillende zorgaanbieders gekeken waar de cliënt passende zorg kan krijgen. Op basis van de datum start multidisciplinair overleg wordt inzichtelijk gemaakt wat de doorlooptijd is tussen de eerste aanmelding bij de Zorgaanbieder en de datum start multidisciplinair overleg.
Datum eind multidisciplinair overleg (of vergelijkbaar overleg tussen verschillende zorgaanbieders)	De datum start multidisciplinair overleg is noodzakelijk om het einde van de wachttijd bij het multidisciplinair overleg te bepalen (indien aanbieder niet goed de aanmelding registreert). Hiermee wordt de doorlooptijd van het zorgbemiddelingstraject inzichtelijk gemaakt.
Productcode/opdracht bij start multidisciplinair overleg	De productcode/opdracht bij start van het multidisciplinair overleg is noodzakelijk omdat de vraag soms verandert gedurende de wachttijd bij het multidisciplinair overleg.
Productcode/opdracht bij eind multidisciplinair overleg	Zie hierboven.
Verwijzer	De verwijzer is een gestandaardiseerde lijst met vaste waarden, het type verwijzer. Deze gegevens zijn te herleiden uit het iJw berichtenverkeer, maar worden opgevraagd in geval de cliënt nog niet in zorg is genomen. Deze gegevens worden gebruikt om inzichtelijk te maken hoe de wachtlijsten zich verhouden tot het type verwijzer.
Optioneel: Ingangsdatum toewijzing (uit iJW301)	<i>Kan eventueel vervallen. Als er BSN's beschikbaar zijn, kunnen BSN data gekoppeld worden aan toewijzingsdata en is een extra uitvraag hierop niet nodig.</i>
Optioneel: Begin zorg (uit iJW305)	<i>Kan eventueel vervallen. Als er BSN's beschikbaar zijn, kunnen BSN data gekoppeld worden aan toewijzingsdata en is een extra uitvraag hierop niet nodig.</i>



Deze handreiking van het OZJ is tot stand gekomen in samenwerking met PwC Legal. Hij is bedoeld als algemene informatie ten behoeve van gemeenten en kan niet worden gezien (professioneel) advies. De handreiking behoeft periodieke updates (bijvoorbeeld als gevolg van wetswijzigingen). Aanvullende toetsing voor passend maatwerk is noodzakelijk. Voor nadere informatie of advisering op maat kunt u contact opnemen met: Martje Weusten, martje.weusten@pwc.com en Inge Bakker, inge.bakker@vng.nl, van het Team Aanpak Wachttijden binnen het OZJ. Voor meer informatie zie ook:

- <https://www.pwc.nl/nl/dienstverlening/legal-services.html>
- <https://www.voordejeugdenhetgezin.nl/aanpak-wachttijden>