

OVEREENKOMST GEZAMENLIJKE VERWERKINGSVERANTWOORDELIJKEN INZAKE
GEMEENSCHAPPELIJKE REGELING JEUGDHULP RIJNMOND

A. ONDERGETEKENDEN:

I. Openbaar Lichaam Jeugdhulp Rijnmond (OLJR), gevestigd te Rotterdam aan de Coolsingel 40, ingeschreven in het handelsregister onder KvK nummer 62019163, namens deze rechtsgeldig vertegenwoordigd door de voorzitter van het algemeen bestuur, de heer R. Buijt, en Secretaris-Directeur, mevrouw S. Hammer,;

en

II. Gemeente Rotterdam, gevestigd te Rotterdam aan de Coolsingel 40, ingeschreven in het handelsregister onder KvK nummer 62019163, namens deze rechtsgeldig vertegenwoordigd door de conerndirecteur Maatschappelijke Ontwikkeling, heer E. Hadziavdic;

en

III. Gemeente, gevestigd te aan de, ingeschreven in het handelsregister onder KvK nummer, namens deze rechtsgeldig vertegenwoordigd door ,, (naam);

De hierboven genoemde partijen, zijn hierna gezamenlijk ook aan te duiden als "Partijen" en ieder afzonderlijk als "Partij", "Gemeente" of "OLJR".

B. OVERWEGENDE DAT:

- I. Het openbaar lichaam Jeugdhulp Rijnmond (OLJR) een verband is van samenwerkende gemeenten. De regeling betreft het uitvoeren van de bovenlokale taken door middel van onder andere het contracteren van specialistische jeugdhulp. Om te kunnen sturen op passende jeugdhulp heeft het OLJR ook een informatievoorzieningstaak. Om zicht te krijgen op contractafspraken over ingezette hulp, kosten en het zorglandschap leveren gemeenten, zorgaanbieders en ketenpartners gegevens aan over het zorggebruik op casusniveau. Deze gegevens worden verwerkt tot informatie over de ingekochte/gesubsidieerde hulp en getoond in een dashboard. Contractmanagers van de uitvoeringsorganisatie, gemeenten, zorgaanbieders en ketenpartners gebruiken deze informatie in de sturing op passende jeugdhulp. Zie ook bijlage 1 voor een omschrijving van de aard en omvang van de opdracht ;
- II. de gegevens over geleverde hulp op casusniveau uit de cliëntadministraties van gemeenten komen. Een specificatie van de uitgevraagde gegevens bij gemeenten is bijgevoegd, zie bijlage 2;
- III. de Gemeente Rotterdam de uitvoerende gemeente is voor het OLJR;
- IV. bij de samenwerking door Partijen persoonsgegevens worden verwerkt, waarbij zij gezamenlijk het doel en de middelen van de verwerking(en) bepalen en dus als uitgangspunt nemen dat er sprake is van een gezamenlijke verwerkingsverantwoordelijkheid als bedoeld in artikel 26 AVG;
- V. Partijen bij het uitvoeren van hun publieke taak veelal bijzondere categorieën van persoonsgegevens (gevoelige gegevens) verwerken in de zin van de Algemene Verordening Gegevensbescherming ("AVG");
- VI. Partijen gezamenlijk persoonsgegevens verwerken en hun respectieve verantwoordelijkheden vastleggen in het kader van het verwerken van persoonsgegevens zoals beschreven in Bijlage 2;

- VII. Partijen afspraken willen maken ten aanzien van de samenwerking en deze wensen vast te leggen in de onderhavige overeenkomst gezamenlijke verwerkingsverantwoordelijken inzake de Gemeenschappelijke Regeling Jeugdhulp Rijnmond (hierna te noemen: Overeenkomst);
- VIII. Partijen nog nadere schriftelijke afspraken kunnen maken omtrent de uitvoering van de dienstverlening, kwaliteit, vergoeding van de kosten en aansprakelijkheid;
- IX. voor zover er begrippen in de overeenkomst worden benoemd – die overeenstemmen met definities uit art. 4 AVG, UAVG of sectorale wetgeving – prevaleert de uitleg zoals die door de wetgever in die wetten staat benoemd.

C. VERKLAREN ALS VOLGT TE ZIJN OVEREENGEKOMEN:

Artikel 1 - Definities

1.1 Voor de definities die worden gebruikt in deze Overeenkomst in het kader van de verwerking van persoonsgegevens (zoals maar niet beperkt tot: persoonsgegevens, verwerking, betrokkene, verwerkingsverantwoordelijke, verwerker, inbreuk in verband met persoonsgegevens en derde) wordt aangesloten bij de overeenkomstige definities uit de Algemene Verordening Gegevensbescherming (AVG).

1.2 De volgende aanvullende definities zijn alleen van kracht binnen deze Overeenkomst:

Bijlagen:	aanhangsels bij deze Overeenkomst, die na door beide Partijen te zijn geparafeerd, deel uitmaken van deze Overeenkomst.
OLJR	Openbaar Lichaam Jeugdhulp Rijnmond
De regeling:	de Gemeenschappelijke Regeling Jeugdhulp Rijnmond (GRJR).
Samenwerkingsovereenkomst:	de onderhavige overeenkomst met inbegrip van alle Bijlagen.
De gemeente:	een aan deze samenwerkingsovereenkomst deelnemende gemeente en gezamenlijk verwerkingsverantwoordelijke.
Colleges:	de colleges van burgemeester en wethouders van de gemeenten.
Bovenlokale taken:	gemeentelijke taken in het kader van de Jeugdwet waarvan de deelnemende colleges hebben vastgesteld dat deze in gezamenlijkheid worden uitgevoerd.
Uitvoerende Gemeente:	de door het algemeen bestuur aangewezen gemeente die in opdracht van en namens het algemeen of dagelijks bestuur belast is met de uitvoering van de bovenlokale taken. De uitvoeringsorganisatie (UO) van de GRJR is ondergebracht bij de uitvoerende gemeente.
Derden:	anderen dan Partijen.
Medewerkers:	personen die werkzaam zijn voor Partijen, in dienstbetrekking dan wel tijdelijk ingehuurd.
Gegevens:	alle geleverde gegevens op casusniveau door gemeente of derden.
DPIA GRJR:	Data Protection Impact Assessment op de GRJR-gegevensverwerkingen betreffende de informatievoorziening.

1.3 Daar waar een definitie in enkelvoud wordt aangeduid, wordt tevens het meervoud bedoeld.

Artikel 2 – Totstandkoming en duur van de Overeenkomst

2.1 Deze Overeenkomst treedt in werking op het moment dat deze door Partijen is ondertekend en heeft een looptijd voor onbepaalde tijd.

Artikel 3 – Onderwerp van de Overeenkomst

3.1 Onderdeel van de gemeentelijke taakuitvoering vanuit de Jeugdwet betreft de informatievoorziening ten behoeve van het sturen op de jeugdhulp, jeugdbescherming, jeugdreclassering en Veilig Thuis. Er zijn

verschillende partijen betrokken bij de aanlevering van de informatie: 13 gemeenten, OLJR, gecontracteerde zorgaanbieders en ketenpartners. Dit zijn de leveranciers van gegevens aan het OLJR. De gegevens zelf worden met name op casusniveau verzameld, de informatievoorziening is op niveau contract/zorgaanbieder en zorglandschap. Om de jeugdhulp goed in beeld te brengen, is het nodig dat de gegevens per traject aan elkaar gekoppeld kunnen worden. Zo kunnen doorlooptijden en knelpunten in de jeugdhulpketen in beeld worden gebracht. Alle leveranciers ontvangen geaggregeerde rapportages terug via het dashboard.

- 3.2 Het OLJR en de bij de GRJR deelnemende gemeenten zijn gezamenlijk verwerkingsverantwoordelijk in de zin van artikel 26 AVG.
- 3.3 Deze Overeenkomst regelt de uniforme randvoorwaarden op het gebied van gegevensverwerking waaraan Partijen dienen te voldoen in het geval van de verwerking van persoonsgegevens.
- 3.4 Partijen houden zich bij het verwerken van persoonsgegevens aan alle toepasselijke wet- en regelgeving, waaronder de geldende wet- en regelgeving over de verwerking van persoonsgegevens.
- 3.5 Partijen verwerken niet meer persoonsgegevens dan strikt noodzakelijk is voor de doeleinden van de verwerking, zoals beschreven in Bijlage 2, en niet verder dan noodzakelijk is voor het kunnen uitvoeren van de Overeenkomst.

Artikel 4 – Algemene verplichtingen

- 4.1 In het kader van de Gemeenschappelijke Regeling Jeugdhulp Rijnmond verwerken partijen (persoons)gegevens. Dit betreft het verzamelen van, het ordenen/structureren, opslaan en combineren van (persoons)gegevens.
- 4.2 Partijen zullen de persoonsgegevens behoorlijk, zorgvuldig en in overeenstemming met de wet, waaronder begrepen maar niet uitsluitend, de AVG en aanverwante wet- en regelgeving, verwerken.
- 4.3 Partijen verwerken persoonsgegevens alleen op de wijze zoals overeengekomen in onderhavige Overeenkomst en zullen de persoonsgegevens niet op een andere manier verwerken, tenzij Partijen dit gezamenlijk nader overeenkomen.
- 4.4 Partijen zullen er zorg voor dragen dat uitsluitend die persoonsgegevens worden verstrekt die op grond van de geldende wet- en regelgeving mogen worden ontvangen. Partijen verstrekken enkel inhoudelijk juiste en volledige persoonsgegevens aan elkaar.
- 4.5 Partijen zullen de persoonsgegevens bewaren in overeenstemming met gemaakte afspraken en de geldende (wettelijke) bewaartermijnen.
- 4.6 Partijen die Derden inschakelen bij de verwerkingen doen dat onder eigen verantwoordelijkheid en aansprakelijkheid.
- 4.7 De verplichtingen die voortvloeien uit deze Overeenkomst, gelden ook voor degenen die onder het gezag van Partijen persoonsgegevens verwerken, zoals medewerkers van Derden.
- 4.8 Partijen zullen in overeenstemming met de geldende wet- en regelgeving technische en organisatorische maatregelen treffen, in stand houden en zo nodig aanpassen om een op het risico afgestemde beveiliging van de persoonsgegevens te waarborgen. Daarbij zal rekening worden gehouden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen.

Artikel 5– Geheimhouding

- 5.1 Partijen, personen in dienst van Partijen, organisaties en/of personen werkzaam ten behoeve van Partijen, hebben een geheimhoudingsplicht.
- 5.2 Deze geheimhoudingsplicht is niet van toepassing als (en voor zover) Partijen een wettelijke verplichting hebben om de informatie aan Derden te verstrekken.

Artikel 6 – Beveiliging

- 6.1 Partijen dragen zelf de zorg voor het nemen van voldoende en passende technische en organisatorische maatregelen om de persoonsgegevens te beveiligen tegen verlies, toegang door onbevoegden of tegen enige vorm van onrechtmatige verwerking met inachtneming van het bepaalde in artikel 32 AVG.
- 6.2 Naast de maatregelen genoemd in artikel 32 lid 1 AVG, nemen Partijen - waar passend – onder meer de volgende maatregelen:
 - a) een passend beleid voor de beveiliging van de verwerking van de persoonsgegevens;
 - b) maatregelen om te waarborgen dat enkel geautoriseerde medewerkers toegang hebben tot de persoonsgegevens die in het kader van de Overeenkomst worden verwerkt;
 - c) het regelen van procedures rondom het verlenen van toegang tot persoonsgegevens (waaronder een registratie- en afmeldprocedure voor toewijzing van toegangsrechten), en het in logbestanden vastleggen van gebeurtenissen betreffende gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen. Partijen maken nadere afspraken ten einde in de gelegenheid gesteld te worden om I logbestanden periodiek te controleren.
- 6.3 Partijen zullen de door haar getroffen beveiligingsmaatregelen periodiek evalueren en aanscherpen, aanvullen of verbeteren voor zover de eisen (of technologische) ontwikkelingen daartoe aanleiding geven.
- 6.4 In Bijlage 3 worden de afspraken tussen Partijen vastgelegd over de passende technische en organisatorische beveiligingsmaatregelen, alsmede over de inhoud, vorm en de werkwijze die Partijen verstrekken over de afgesproken beveiligingsmaatregelen.
- 6.5 Partijen zullen elkaar alle relevante informatie verschaffen die nodig is om de kwaliteit van de uitvoering van de Regeling en de naleving van de Overeenkomst te controleren.

Artikel 7 – Kennisgeving van beveiligingsincidenten en Inbreuken

- 7.1 In het geval van een (vermoeden van):
 - a) Een beveiligingsincident;
 - b) Een inbreuk in verband met persoonsgegevens die Partijen verwerken of door Derden laten verwerken, ten behoeve van de Overeenkomst, die (mogelijk) nadelige gevolgen heeft voor betrokkene(n) (hierna te noemen: incident), stellen Partijen elkaar uiterlijk binnen 24 uur na ontdekking van het incident op de hoogte, volgens, in overeenstemming met lid 4 van dit artikel.
- 7.2 De verantwoordelijkheid van Partijen voor het melden van een incident aan de Autoriteit Persoonsgegevens en/of de betrokkene is afhankelijk van het de verblijfplaats van de betrokkene. Wanneer de verblijfplaats van de betrokkene in het werkgebied van een Partij valt is deze Partij verantwoordelijk voor het melden van een incident conform artikel 33 en artikel 34 AVG.
- 7.3 Partijen sturen de benodigde informatie naar onder Bijlage 4 genoemd contactperso(o)n(en). Partijen garanderen dat de verstrekte informatie volledig, correct en accuraat is.
- 7.4 Elke Partij is verplicht om maatregelen te treffen die redelijkerwijs van hem kunnen worden verwacht om het incident zo snel mogelijk te herstellen dan wel de verdere gevolgen zoveel mogelijk te beperken.

Artikel 8 – Inschakelen Derden

- 8.1 Partijen zullen, behoudens enige wettelijke verplichting hiertoe, de persoonsgegevens uitsluitend aan Derden verstrekken voor de uitvoering van zijn taken zoals benoemd in de Overeenkomst.
- 8.2 Partijen zullen de persoonsgegevens in geen geval en op geen enkele wijze verstrekken aan Derden om commerciële redenen.
- 8.3 Indien een Partij bij de uitvoering van deze Overeenkomst gebruik maakt van Derden, dan maakt zij hiertoe afspraken met deze Derden. De afspraken dienen te voldoen aan de verplichtingen in de AVG en deze Overeenkomst. De Partij die een Derde inschakelt, staat in voor een correcte naleving van deze plichten.
- 8.4 Indien Partijen verplicht zijn op grond van een wettelijke verplichting persoonsgegevens te verstrekken, zal de Partij de ander terstond hieromtrent informeren, tenzij een wettelijk voorschrift dit verbiedt.

Artikel 9 – Doorgifte van persoonsgegevens buiten Europese Economische Ruimte (EER)

- 9.1 Partijen verwerken en slaan geen persoonsgegevens op buiten de Europese Economische Ruimte (EER), tenzij de andere Partijen daarvoor uitdrukkelijk en schriftelijk toestemming hebben gegeven.

Artikel 10 – Transparantie en omgang met rechten van betrokkenen

- 10.1 Partijen informeren de betrokkenen conform artikelen 12, 13 en 14 AVG omtrent alle gegevensverwerkingen die geschieden in het kader van de Regeling. Deze verplichting houdt onder meer in dat Partijen de vereiste informatie op een gemakkelijk toegankelijke wijze aan betrokkenen kenbaar maken, bijvoorbeeld door het beschikbaar stellen van een privacyverklaring of enig ander (digitaal) document.
- 10.2 De verantwoordelijkheid voor het afhandelen van verzoeken van betrokkenen ingevolge artikel 15 tot en met 22 AVG j.o 12 AVG is afhankelijk van het de verblijfplaats van de betrokkene. Als de verblijfplaats van de betrokkene in het werkgebied van een Partij valt is deze Partij verantwoordelijk voor het afhandelen van een dergelijk verzoek. Partijen kunnen nader schriftelijk afspraken maken met betrekking tot de praktische uitvoering van deze verzoeken.
- 10.3 Partij waarbij het verzoek binnenkomt is ook verantwoordelijk voor het melden van dit verzoek bij overige betrokken Partijen, zodat ook deze Partijen gevolg kunnen geven aan dit verzoek.
- 10.4 Indien een Partij een verzoek van een betrokkene ter uitoefening van zijn of haar rechten ontvangt dat niet onder haar verantwoordelijkheid valt, dan zal deze Partij het verzoek onmiddellijk doorsturen naar de verantwoordelijke Partij, onder vermelding van voldoende informatie op basis waarvan contact kan worden opgenomen met de betrokkene.
- 10.5 In geval van een verzoek van een betrokkene, zullen Partijen elkaar over en weer alle medewerking verlenen die redelijkerwijze noodzakelijk is om binnen de wettelijke termijnen te voldoen aan de verplichtingen met betrekking tot de uitoefening van de rechten van betrokkenen op basis van de AVG.

Artikel 11 – Het verlenen van bijstand en medewerking

- 11.1 Partijen verlenen bijstand bij het doen nakomen van de rustende verplichtingen op grond van de AVG en ander toepasselijke wet- en regelgeving over de verwerking van persoonsgegevens, zoals:
- a) het vervullen van de plicht om aan verzoeken van de in AVG vastgelegde rechten van de betrokkene binnen de wettelijke termijnen te voldoen, zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens;
 - b) het uitvoeren van controles en audits zoals bedoeld in artikel 6 van deze Overeenkomst;
 - c) het uitvoeren van een gegevensbeschermingseffectbeoordeling (PIA of DPIA) en een eventuele daaruit voortvloeiende verplichte voorafgaande raadpleging van de Autoriteit Persoonsgegevens;
 - d) het voldoen aan verzoeken van de Autoriteit Persoonsgegevens of een Functionaris voor Gegevensbescherming;
 - e) het voorbereiden, beoordelen en melden van incidenten zoals in artikel 7 van deze Overeenkomst.
- 11.2 Een verzoek of onderzoek van de Autoriteit Persoonsgegevens dan wel van de Functionaris voor Gegevensbescherming met betrekking tot de verwerking van de persoonsgegevens, wordt door de Partijen, voor zover wettelijk is toegestaan, onverwijld doorgestuurd naar de Partij, die verantwoordelijk is voor de afhandeling van het verzoek of onderzoek.
- 11.3 Partijen brengen elkaar geen kosten in rekening, zolang de bijstand in alle redelijkheid is verleend.

Artikel 12 – Aansprakelijkheid

- 12.1 In het geval een Partij aansprakelijk is, zal de aansprakelijke Partij verplicht zijn de schade te vergoeden conform het bepaalde in titel I afdeling 10 Boek 6 BW en artikel 82 AVG. Eventuele aan een Partij opgelegde boetes door toezichthouders in verband met een tekortkoming in de nakoming van één of meer verplichtingen van een andere Partij onder de Overeenkomst of toepasselijke wetgeving kunnen eveneens conform artikel 82 AVG naar rato worden verhaald op de andere Partij.

12.2 Partijen vrijwaren elkaar en stellen elkaar schadeloos ter zake van alle schade, inclusief opgelegde boetes door toezichthouders, in verband met een tekortkoming in de nakoming van deze verplichting of één of meer verplichtingen van een Partij uit hoofde van toepasselijke wetgeving en de Overeenkomst.

Artikel 13 – Beëindiging van de Overeenkomst

13.1 Deze Overeenkomst kan worden opgezegd door middel van een schriftelijk besluit tot opzegging namens de betreffende Partij.

13.2 Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van deze Overeenkomst voort te duren, blijven ook na beëindiging gelden. Tot deze bepalingen behoren onder meer, doch niet uitsluitend, artikel 5 (Geheimhouding) en artikel 12 (Aansprakelijkheid).

13.3 Partijen dienen nadere afspraken te maken voor de verplichtingen die na beëindiging voortduren. Deze te maken afspraken vloeien voort uit artikel 12 lid 1 AVG en dienen in elk geval de volgende onderwerpen te regelen:

- a) over de wijze waarop en binnen welke termijn de geleverde persoonsgegevens worden vernietigd;
- b) bewaartermijnen;
- c) wijze van overdracht.

Artikel 14 – Toepasselijk recht en forumkeuze

14.1 Op deze Overeenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is uitsluitend Nederlands recht van toepassing.

14.2 Alle geschillen die ontstaan naar aanleiding van deze Overeenkomst worden beslecht op dezelfde wijze zoals uiteengezet in de Regeling.

Artikel 15 – Slotbepalingen

15.1 Indien één of meer bepalingen van deze Overeenkomst niet rechtsgeldig blijkt te zijn, zal de Overeenkomst voor het overige van kracht blijven. Partijen zullen in overleg treden over de bepalingen die niet rechtsgeldig zijn en zullen deze, voor zover mogelijk, vervangen door een bepaling die wel rechtsgeldig is en zoveel mogelijk aansluit bij de strekking van de te vervangen bepaling.

15.2 In geval van wijzigingen in de dienstverlening, de toepasselijke wet- of regelgeving of andere relevante omstandigheden die van invloed zijn op de Gegevensverwerkingen, zullen Partijen in overleg treden over een eventueel benodigde wijziging van deze Overeenkomst.

15.3 Wijzigingen kunnen uitsluitend schriftelijk door de Partijen onderling worden overeengekomen.

D. ONDERTEKENING

Aldus overeengekomen en in meervoud ondertekend,

Rotterdam 2023

Het algemeen bestuur van het Openbaar Lichaam Jeugdhulp Rijnmond,
namens deze:

.....

.....

R. Buijt
Voorzitter

S. Hammer

Secretaris-Directeur

en

Het college van B en W van de gemeente Rotterdam,
namens deze:

.....

E.Hadziavdic
Concerndirecteur Maatschappelijke Ontwikkeling

en

Het college van B en W van de gemeente,
namens deze:

.....

(naam)
Directeur

BIJLAGE 1 BIJ DE OVEREENKOMST GEZAMENLIJKE VERWERKINGSVERANTWOORDELIJKEN

De aard en omvang van een Opdracht

Doel van de verwerking

Het openbaar lichaam Jeugdhulp Rijnmond is een verband van samenwerkende gemeenten in het kader van de gemeenschappelijke regeling Jeugdhulp Rijnmond. De samenwerking betreft het uitvoeren van de bovenlokale taken door middel van onder andere het contracteren van specialistische jeugdhulp. Om te kunnen sturen op passende jeugdhulp heeft het OLJR ook een informatievoorzieningstaak. Om zicht te krijgen op contractafspraken over ingezette hulp, kosten en het zorglandschap leveren gemeenten, zorgaanbieders en ketenpartners gegevens aan over het zorggebruik op casusniveau. Deze gegevens worden verwerkt tot informatie over de ingekochte/gesubsidieerde hulp en getoond in een dashboard. Rapportage hiervan gebeurt altijd op geaggregeerd niveau, waarbij er voor gezorgd wordt dat informatie nooit herleidbaar is tot één kind of jeugdige. Enkel in de gevallen dat het dit nodig voor controle van de rechtmatigheid of met het oog op verbeteringen in de datakwaliteit en de aansluiting van administraties, worden gegevens op casusniveau verstrekt aan gemeenten. Contractmanagers van de uitvoeringsorganisatie, gemeenten, zorgaanbieders en ketenpartners gebruiken deze informatie in de sturing op passende jeugdhulp.

Aanlevering

Gegevens worden door gemeenten aan de UO GRJR verstrekt volgens de afgesproken termijnen zoals genoemd in het Administratieprotocol GRJR (dit protocol wordt periodiek aangepast en vastgesteld door gemeenten. De meest recente versie is te vinden de website www.jeugdhulprijnmond.nl). De gegevens worden volgens het door de UO verstrekte format aangeleverd in het Mendix portaal (Betaaltool Zorg; BTZ). Iedere gemeente heeft tenminste één medewerker die geautoriseerd is om de gevraagde gegevens aan te leveren.

De gegevens van gemeenten worden door gemeenten aan de UO verstrekt via de BTZ:

- Gemeenten doen maandelijks of frequenter een upload van deze gegevens in het voorportaal van Mendix (de BTZ)
- Tijdens de upload wordt binnen het low-code platform Mendix de data direct automatisch gepseudonimiseerd en worden de originele BSN's verwijderd. De versleuteling die gebruikt wordt is één-richting (*one-way encryption*), wat betekent dat het gebruikte gepseudonimiseerde BSN niet terug herleidbaar is naar het originele BSN. Het betreft hier een standaard SHA512 hash, waarbij de BSN wordt voorzien van een pre-sleutel voor extra veiligheid. De gebruikte pre-sleutel is vastgelegd bij wijzigingsbeheer.
- Na validatie door gebruiker worden de gegevens doorgezet naar de Mendix database.
- De UO ontvangt de gegevens enkel met gehasht BSN in de Mendix database
- Daarna voert de beheerder enkele bestandscontroles uit op de volledigheid van de aangeleverde gegevens. Indien niet akkoord dient de aanleverende partij een verbeterd bestand aan te leveren.

Toegang en autorisatie

Gemeenten hebben zowel toegang tot het Mendix portaal (BTZ) voor de upload van gegevens als tot de dashboards GRJR. Door de UO wordt periodiek gecontroleerd of de opgegeven gebruikers nog steeds toegang moeten hebben tot deze applicaties. Het is aan de gemeenten om wijzigingen in autorisaties door te geven aan de UO .

Kwaliteitscontrole gegevens

Gemeenten dragen zorg voor gegevens die tijdig, juist en compleet worden aangeleverd. Kader voor tijdige, juiste en complete gegevens zijn te vinden in het Administratieprotocol GRJR (zie www.jeugdhulprijnmond.nl). De UO draagt zorg voor rapportages over de kwaliteit van deze gegevens via de met gemeenten gedeelde dashboards.

Opslag

Gegevens worden opgeslagen in het voorportaal van Mendix, de database van Mendix en het DWH Rotterdam. Daarnaast vinden er (incidentele) verwerkingen plaats in Excel. Bestanden worden hiervoor opgeslagen in één afgeschermd map in het bewaarsysteem DIVA. Voor de opslag door de UO van gegevens gelden de volgende bewaartermijnen:

- Vijf jaar: cat. 19.1 van de VNG selectielijst voor gemeenten en intergemeentelijke organen 2020 - niet financiële informatie (tzt gegevens lokale teams)
- Zeven jaar: cat. 19.1.1 van de VNG selectielijst voor gemeenten en intergemeentelijke organen 2020 - financiële informatie (toewijzingen en declaraties)

Verwerking

- Vanuit de Mendix database worden de gepseudonimiseerde data doorgevoerd naar het DWH van de gemeente Rotterdam;
- In het DWH worden de gegevens opgeslagen
- Een eerste verwerking van de gegevens vindt plaats in het DWH. Hierin wordt algemene logica toegepast, d.w.z. bewerkingen die voor iedere volgende analyse gelden.
- Microsoft PowerBI maakt connectie met het Datawarehouse om de gegevens uit het DWH in PowerBI in te laden. Uit te voeren maatregel: sluiten van verwerkersovereenkomst met OBI en gebruikersovereenkomst per informatieproduct. Maatregel is opgenomen in maatregelenoverzicht.
- De gegevens worden vervolgens bewerkt tot rapportages en ontsloten via PowerBI of Excel. Hieruit volgen rapportages:
 - o Op geaggregeerd niveau
 - o Op regelniveau t.b.v. administratieve aansluiting (rechtmatigheid)

Er zijn geen fysieke documenten met persoonsgegevens. Er worden wel persoonsgegevens gedeeld per beveiligde mail of dashboard t.b.v. de administratieve aansluiting tussen gemeenten en zorgaanbieders. Vanwege de rechtmatigheid en om te kunnen sturen op de datakwaliteit is deze terugkoppeling noodzakelijk. Daarom wordt aan gemeenten teruggekoppeld waar er wel en geen aansluiting is te vinden op niveau van de toewijzing. De BSN wordt hierbij niet gedeeld (deze is namelijk onomkeerbaar gehasht). Hiertoe worden slechts persoonsgegevens gedeeld met gemeenten van jeugdigen uit de betreffende gemeente, die uiteindelijk in de cliëntadministratie van gemeenten moeten worden ingevoerd. Het gaat dus in alle gevallen om persoonsgegevens die:

1. Bij gemeenten bekend zijn, of;
2. Mogelijk bij gemeenten in de cliëntadministratie opgenomen moeten worden (en daarmee al bekend hadden moeten zijn)

Het is de verantwoordelijkheid van gemeenten om de gegevens die zij ontvangen over de eigen jeugdigen zorgvuldig te verwerken.

Verwijderen

Een individuele jeugdige kan uit de gegevensset verwijderd worden. Hiertoe dient een jeugdige (e/o diens ouders/verzorgers) een verzoek in te dienen bij de gemeente. De gemeente is verantwoordelijk

voor het omzetten van de toewijzing naar een toewijzing waaruit niet op te maken valt welke hulp het betreft, de zogenaamde opt-out regeling. Daarmee worden eerdere regels overschreven bij een nieuwe upload van gegevens bij de UO GRJR (in Mendix; BTZ). De regel blijft wel inzichtelijk, anders kan er niet betaald worden. De regel levert echter geen informatie op over de ontvangen hulp. Andere mogelijkheid: opvoeren BSN in BTZ en hierna o.b.v. de ontstane hash de regels die betrekking hebben op deze jeugdige verwijderen uit de datasets.

Bijlage 2 bij de Overeenkomst

Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen

Hieronder staan de grondslag voor de totale verwerking en de verwerkingsdoelen per aangeleverd gegeven toegelicht.

Grondslag voor verwerking

Voor een verwerking van persoonsgegevens vereist de Algemene Verordening Gegevensbescherming (AVG) een wettelijke grondslag om te spreken van een rechtmatige verwerking.

In dit geval vloeit deze grondslag voort uit art. 7.4.1 lid 2 Jeugdwet:

“Het college verwerkt gegevens ten behoeve van een doelmatig, doeltreffend en samenhangend gemeentelijk beleid ten aanzien van preventie, de toegang tot en verlening van jeugdhulp, de uitvoering van kinderschermingsmaatregelen en jeugdreclassering en het advies- en meldpunt huiselijk geweld en kindermishandeling, alsmede ten behoeve van de verwerking, bedoeld in het eerste lid.”

In samenhang met de artikelen 7.4.3 jo 7.4.4. lid 1 Jeugdwet geeft dit de mogelijkheid om gegevens aangeleverd door Jeugdhulpaanbieders, gemeenten en ketenpartners verder te verwerken om te onderzoeken of het gemeentelijk beleid doelmatig en doeltreffend is, hetgeen het doel is van de verwerking. In het navolgende wordt deze grondslag verder uitgewerkt.

In Tabel 1 wordt beschreven op welke wijze de verschillende informatie wordt aangeleverd, opgeslagen en verwerkt. In tabel 2 staan de verwerkingsdoelen per uitgevraagd veld toegelicht. In tabel 3 staan de inschakelde verwerkers toegelicht. Ook is de ICT-architectuur inzichtelijk gemaakt in figuur 1.

Tabel 1. Aanlevering gegevens*

Gegevens	Via	Leverende partij	Opslag	Verwerking
Declaraties	BTZ	Gemeenten	Mendix/DWH/DIVA	PowerBI/Excel
Toewijzingen	BTZ	Gemeenten	Mendix/DWH/DIVA	PowerBI/Excel
Optioneel: tzt lokale teams	BTZ (tzt)	Gemeenten	Mendix/DWH	tzt PowerBI

*Voor de MVS-gemeenten geldt deze levering uitsluitend voor de periode dat en ingekochte zorg/hulp waaraan zij regionaal nog deelnemen.

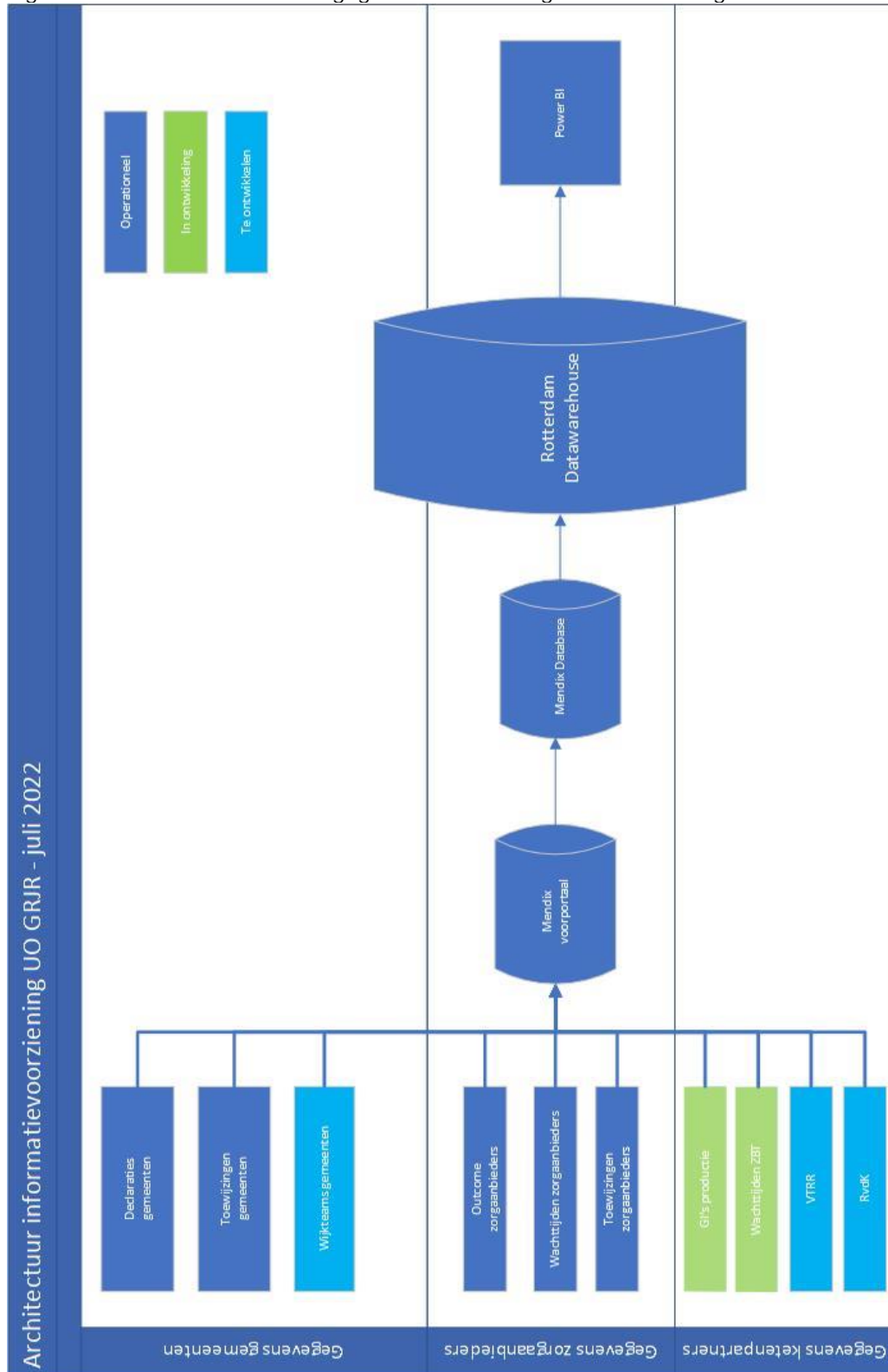
Tabel 2. Verwerkingsdoelen aangeleverde gegevens

Gehasht BSN	Financiële informatie, procesanalyse, datakwaliteit
Postcode4 client	Financiële informatie, procesanalyse, datakwaliteit
Geboortejaar	Beleidsanalyse, datakwaliteit
Gemeente(code)	Betaling, financiële informatie, procesanalyse, datakwaliteit
Beschikkingnummer	Betaling, financiële informatie, procesanalyse, datakwaliteit
Toewijzingnummer	Betaling, financiële informatie, procesanalyse, datakwaliteit
AGB-code/lokaal team/partnercode	Betaling, financiële informatie, procesanalyse, datakwaliteit
Productcode	Financiële informatie, procesanalyse, datakwaliteit
Toegekend weekbudget in €	Financiële informatie, procesanalyse, datakwaliteit
Ingangsdatum toewijzing (uit iJW301)	Financiële informatie, procesanalyse, datakwaliteit
Einddatum toewijzing (uit iJW301)	Financiële informatie, procesanalyse, datakwaliteit
Begindatum Zorg (uit iJW305) / datum aanvang	Financiële informatie, procesanalyse, datakwaliteit
Einddatum Zorg (uit iJW307) / datum einde	Financiële informatie, procesanalyse, datakwaliteit
Verwijzer	Financiële informatie, procesanalyse, datakwaliteit
Reden beëindiging jeugdhulp	Procesanalyse
Alle overige regels iJW berichtenverkeer	Financiële informatie, procesanalyse, datakwaliteit

Tabel 3. Ingeschakelde verwerkers door Partijen

Naam Systeem	Verwerker	Specificatie verwerking
BTZ	UO	Opslaan, bewerken en doorsturen van gegevens, o.a. ten behoeve van waarborgen datakwaliteit
DWH	Gemeente Rotterdam, afd. OBI	Opslaan en eerste bewerking
PowerBI	Gemeente Rotterdam, afd. OBI	Bewerking en rapportage gegevens

Figuur 1. ICT-architectuur van gegevensaanlevering en - verwerking



Bijlage 3 bij de Overeenkomst

Overzicht van de te nemen passende technische en organisatorische maatregelen

Conform artikel 6 van deze Overeenkomst dienen Partijen in ieder geval de volgende maatregelen te nemen:

Authenticatie	Er is voor toegang tot persoonsgegevens een authenticatiemiddel gebruikt dat passend is (zoals wachtwoorden, smartcards, tokens of digitale certificaten). Partijen dragen zorg voor een veilige wijze van beheer van deze middelen en een veilige wijze van verstrekking van deze middelen aan Medewerkers/Derden.
Autorisaties	Partijen houden een actuele lijst bij van geautoriseerd personeel en zorgen dat deze lijst zo beperkt mogelijk is. Deze lijst wordt op verzoek van een Partij getoond. Autorisaties zijn persoonsgebonden en worden door verwerker periodiek gecontroleerd op juistheid en volledigheid volgens een gedocumenteerd proces.
Back-ups	Van de persoonsgegevens wordt tenminste dagelijks een back-up gemaakt om te verzekeren dat het eventuele verlies van persoonsgegevens niet meer dan 1 dag bedraagt. De back-ups worden op een veilige plaats bewaard, beschermd tegen toegang door onbevoegden en periodiek getoetst door de verwerker op juiste werking.
Beveiligingsbeleid	Partijen beschikken over een actueel en door hoger management goedgekeurd (informatie)beveiligingsbeleid.
Calamiteiten	Partijen zorgen dat zij voldoende zijn voorbereid op calamiteiten. Hierbij kan gedacht worden aan het gebruik van uitwijklocaties, crisisorganisatie, uitwijkdraiboeken en het uitvoeren van uitwijktesten.
Inbreuk	Partijen zullen elkaar onverwijld op de hoogte brengen van iedere inbreuk in verband met persoonsgegevens. Informatie over de Inbreuk (bijvoorbeeld bewijsmateriaal) wordt door de Partijen adequaat gedocumenteerd en bewaard.
Logging en monitoring	Partijen zorgen voor passende logging van toegang tot de persoonsgegevens.
Malware	Partijen nemen adequate maatregelen tegen malware en andere schadelijke software (bijvoorbeeld door het gebruik van firewalls en antivirussoftware).
Screening en geheimhouding	Partijen beheersen de risico's aangaande eigen medewerkers door middel van toereikende geheimhoudingsverklaringen en screening.
Toegangsbeveiliging	Partijen treffen voorzieningen voor adequate fysieke en logische toegangsbeveiliging tot de verwerkte persoonsgegevens en de ruimtes waarin deze gegevens zijn opgeslagen of worden Verwerkt (en tijdens transport).
Updates en patches	Partijen waarborgen dat de voor de verwerking benodigde software en systemen beschikken over de laatste updates en patches (patch management).
Versleuteling	Partijen waarborgen dat er deugdelijke versleuteling ('encryptie') wordt toegepast bij de opslag en/of verzending van persoonsgegevens om te waarborgen dat alleen geautoriseerde personen toegang hebben tot de persoonsgegevens. Partijen dragen zorg voor adequate beveiliging van sleutel materiaal zoals (wachtwoorden en encryptiesleutels).
Wachtwoordbeleid	Partijen hebben een adequaat wachtwoordbeleid waarin de eisen aan wachtwoorden staan beschreven. Deze eisen worden ook voor Verwerkers afgedwongen in de betreffende systemen voor allen met toegang tot de persoonsgegevens.

Bijlage 4 bij de Overeenkomst
Overzicht van Contactgegevens van Partijen

Namens

Contactpersoon	
Naam	
E-mail	
Telefoonnummer	
Functionaris voor de Gegevensbescherming	
Naam	
E-mail	
Telefoonnummer	

Namens

Contactpersoon	
Naam	
E-mail	
Telefoonnummer	
Functionaris voor de Gegevensbescherming	
Naam	
E-mail	
Telefoonnummer	

Namens

Contactpersoon	
Naam	
E-mail	
Telefoonnummer	
Functionaris voor de Gegevensbescherming	
Naam	
E-mail	