NET2LEGAL CONSULTANTS

Privacy Impact Assessment (PIA) deelproject Justitiële Keteninformatisering

'Risico's en Privacy by Design bij de justitiële ketenberichten voor de Jeugdwet'

Opdrachtgevers:
Ministerie van VWS, Directie Jeugd
Ministerie van VenJ, Directie Justitieel Jeugdbeleid

Uitgebracht ten behoeve van:
Deelproject Justitiële Keteninformatisering
Project Beleidsinformatie Stelselherziening Jeugd

Uitgebracht door:
Net2Legal Consultants

Versie: 1.0
5 november 2014

Inhoudsopgave

Uitvoering en versiebeheer

De PIA voor het deelproject data en systematiek beleidsinformatie jeugd is uitgevoerd door Net2Legal Consultants in de periode 15 mei 2014 tot 15 oktober 2014.

Deze PIA is een tweede uit een reeks van drie PIA's die in het kader van het *Project Beleidsinformatie Stelselherziening Jeugd* uitgevoerd worden. Een eerste PIA over de eenmalige gegevensoverdracht bij de transitie naar de Jeugdwet is bij Brief van 13 december 2013 aan de Eerste en Tweede Kamer gezonden (TK 31 839, nr. 334).

Bij de PIA is gebruik gemaakt van enkele relevante onderdelen uit het *Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst* van 24 juni 2013 (Bijlage bij TK, 26 643, nr. 282). Het Toetsmodel dient vanaf 1 september 2013 standaard te worden toegepast bij ontwikkeling van nieuwe wetgeving en beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien. Zie voor het Toetsmodel ook Bijlage 3.

De PIA is uitgevoerd overeenkomstig de door Net2Legal en PBLQ ontwikkelde flexibele methodiek http://www.pblq.nl/themas/privacy/privacy-impact-assesment

De PIA is samengesteld op basis van de in Bijlage 1 vermelde basisdocumenten, de ter beschikking gestelde projectdocumentatie en op basis van de eerdere project-advisering. De opsteller van deze PIA-rapportage is sinds februari 2013 als adviseur voor privacy-onderwerpen verbonden aan het Project Beleidsinformatie Stelselherziening Jeugd.

Op de eerste conceptversie (0.1) is commentaar gegeven door de leden van het deelproject. Andere conceptversies (0.2 en 0.9) zijn van commentaar voorzien door de leden van het deelproject, de FG van VenJ, de auditor van het deelproject, de beleidsdirectie betreffende jeugd van VenJ, de RvdK en het CJIB.

Een PIA is geen eindstation of einddocument. Aanpassing of aanvulling van een PIA is nodig als het onderwerp (object) van de PIA een nieuwe fase bereikt. Voor wat de Justitiële Keteninformatisering betreft, kan dit het geval zijn als in de toekomst nieuwe berichten toegevoegd worden die via de (nieuw) ontwikkelde berichten infrastructuur CORV verzonden worden.

Versiebeheer

Versie	Datum	Status	Auteur	Omschrijving
0.1	16-06-2013	Concept	Net2Legal mr. dr. E. Schreuders	Concept voor commentaar door de projectleiding
0.2	15-07-2014	Concept	Net2Legal mr. dr. E. Schreuders	Aanvulling met opmerkingen en commentaar. Concept voor commentaar door projectleiding, Functionaris gegevensbescherming VenJ En betrokken partijen
0.9	15-08-2014	Concept	Net2Legal mr. dr. E. Schreuders	Aanvulling met opmerkingen en commentaar. Toevoeging Bijlage 3.
1.0	05-11-2014	Definitief	Net2Legal mr. dr. E. Schreuders	Opmerkingen verwerkt. Eindversie

DEEL I SAMENVATTING EN ACHTERGROND

1 Samenvatting, risico beoordeling, bevindingen en aanbevelingen

1.1 De Jeugdwet en justitiële keteninformatisering

De nieuwe Jeugdwet zal, zo is voorzien, per 1 januari 2015 in werking treden. Het voornaamste doel van de Jeugdwet is dat alle kinderen gezond en veilig opgroeien, hun talenten ontwikkelen en meedoen in de samenleving naar vermogen. Het gaat daarbij om preventie en uitgaan van eigen kracht van jeugdigen, ouders en het sociale netwerk het minder snel medicaliseren, meer ontzorgen en normaliseren, eerder (jeugd)hulp op maat voor kwetsbare kinderen, integrale hulp met betere samenwerking rond gezinnen en meer ruimte voor jeugdprofessionals en vermindering van regeldruk.

De Jeugdwet brengt door de nieuwe rol van gemeenten en de AMHK's veranderingen met zich mee bij de verantwoordelijkheden in de beschermings- en jeugdstrafrechtketen. Justitiële organisaties, gemeenten en private partijen dienen nauw samen te werken om de doelstellingen van een effectiever, efficiënter en een financieel eenvoudiger jeugdzorgstelsel te bewerkstelligen. In het nieuwe jeugdstelsel krijgen gemeenten en justitiële organisaties andere verantwoordelijkheden bij de uitvoering van de jeugdbescherming en jeugdreclassering (het gedwongen kader). Efficiënte en effectieve informatie-uitwisseling tussen betrokken partijen is daarbij cruciaal voor een goede uitvoering van de Jeugdwet. Deze PIA ziet voor wat de informatie-uitwisseling betreft op de justitiële keteninformatisering.

1.2 De onderwerpen van de PIA

Een PIA toetst, kort gezegd, **óf** de voorziene gegevensverwerking inderdaad doorgang dient te vinden, **welke** gegevensverwerkingen dan noodzakelijk zijn en vervolgens **hoe** deze gegevensverwerkingen plaats mogen vinden. In deze PIA staan **de risico's** bij justitiële keteninformatisering en de daarbij behorende berichten centraal.

In deze PIA staan de taken en werkzaamheden van het deelproject justitiële keteninformatisering centraal. Daarbij gaat het als eerste om de (nieuwe) justitiële ketenberichten die ter uitvoering van de Jeugdwet met behulp van een nieuwe berichteninfrastructuur tussen de gebruikers verzonden worden. Het zijn berichten tussen het gemeentelijk domein, het justitieel domein en gecertificeerde instellingen over jeugdbescherming, jeugdreclassering en meldingen door de politie. Dit is een meer regelgevende insteek van de PIA. Als tweede gaat het om de nieuwe berichteninfrastructuur: de Collectieve Opdracht Routeer Voorziening (CORV). De CORV is een digitaal knooppunt dat zorgt voor de elektronische afhandeling van het formele berichtenverkeer (de justitiële ketenberichten) tussen justitiepartijen en het gemeentelijke domein. Hierbij gaat het vooral om een ICT aspect waarbij informatiebeveiliging voorop staat. Als derde komt ook kort de inbedding van de justitiële keteninformatisering in de informatiehuishouding van de gebruikers aan de orde.

1.3 De Privacy-risico's bij keteninformatisering en berichtenverkeer

De verwerking van persoonsgegevens bij de Jeugdwet, bij keteninformatisering en bij de tussen ketenpartijen te verstrekken informatie (berichten) vereist aandacht. Er zijn risico's aan verbonden. Het algemene risico in verband met privacy en de verwerking van persoonsgegevens bij berichten en berichten infrastructuren is een onrechtmatige verspreiding van gegevens. Bij deze verspreiding zijn er drie aspecten:

- de niet toegestane verstrekking van gegevens als gegevens niet aan de ontvanger verstrekt mogen worden, bijvoorbeeld als er een specifieke geheimhoudingsverplichting is, of als de gegevens niet noodzakelijk zijn voor de ontvanger. Dit ziet op de inhoud van de berichten;
- de niet toegestane verstrekking van gegevens als de berichten niet bij de juiste ontvanger bezorgd worden. Dit ziet in het bijzonder op de werking van de berichten infrastructuur en de wijze waarop berichten geadresseerd worden;
- een onvoldoende informatiebeveiliging waardoor de gegevens (te) kwetsbaar worden voor bijvoorbeeld verlies of diefstal.

Het *PIA toetsmodel* voor de justitiële keteninformatisering, bestaat uit de volgende onderdelen.

Een onderdeel over de berichten, bestaande uit:
- de positionering van de gegevensuitwisseling bij samenwerking;
- de zeggenschap over de berichten en de inhoud;
- de rechtvaardiging van de berichten en de inhoud.

Een onderdeel over de centrale berichteninfrastructuur (CORV), bestaande uit:
- de werking en functies van de berichteninfrastructuur;
- de beheersbaarheid van de berichten infrastructuur.

Een onderdeel over de inbedding in de informatiehuishouding van verzenders en ontvangers van berichten, bestaande uit:
- aandachtspunten voor gebruikers in verband met aansluiting op de CORV;
- elementen die bij aansluiting een rol kunnen spelen.

1.4 De algemene observatie van de PIA

De algemene observatie van de PIA valt positief uit voor het thans gekozen opzet en inrichting van de justitiële ketenberichten bij de uitvoering van de Jeugdwet en de CORV. Deze observatie ziet op de thans ontwikkelde berichten en de CORV. De PIA kan ook gebruikt worden voor de berichten die ook in en na 2015 nog toegevoegd zullen worden om met de CORV te verzenden.

Algemene observatie PIA

Het Deelproject justitiële keteninformatisering heeft bepaald veel werk verricht in het kader van een zorgvuldige opzet en werking van de berichten en de CORV. Daarbij zijn maatregelen getroffen om de risico's:

- op niet toegestane verstrekking van gegevens in verband met specifieke geheimhoudingsverplichtingen en de noodzakelijkheid van de door ontvangers te ontvangen gegevens (doelbinding);
- betreffende een juiste en zorgvuldige bezorging van de berichten en de wijze waarop berichten geadresseerd worden, en
- in verband met informatiebeveiliging,

zoveel mogelijk te beperken.

De inspanning om de risico's zoveel mogelijk te beperken betreffen vooral:

- de keuze om de nieuw in te richten berichten infrastructuur strikt te beperken tot een op maat ontwikkelde routeringsvoorziening;
- reeds bij de ontwikkeling nadrukkelijk en ook vanuit privacy oogpunt aandacht te besteden aan het toekomstig beheer, en
- het ontwikkelen van de inhoud van de berichten in samenspraak met de betrokken partijen, waaruit duidelijk blijkt dat beperking van de te verstrekken gegevens tot de noodzakelijke gegevens en een goede wettelijke onderbouwing van de berichten en hun inhoud leidend geweest zijn.

Daarnaast heeft het Deelproject justitiële ketensamenwerking in samenspraak met o.a. de VNG en veldpartijen ook ruim aandacht besteed aan de risico's en privacy aspecten die betrekking hebben op het aansluiten op de CORV en waarbij de te nemen maatregelen behoren tot de verantwoordelijkheid van de aansluitende partijen.

Het zijn deze inspanningen die ertoe geleid hebben dat er zowel technisch, organisatorisch als inhoudelijk sprake is van privacy by design.

De twee aanbevelingen die gedaan worden zien dan ook meer op ondersteuning van en nader richting geven voor de werkzaamheden van het Deelproject justitiële keteninformatisering, dan dat ze betrekking (zouden) hebben op onderwerpen die nog niet of nog niet voldoende onderkend zouden zijn.

1.5 Risico-beoordeling, bevindingen en aanbevelingen

In deel II van de PIA is de risicobeoordeling opgenomen over de berichten, de berichteninfrastructuur en de inbedding in de informatiehuishouding van de verzenders en ontvangers van berichten. Tevens worden in de PIA diverse bevindingen en een tweetal aanbevelingen vermeld.

Op enkele plaatsen wordt verwezen naar een ministeriële regeling op basis van artikel 7.3.11, lid 4, van de Jeugdwet (dit lid 4 zal bij aanname van de Invoeringswet Jeugdwet vernummerd worden tot het vijfde lid. In deze PIA zal (nog) gesproken worden over het vierde lid). In die regeling zullen zowel berichten, de CORV als het gebruik van de CORV nader geregeld worden.

2 Privacy Impact Assessments

2.1 Een omschrijving van de PIA

Een PIA kan worden omschreven als een hulpmiddel bij het inschatten van privacy risico's bij wetgeving en bij ICT- projecten. Een PIA dient om tijdig inzicht te krijgen wat de gevolgen en risico's van wetgeving, een project of activiteit kunnen zijn, vooral voor wat betreft inbreuken op de persoonlijke levenssfeer. Daarbij worden ook aanbevelingen meegenomen voor het treffen van maatregelen om de geconstateerde risico's af te wenden. Met de aanbevelingen en maatregelen richt de PIA zich ook op privacy-beleid. Uiteindelijk moet de PIA inzicht geven in hoeverre en onder welke voorwaarden het project, eventueel met aanvullende maatregelen, doorgang kan vinden. Een PIA draagt daarmee bij aan het vermijden of verminderen van privacy risico's. Een impact assessment (effectbeoordeling) wordt door de International Association for Impact Assessment (IAIA) wat formeel omschreven als "de identificatie van toekomstige gevolgen van een huidige of voorgestelde actie".
Naast de mogelijkheid om een PIA te voeren, zijn er diverse andere privacy hulpmiddelen beschikbaar om de privacyaspecten van gegevensverwerkingen te beoordelen. Veel van deze middelen zijn direct op de toetsing van de naleving van de wettelijke eisen gericht.
Een PIA verschilt van deze hulpmiddelen omdat het zich niet beperkt tot de vraag of de activiteiten en verwerkingen bij wet zijn toegestaan, maar ook hoe het vraagstuk bijvoorbeeld maatschappelijk wordt ervaren. Het beperkt zich daarbij niet alleen tot dataprotectie wet en regelgeving, maar richt zich ook breder op percepties van privacy, en de uitgangspunten van dataprotectie. Een PIA richt zich ook op de vraag of de organisatie in staat is om eventuele tekortkomingen te signaleren, en er bereidheid is om de maatregelen te treffen die het risico kunnen afwenden ('in control').

Een PIA toetst, kort gezegd, **óf** de voorziene gegevensverwerking inderdaad doorgang dient te vinden, **welke** gegevensverwerkingen dan noodzakelijk zijn en vervolgens **hoe** deze gegevensverwerkingen plaats mogen vinden.

Een PIA kan op verschillende momenten uitgevoerd worden. Bijvoorbeeld voorafgaande aan het treffen van regelgeving, voorafgaande aan de ontwikkeling van ICT-projecten of op het moment dat regelgeving of ICT-projecten een nieuwe fase in gaan. In bepaalde gevallen kan een PIA de nadruk hebben op privacy by design, in nadere gevallen kan er meer nadruk zijn op compliance-achtige aspecten. Het onderscheid tussen een vroegtijdige risico-achtige PIA en compliance is echter vaak lastig aan te brengen. De verwevenheid van een risicobeoordeling, privacy by design en compliance-achtige aspecten kwam ook naar voor in het advies van het College bescherming persoonsgegevens van 5 maart 2013 over het Toetsmodel PIA Rijksdienst (z2012-00847).

De benodigde flexibiliteit bij de uitvoering van een PIA houdt in dat een PIA iedere keer maatwerk is. In deze PIA staan de risico's die aan keteninformatisering en het verzenden van berichten tussen ketenpartijen centraal.

2.2 Het ontstaan en de ontwikkeling van de PIA

De PIA als instrument is oorspronkelijk tot ontwikkeling gekomen in landen met een Angelsaksisch georiënteerd rechtssysteem. Zo verschenen er rond 2005 modellen en beschrijvingen voor een PIA van de hand van de Canadese, de Britse en de Australische privacy-toezichthouders. Ook de federale overheid van de Verenigde Staten kwam in die periode met een model en procedure voor het uitvoeren van een PIA. De PIA was daarbij verbonden met het eerder door o.a. de Nederlandse privacy toezichthouder ontwikkelde uitgangspunt van “Privacy Enhancing Technologies” en met het in bijvoorbeeld artikel 13 van de Wet bescherming persoonsgegevens wat impliciet opgenomen uitgangspunt van “Privacy by design”.

Belangrijke ontwikkelingen in Nederland bij de ontwikkeling van een PIA zijn de motie Franken van 17 mei 2011 over het uitvoeren van een PIA in het kader van wetgeving (EK, 31 051, nr. D) en bijvoorbeeld de motie Elissen en Gesthuizen van 13 oktober 2011 over privacy by design en safety by design bij de ontwikkeling van nieuwe ICT-projecten (TK, 26 643, nr. 203). De ontwikkeling en de uitvoering van een PIA kwam ook aan de orde in de Notitie Privacybeleid van het kabinet van 29 april 2011. Ook in het Regeerakkoord komt het uitvoeren van een PIA aan de orde.

In november 2011 was er in het kader van de I-strategie Rijk het besluit van het kabinet om de bestaande maatregelen ten aanzien van de beheersing van grote ICT-projecten van het Rijk uit te breiden met maatregelen ter bescherming van privacy. De reeds bestaande eisen ten aanzien van de inhoud van projectplannen voor grote ICT-projecten zijn daartoe aangevuld met de eis om in het projectplan informatie op te nemen of er bij het project sprake is van het opnemen van privacygevoelige gegevens en koppelingen of verrijking daarvan en om, zo nodig, een PIA uit te voeren.

Inmiddels is voor een PIA voor de Rijksdienst het *Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst* van 24 juni 2013 (Bijlage bij TK, 26 643, nr. 282) verschenen. Het Toetsmodel dient vanaf 1 september 2013 standaard te worden toegepast bij ontwikkeling van nieuwe wetgeving en beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien.

Deze PIA bevat zowel wetgevingsaspecten (de regeling over de voorziene berichten) als het gebruik van een nieuwe ICT-infrastructuur voor het voorziene berichtenverkeer.

3 Het onderwerp (object) van de PIA Justitiële Keteninformatisering

3.1 De justitiële ketenberichten Jeugdwet

De nieuwe Jeugdwet zal, zo is voorzien, per 1 januari 2015 in werking treden. Het voornaamste doel van de Jeugdwet is dat alle kinderen gezond en veilig opgroeien, hun talenten ontwikkelen en meedoen in de samenleving naar vermogen. Het gaat daarbij om preventie en uitgaan van eigen kracht van jeugdigen, ouders en het sociale netwerk het minder snel medicaliseren, meer ontzorgen en normaliseren, eerder (jeugd)hulp op maat voor kwetsbare kinderen, integrale hulp met betere samenwerking rond gezinnen en meer ruimte voor jeugdprofessionals en vermindering van regeldruk.

De Jeugdwet brengt door de nieuwe rol van gemeenten en de AMHK's veranderingen met zich mee bij de verantwoordelijkheden in de beschermings- en jeugdstrafrechtketen. Justitiële organisaties, gemeenten en private partijen dienen nauw samen te werken om de doelstellingen van een effectiever, efficiënter en een financieel eenvoudiger jeugdzorgstelsel te bewerkstelligen. In het nieuwe jeugdstelsel krijgen gemeenten en justitiële organisaties andere verantwoordelijkheden bij de uitvoering van de jeugdbescherming en jeugdreclassering (het gedwongen kader). Efficiënte en effectieve informatie-uitwisseling tussen betrokken partijen is daarbij cruciaal voor een goede uitvoering van de Jeugdwet. Deze PIA ziet voor wat de informatie-uitwisseling betreft op de justitiële keteninformatisering.

In deze PIA staan de taken en werkzaamheden van het deelproject justitiële keteninformatisering centraal. Daarbij gaat het eerste om de (nieuwe) justitiële ketenberichten die ter uitvoering van de Jeugdwet met behulp van een nieuwe als berichteninfrastructuur tussen de gebruikers verzonden worden. Het zijn berichten tussen het gemeentelijk domein, het justitieel domein en gecertificeerde instellingen over jeugdbescherming, jeugdreclassering en meldingen door de politie. Hierbij ligt de nadruk op de regeling van de berichten.
Als tweede gaat het om de nieuwe berichteninfrastructuur de *Collectieve Opdracht Routeer Voorziening* (CORV). De CORV is een digitaal knooppunt dat zorgt voor de elektronische afhandeling van het formele berichtenverkeer (de justitiële ketenberichten) tussen justitiepartijen en het gemeentelijke domein. Hierbij ligt de nadruk op de ICT-aspecten en in het bijzonder informatiebeveiliging.
Als derde komt ook kort de inbedding van de justitiële keteninformatisering in de informatiehuishouding van de gebruikers aan de orde.

De privacy risico's die aan de justitiële keteninformatisering verbonden zijn, zien, zoals hierboven is aangegeven op de berichten die ketenpartijen aan elkaar verzenden, de ICT-infrastructuur die daarvoor gebruikt wordt en de wijze waarop gebruikers aangesloten zijn op de infrastructuur.

Het algemene risico in verband met privacy en de verwerking van persoonsgegevens bij berichten en berichten infrastructuren is een onrechtmatige verspreiding van gegevens. Bij deze verspreiding zijn er drie aspecten:

- de niet toegestane verstrekking van gegevens als gegevens niet aan de ontvanger verstrekt mogen worden, bijvoorbeeld als er een specifieke geheimhoudingsverplichting is of als de gegevens niet noodzakelijk zijn voor de ontvanger. Dit ziet op de inhoud van de berichten;
- de niet toegestane verstrekking van gegevens als de berichten niet bij de juiste ontvanger bezorgd worden. Dit ziet vooral op de werking van de berichten infrastructuur en de wijze waarop berichten geadresseerd worden;
- een onvoldoende informatiebeveiliging waardoor de gegevens (te) kwetsbaar worden voor bijvoorbeeld verlies of diefstal.

In deel II wordt, gebaseerd op de algemene risico's, een risico-toetsmodel gebruikt dat specifiek betrekking op keteninformatisering en berichtenverkeer. De verschillende onderdelen en onderwerpen die in deel II aan de orde komen vormen zo het *PIA-toetsmodel* voor de privacyaspecten en privacy-risico's bij de justitiële ketenberichten die ter uitvoering van de Jeugdwet met behulp van de CORV als berichten infrastructuur tussen de gebruikers van de CORV verzonden worden. Zoals gezegd ligt bij de CORV de nadruk op informatiebeveiliging.

Het *PIA-toetsmodel* voor de justitiële keteninformatisering, bestaat uit de volgende onderdelen.

Een onderdeel over de berichten (paragraaf 5), bestaande uit:
- de positionering van de gegevensuitwisseling bij samenwerking;
- de zeggenschap over de berichten en de inhoud;
- de rechtvaardiging van de berichten en de inhoud.

Een onderdeel over de centrale berichteninfrastructuur CORV (paragraaf 6), bestaande uit:
- de werking en functies van de berichteninfrastructuur;
- de beheersbaarheid van de berichten infrastructuur.

Een onderdeel over de inbedding in de informatiehuishouding van verzenders en ontvangers (paragraaf 7), bestaande uit:

- aandachtspunten voor gebruikers in verband met aansluiting op de CORV;
- elementen die bij aansluiting een rol kunnen spelen.

In het PIA-Toetsmodel wordt aangegeven in welke mate risico's aanwezig zijn (laag, midden, hoog) en welke factoren een rol spelen bij de mate waarin de risico's aanwezig zijn. Een specifiek aspect bij de mate waarin risico's aanwezig zijn, ziet op alternatieven die aanwezig en het alternatief dat gekozen is. Zo is bijvoorbeeld duidelijk dat de keuze voor de aanleg van een

centraal bestand dat door zo'n 400 gemeenten bevraagd zou kunnen worden, een keuze is met meer risico's dan de keuze voor het inrichting van een infrastructuur die het op gestructureerde wijze mogelijk maakt dat (enkel) berichten verzonden worden zonder centrale opslag van persoonsgegevens.

3.2 Het deelproject Justitiële Keteninformatisering

De justitiële ketenberichten Jeugdwet behoren tot het deelproject *Justitiële Keteninformatisering*. Het deelproject is één van de onderdelen van het *Project Beleidsinformatie Stelselherziening Jeugd*. Het Project Beleidsinformatie Stelselherziening Jeugd is een gezamenlijk project van de ministeries van VWS en VenJ. Tot het gehele project behoren de deelprojecten:

- Data en systematiek Beleidsinformatie;
- Standaarden voor gegevensuitwisseling;
- Justitiële Keteninformatisering;
- Eenmalige overdracht cliëntgegevens.

In het *Projectplan Beleidsinformatie Stelselherziening Jeugd* van 8 november 2012 (Projectplan) wordt de kern van het deelproject Justitiële Keteninformatisering als volgt omschreven (p. 2):

> *3. Versterken van ketensamenwerking op het gebied informatievoorziening*
>
> In de justitiële jeugdketen zijn op hoofdlijnen twee ketens te onderscheiden namelijk:
>
> 1. De jeugdstrafrechtketen met daarin partners als de politie, het Openbaar Ministerie (OM) de Raad voor de Kinderbescherming (RvdK), ZM, reclassering en justitiële jeugdinrichtingen.
> 2. De jeugdbeschermingsketen met daarin onder meer de RvdK en de Rechterlijke macht de gemeenten en BJZ's gaan in deze keten een andere rol vervullen.
>
> Zowel de ketenpartners als de nieuwe actoren dienen meegenomen te worden in de ontwikkelingen aangezien de gemeenten en justitiële ketens in elkaar gehaakt dienen te worden; zo het 'invoegen' van de toekomstige gecertificeerde instellingen voor jeugdreclassering en jeugdbescherming.
>
> Hiertoe zal de informatievoorziening geregeld moeten worden.

In het Projectplan is voorzien in aandacht voor de privacyaspecten bij de verschillende deelprojecten, zoals het deelproject over de eenmalige gegevensoverdracht. Over aandacht voor privacyaspecten wordt op p.2 van het Projectplan vermeld:

> Een belangrijk doel is het vroegtijdig anticiperen op privacyaspecten. Hierdoor wordt tijdig geborgd dat de informatievoorziening en gegevensverwerking op ketenniveau

> binnen het nieuwe stelsel aan alle privacy eisen voldoet. Juridische borging en privacy worden geborgd in de afzonderlijke deelprojecten.

De uitvoering van een PIA voor de deelprojecten komt ook aan bod. Voor wat een PIA over de Justitiële Keteninformatisering betreft, vermeld het Projectplan op p. 9 als één van de resultaten:

> a) Privacy Impact Assessment (PIA) voor de data-uitvragen en beheer van het bestand.

Verder komt de benodigde aandacht voor privacy en het uitvoeren van een PIA uitgebreid aan de orde in onderdeel 4 van het *Beslisdocument Interacties tussen gemeenten, gecertificeerde instellingen en de justitiële jeugdketens in het nieuwe jeugdstelsel* van het project van 11 april 2013.

3.3 De PIA ter uitvoering van het Projectplan, de motie Bergkamp en het regeringsbeleid betreffende een PIA voor de Rijksdienst

Deze PIA geeft uitvoering aan de in het Projectplan voorziene PIA voor het deelproject justitiële keteninformatisering en geeft tevens uitvoering aan de motie Bergkamp van 4 april 2013 over een PIA betreffende de uitwisseling van gegevens over cliënten tussen partijen als provincies, gemeenten en bureau jeugdzorg (TK, 31 839, nr. 279). De PIA is voor de eerste maal aangekondigd in de brief aan de Tweede Kamer van de Staatssecretarissen van VWS en VenJ van 13 mei 2013 (TK, 31 839 nr. 290).
Daarnaast geeft de PIA uitvoering aan het regeringsbeleid dat vanaf 1 september 2013 standaard een PIA dient te worden uitgevoerd bij ontwikkeling van nieuwe wetgeving en beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien (zie: TK, 26 643, nr. 282). De PIA omvat daartoe de onderdelen en onderwerpen zoals opgenomen zijn in het *Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst van 24 juni 2013* (Bijlage bij TK, 26 643, nr. 282). Zie in dit verband ook Bijlage 3.
De PIA geeft ten aanzien van de regeling van de berichten tevens uitvoering aan de Motie Franken van 17 mei 2011 over het uitvoeren van een PIA in het kader van wetgeving (EK, 31 051, nr. D).
Voor wat de nieuw in te richten berichteninfrastructuur betreft, geeft de PIA aan de Motie Elissen en Gesthuizen van 13 oktober 2011 over privacy by design en safety by design bij de ontwikkeling van nieuwe ICT-projecten (TK, 26 643, nr. 203).

4 Beschrijving van de justitiële keteninformatisering en de CORV

4.1 Algemene beschrijving van de justitiële keteninformatisering

Uitgangspunt bij de justitiële keteninformatisering is dat de ketensamenwerking tussen de verschillende betrokken partijen eenduidige afspraken over de informatie-uitwisseling vereist. Als alle betrokken partijen separaat onderlinge afspraken over gegevensuitwisseling maken leidt dit tot extra administratieve lasten, minder overzicht, mogelijke rechtsongelijkheid bij bijvoorbeeld verzoeken tot onderzoek aan de RvdK, en meer kans op vertraging en fouten in de uitvoering. Tevens zal een goede informatiebeveiliging bij allerlei verschillende en afwijkende afspraken en methoden om gegevens te verzenden onder druk komen te staan.

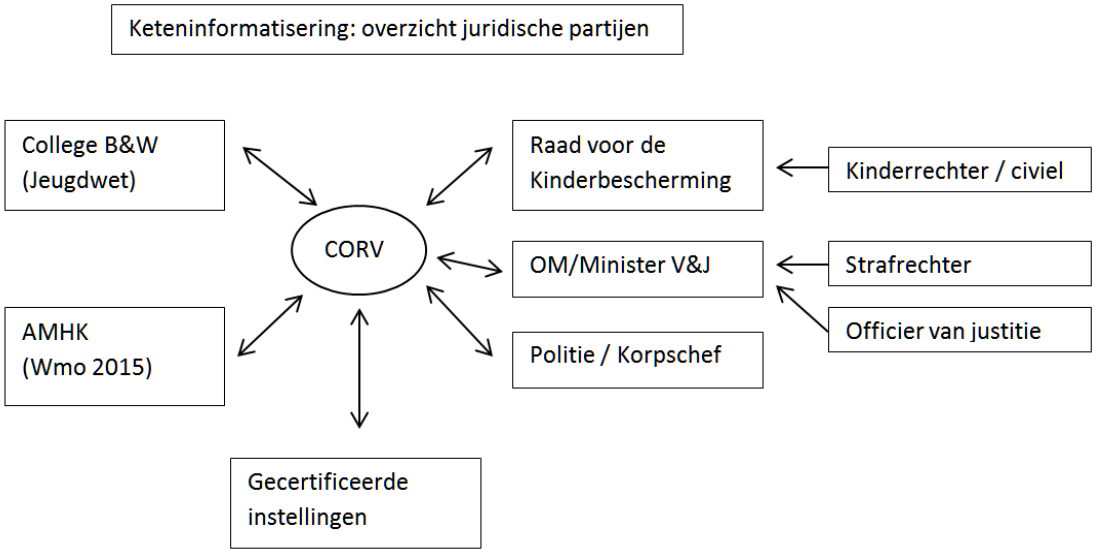
Bij de justitiële keteninformatisering gaat het om formele berichten tussen justitiepartijen, het gemeentelijke domein en de gecertificeerde instellingen. De berichten hebben betrekking op jeugdbescherming (kinderbeschermingsmaatregelen), jeugdreclassering en zorgmeldingen door de politie. Om die reden wordt gesproken van 'justitiële' keteninformatisering. Met de term 'formeel' wordt aangegeven dat de berichten door de verzender verstuurd worden als het sluitstuk van bepaalde werkzaamheden van de verzender; het gevolg of resultaat van een proces of deelproces. Voor de ontvanger van berichten zijn de berichten juist het startpunt voor het uitvoeren van de taken en werkzaamheden. Het gaat in die zin (veelal) om daadwerkelijke opdrachten waarbij actie wordt verwacht van de ontvangende partij. De formele berichten zien daarbij op hét overdrachtsmoment van werkzaamheden tussen de betrokken ketenpartijen.
De ontwikkeling van welke berichten betreffende jeugdbescherming en jeugdreclassering door bepaalde partijen aan elkaar gezonden worden en de inhoud van die berichten, is een onderdeel van de taken en werkzaamheden van het Deelproject justitiële keteninformatisering. Een uitzondering hierop vormen de meldingen door de politie. Weliswaar heeft het Deelproject daarbij een stimulerende rol, maar is er geen inhoudelijke rol t.a.v. de meldingen.
De risicobeoordeling van dit deel van de werkzaamheden van het Deelproject over de berichten en hun inhoud komt aan de orde in paragraaf 5 over de berichten.

Het 'formele' karakter van de berichten geeft tevens het belang aan van eenduidige afspraken over de informatie-uitwisseling. Verzekerd dient te worden dat de overdracht van informatie op momenten waarbij de werkzaamheden van de verzendende partij als het ware beëindigen en vervolgens voorgezet dienen te worden door de ontvangende partij, juist, accuraat en snel plaatsvindt. Zonder een adequate informatieverstrekking van verzender aan ontvanger zou de keten c.q. het proces, van jeugdbescherming, de uitvoering van jeugdreclassering en het behandelen van zorgmeldingen gedaan door de politie onnodige vertraging op kunnen lopen en zelfs stil kunnen vallen.

Juist omdat het essentieel is dat op de momenten waarbij de werkzaamheden van de ene ketenpartner overgenomen worden door de andere ketenpartners, de informatieverstrekking juist, accuraat en snel plaatsvindt, wordt voor het verzenden van berichten over jeugdbescherming, jeugdreclassering en zorgmeldingen door de politie, een (nieuwe)

voorziening ontwikkeld en ingericht. Het gaat bij deze nieuwe voorziening om de CORV. CORV staat hierbij voor Collectieve Opdracht Routeer Voorziening. Het is een digitaal knooppunt dat zorgt voor de elektronische afhandeling van het berichtenverkeer tussen de betrokken partijen. De CORV is daarbij wel te zien als een 'postkantoor ofwel -routeer' voorziening. De CORV ontvangt berichten van een verzender, transformeert de berichten naar het juiste berichtenformat en stuurt deze door naar de ontvanger. Uitgangspunt is dat de digitale berichtuitwisseling via de CORV, veilig en snel en met gegarandeerde aflevering plaatsvindt. In die zin kan de vergelijking gemaakt worden met aangetekende post.
Ook het ontwikkelen en inrichten van de nieuwe CORV is een onderdeel van de taken en werkzaamheden van het Deelproject justitiële keteninformatisering.

In onderstaand schema wordt een overzicht gegeven van de partijen die gelet op de in wetgeving aan hen toebedeelde taken en werkzaamheden betrokken zijn bij de justitiële keteninformatisering en de CORV als centrale berichten routeervoorziening.



Bij de colleges van B&W zien de berichten en de aansluiting op de CORV op de toeleidingstaak van gemeenten bij de uitvoering van de Jeugdwet (art. 2.3 Jeugdwet), het eventueel doen van een verzoek tot onderzoek (VTO) aan de Raad voor de Kinderbescherming (art. 2.4, lid 1, Jeugdwet) en de verantwoordelijkheid voor en financiering van de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering (art. 2.4 Jeugdwet). Hierbij speelt ook de gewenste regievoering door gemeenten een rol. In bijvoorbeeld de brief van de Staatssecretarissen van VWS en VenJ aan de nieuwe wethouders Jeugd van 24 juni 2014 wordt daarbij gesproken over een eenvoudiger jeugdstelsel gericht op een integrale aanpak; 1-gezin, 1-plan, 1-regisseur. Hulpverleners werken daarbij samen rond gezinnen. Zij doen een beroep op de eigen kracht en op het sociale netwerk van kinderen en hun ouders. De nadruk komt te liggen op preventie. Op normaliseren. Op lichte hulp. Ook het doel van het jeugdstrafrecht (het bevorderen van passende sanctionering en resocialisatie waarbij rekening wordt gehouden met de ontwikkelingsfase van de jeugdige), sluit aan bij een integrale aanpak.

Bij de AMHK's zien de berichten en de aansluiting op de CORV op de taken en werkzaamheden van de nieuwe AMHK's die geregeld worden in hoofdstuk 4 van de Wmo 2015. In het bijzonder gaat het om het fungeren als meldpunt voor gevallen of vermoedens van huiselijk geweld of kindermishandeling (art. 4.1.1, lid 1, Wmo 2015), het eventueel doen van een verzoek tot onderzoek (VTO) aan de Raad voor de Kinderbescherming (art. 4.1.1, lid 2, onder e, Wmo 2015) en het informeren van de gemeente daarover (art. 4.1.1, lid 2, onder f, Wmo 2015).

Bij de Raad voor de Kinderbescherming hebben de berichten en de aansluiting op CORV betrekking op de centrale positie in het kader van kinderbeschermingsmaatregelen. De Raad doet onderzoek (art. 3.1, lid 1 en 2, Jeugdwet), verzoekt de kinderrechter tot het opleggen van kinderbeschermingsmaatregelen (art. 254, 261 en 266 Boek 1 Burgerlijk Wetboek) en is, als verzoeker, belast met het informeren van bijvoorbeeld gemeenten en gecertificeerde instelling over de door de rechter opgelegde kinderbeschermingsmaatregelen. Daarbij informeert of overlegt de Raad met de betrokken gemeenten (art. 3.1, lid 3, en lid 6, Jeugdwet). Voor wat jeugdreclassering betreft kan de Raad een gecertificeerde instelling inschakelen voor vrijwillige begeleiding (art. 77hh, lid 2, Wetboek van Strafrecht).

Bij het Openbaar ministerie en de Minister van VenJ zien de berichten en de aansluiting op de CORV op de tenuitvoerlegging van rechterlijke beslissingen en strafbeschikkingen. Onderdeel hiervan is de jeugdreclassering opgelegd door de rechter of door de Officier van Justitie.
Op dit moment is het Openbaar ministerie belast met de tenuitvoerlegging van rechterlijke beslissingen en strafbeschikkingen (art. 553 en art. 572 Wetboek van Strafvordering). In de (nabije) toekomst zal de Minister van VenJ belast worden met de tenuitvoerlegging van rechterlijke beslissingen en strafbeschikkingen (artikel 6:1:1, lid 1, van het conceptwetsvoorstel Wet herziening tenuitvoerlegging strafrechtelijke beslissingen, consultatieversie van 4 november 2013).

De politie heeft per jaar contact met ongeveer 30.000 jeugdigen die mogelijk zorg of hulp behoeven. Dan gaat het om jeugdigen die bedreigd of verwaarloosd worden, getuige of (vermoedelijk) slachtoffer of dader zijn van huiselijk geweld, om jeugdigen die zwerf- of wegloopgedrag vertonen of betrokken zijn bij kinderprostitutie of slachtoffer van 'loverboys'. Het gaat hierbij ook om jeugdigen onder de 12 jaar die verdacht worden van het plegen van een strafbaar feit terwijl zij niet strafrechtelijk aansprakelijk gesteld kunnen worden. Onder de huidige Wet op de jeugdzorg doet de politie hiervan melding bij 'de toegang' van het bureau jeugdzorg. Met de Jeugdwet en de Wmo 2015 wordt het ontvangen en behandelen van politiemeldingen een taak van de gemeenten en de AMHK's. De meldingen door de politie (de berichten) en de aansluiting op de CORV vloeien voort uit de algemene politietaken, in het bijzonder het verlenen van hulp aan hen die deze behoeven. Bij kindermishandeling speelt ook de daadwerkelijke handhaving van de rechtsorde (art. 3 Politiewet 2012).

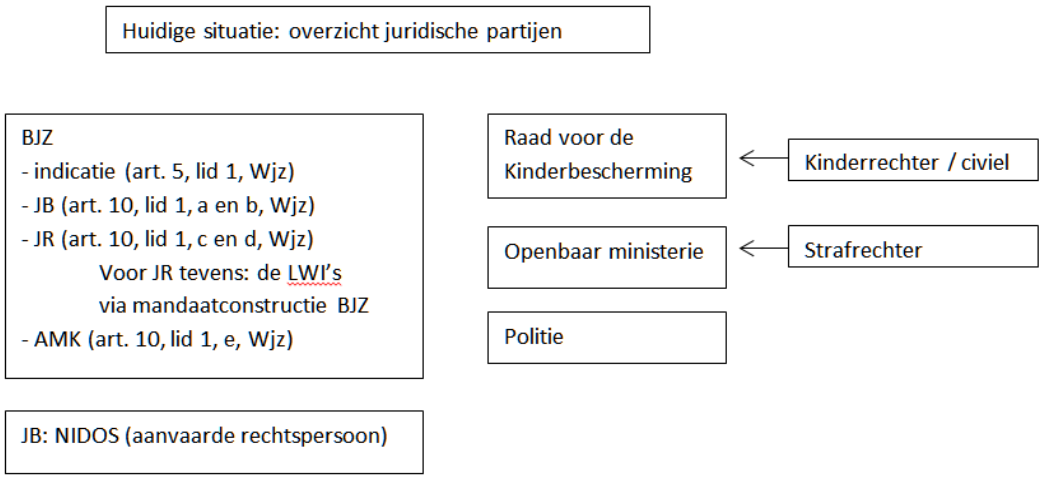
Bij de gecertificeerde instellingen zien de berichten en de aansluiting op de CORV op de taken en werkzaamheden bij de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering (art. 3.2 Jeugdwet). Ook kan een verzoek tot onderzoek (VTO) aan de Raad voor de Kinderbescherming gedaan worden (art. 3.1, lid 1, Jeugdwet). Daarbij informeert of

overlegt de gecertificeerde instelling met de betrokken gemeenten (art. 3.1, lid 4, en art. 3.5 Jeugdwet).

Zoals uit bovenstaand overzicht blijkt, worden de kinderrechter die beslist over kinderbeschermingsmaatregel en de strafrechter of de officier van justitie die jeugdreclassering oplegt, niet direct aangesloten op de CORV. Dit past bij de inrichting van het procesrecht en de scheiding tussen de rechtsprekende en de uitvoerende macht, waarbij de beslissende rechter niet belast is met de uitvoering of tenuitvoerlegging van beslissingen. Bij kinderbeschermingsmaatregelen is het de RvdK als centrale partij en verzoeker die, als verzoeker tot het opleggen van een kinderbeschermingsmaatregel, belast is met het informeren van bijvoorbeeld gemeenten en gecertificeerde instelling over de door de rechter opgelegde kinderbeschermingsmaatregelen. In het strafrecht is het OM, en binnenkort de Minister van VenJ, belast met de tenuitvoerlegging van jeugdreclassering in het kader van de executieverantwoordelijkheid.

Het belang van eenduidige afspraken over de informatie-uitwisseling (de berichten) en de CORV als nieuwe berichten routeervoorziening blijkt ook uit een vergelijking met de huidige situatie van de Wet op de jeugdzorg (Wjz).

De partijen die in de huidige situatie een rol spelen bij kinderbeschermingsmaatregelen, jeugdreclassering en zorgmeldingen door de politie zijn opgenomen in onderstaand overzicht.



Uit het overzicht blijkt dat de huidige Bureaus Jeugdzorg (BJZ) een centrale rol vervullen. Zo behandelen de BJZ zorgmeldingen van de politie (art. 5, lid 1, Wjz) en fungeren de BJZ als AMK's bij kindermishandeling (art. 10, lid 1, onder e, Wjz). Daarnaast zijn de BJZ belast met de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering (art. 10, lid 1, onder a t/m d, Wjz). De landelijk werkende instellingen, zoals het Leger des Heils en de William Schrikker Stichting vervullen hun werkzaamheden onder de paraplu van de BJZ (mandaatregeling LWI). De Stichting NIDOS is belast met de zorg en de uitvoering van

maatregelen ten aanzien van alleenstaande minderjarige asielzoekers (AMA's) en vergelijkbare jeugdigen. Het gaat daarbij om jongeren:

- die jonger dan twaalf jaar zijn, voor wie een asielaanvraag eerst wordt ingediend als Nidos de voogdij over hen heeft verkregen;
- van wie de moeder onder voogdij staat van Nidos en voor of door wie een aanvraag om een (reguliere) verblijfsvergunning onder de beperking 'verblijf bij moeder' is ingediend;
- die op Nederlands grondgebied worden aangetroffen en slachtoffer zijn geworden van mensenhandel en door of voor wie een (reguliere) aanvraag om een verblijfsvergunning onder de beperking 'slachtoffer-aangever van mensenhandel' wordt ingediend;
- die op een luchthaven in Nederland onbegeleid worden aangetroffen en door of voor wie een reguliere aanvraag wordt of kan worden ingediend;
- die alleen achterblijven in een opvangcentrum van het COA nadat hun ouders met onbekende bestemming zijn vertrokken;
- die onder toezicht zijn gesteld van Nidos en wier ouder(s) zijn ontheven of ontzet van het gezag, dan wel met onbekende bestemming zijn vertrokken.

De belangrijke wijziging in het nieuwe stelsel is dat de taken van de huidige 15 Bureaus jeugdzorg vervangen worden door taken voor de gemeenten, de nieuwe gecertificeerde instellingen en de AMHK's. Wat aantallen betreft worden de huidige minder dan 20 partijen (15 Bureaus jeugdzorg, de LWI's en NIDOS) vervangen door bijna 400 gemeenten, naar verwachting zo'n 25 gecertificeerde instellingen en ruim 25 AMHK's. Deze wijzigingen zijn hieronder weergegeven.

Huidige situatie (Wjz)	**Toekomstig (Jeugdwet, Wmo 2015)**
BJZ indicatie (art. 5 Wjz)	College B&W toeleiding
BJZ JB (art. 10, 1, a en b Wjz)	Gecertificeerde instellingen
BJZ JR (art. 10, 1, c en d Wjz)	Gecertificeerde instellingen
JR: LWI's via mandaatconstructie BJZ	Gecertificeerde instellingen
BJZ AMK (art. 10, 1, e Wjz)	AMHK's
JB: NIDOS	NIDOS als gecertificeerde instelling

Voor wat de justitiepartijen betreft, zijn er geen inhoudelijke wijzigingen. Enkel bij de tenuitvoerlegging van jeugdreclassering zal de Minister van VenJ de huidige taken van het Openbaar ministerie overnemen. De taken en werkzaamheden van de justitiepartijen zijn hieronder weergegeven.

Huidige situatie	**Toekomstig**
Raad voor de Kinderbescherming	Raad voor de Kinderbescherming
Kinderrechter / civiel	Kinderrechter / civiel
Openbaar Ministerie (executie)	Minister van VenJ (executie)
Strafrechter	Strafrechter
Politie	Politie

Alleen al het aantal nieuwe partijen geeft aan waarom voor de toekomstige informatieverstrekking eenduidige afspraken over de berichten en ondersteuning door de nieuwe CORV noodzakelijk zijn. Alleen dan kan voorkomen worden dat binnen de keten c.q. het proces, van jeugdbescherming, de uitvoering van jeugdreclassering en het behandelen van meldingen door de politie geen onnodige vertraging optreedt en dat de digitale berichtuitwisseling via de CORV, veilig en snel en met gegarandeerde aflevering plaatsvindt.

4.2 De berichten

Bij de via de CORV te verzenden berichten gaat het om berichten die behoren bij het proces van kinderbeschermingsmaatregelen. Het gaat om berichten betreffende:

- een verzoek tot onderzoek (VTO) in te stellen door de Raad voor de Kinderbescherming en het vervolg bij de Raad. Een uitzondering hierop vormen de spoedmeldingen;
- een ambtshalve onderzoek ingesteld door de Raad voor de Kinderbescherming en het vervolg daarvan, en
- een door de rechter opgelegde kinderbeschermingsmaatregel.

Bij de te verzenden berichten gaat het eveneens om berichten betreffende door de rechter of de officier van justitie opgelegde jeugdreclassering en eventueel in dat kader opgelegde jeugdhulp. Tot dit domein behoort ook de door de Raad voor de kinderbescherming in het kader van vrijwillige ‘jeugdreclassering’ aangewezen begeleiding.

Als derde gaat het bij de berichten om meldingen van de politie over bijvoorbeeld kindermishandeling of zorgmeldingen in verband met eventuele opgroei- en opvoedproblemen. De voorziene berichten hebben geen betrekking op acute noodsituaties. Dergelijke meldingen geschieden bijvoorbeeld per telefoon en vinden in die zin plaats buiten de CORV om.

Bij de inhoudelijke berichten die verzonden worden, kan een onderscheid gemaakt worden tussen:

- primaire berichten ten behoeve van de ontvanger en de door de ontvanger uit te voeren werkzaamheden;
- een kopie van primaire berichten, bijvoorbeeld ten behoeve van regievoering door de Raad voor de Kinderbescherming bij jeugdreclassering, en
- notificaties waarbij enkel medegedeeld wordt dat een bepaalde gebeurtenis plaatsgevonden heeft. Hierbij kan gedacht worden aan berichten aan de gemeente over het feit dat jeugdreclassering of een kinderbeschermingsmaatregel is opgelegd of dat de RvdK ambtshalve een onderzoek heeft ingesteld.

Meer technisch bezien gaat het naast de inhoudelijke berichten ook om:

- afleverberichten die de bevestiging inhouden dat een bericht bij de geadresseerde is afgeleverd, en
- foutmeldingen die vervolgens tot gevolg zullen hebben dat het bericht opnieuw verzonden dient te worden.

4.2.1 berichten jeugdbescherming en jeugdreclassering

De diverse berichten bij het proces van kinderbeschermingsmaatregelen en jeugdreclassering zijn uitgebreid en in detail beschreven in:

- Het rapport *Stelselherziening Jeugdbescherming* van de Justitiële Informatiedienst van april 2014
- Het rapport *Ketenproces Jeugdreclassering* van de Justitiële Informatiedienst van 13 juni 2014

Zie in dit verband en ter illustratie ook de in Bijlage 2 opgenomen overzichten over berichten aan de gemeenten. Die overzichten geven een algemene samenvatting van de berichten, de inhoud van de berichten en voor welke taken en werkzaamheden van de ontvanger de berichten verzonden worden.
In bepaalde gevallen kan, in het bijzonder bij jeugdreclassering, door het OM of door de rechter ook jeugdhulp aangewezen worden in aanvulling op de jeugdreclassering. Dergelijke door het OM of de rechter opgelegde jeugdhulp zal eveneens onderdeel uitmaken van de berichten.

4.2.2 Meldingen politie

Zoals reeds is aangegeven, is voorzien in een aansluiting op de CORV voor politiemeldingen en voor het verzenden van meldingen te gebruiken politie-formulieren zijn (deels) al aanwezig en verder in ontwikkeling. Om die reden zijn ook de meldingen door de politie van belang in het kader van deze PIA. De politiemeldingen zien (deels) op meldingen die thans onder de Wet op de jeugdzorg gedaan worden aan de ‘toegang’ van de bureaus jeugdzorg en de AMK’s van de bureaus.

Meldingen door de politie over kindermishandeling, huiselijk geweld en zorgmeldingen betreffende jeugdigen in verband met bijvoorbeeld opgroei – of opvoedproblemen, alsmede meldingen betreffende jeugdigen jonger dan 12 jaar (de 12-minners) die strafbare feiten gepleegd hebben, komen aan de orde in bijvoorbeeld de volgende documenten:

- Het *Logisch ontwerp formulier Zorgmeldingen jeugdige* van vts Politie Nederland van 29 oktober 2012;
- De Factsheet *Zorgmeldingen Jeugd* van de VNG van juni 2014;
- Het *Programma van Eisen ICT-ondersteuning AMHK* van de VNG van 16 mei 2014;
- Het Concept *Model Handelingsprotocol voor het AMHK* van de VNG van 4 juni 2014.

Voor wat de 12-minners betreft kan als voorbeeld ook gewezen worden op het ProKid Signaleringsinstrument 12-. ProKid richt zich primair op het voorkomen van crimineel gedrag bij probleemkinderen, maar is tevens een signaleringssysteem gericht op het vroegtijdig signaleren van problemen bij jeugdigen inzake de psychische, lichamelijke, cognitieve en sociale ontwikkeling.

Ook in verband met gebruik van de CORV is reeds een specifiek bericht voor meldingen door de politie ontworpen.

In de huidige situatie onder de Wet op de jeugdzorg worden meldingen door de politie over kindermishandeling, meldingen over huiselijk geweld waarbij kinderen betrokken en zorgmeldingen over jeugdigen aan de bureaus jeugdzorg gezonden. De huidige zorgformulieren die de politie gebruikt zien ook op dergelijke meldingen.

Onder het nieuwe stelsel van de Jeugdwet en de Wmo 2015 behoren meldingen over kindermishandeling en huiselijk geweld tot de taken van de AMHK's. De zorgmeldingen over jeugdigen waarbij er geen sprake is van kindermishandeling of huiselijk geweld, behoren tot de gemeentelijke toeleidingstaak.

Vanuit een juridisch oogpunt kunnen, voor wat de CORV betreft, in de toekomstige situatie de volgende meldingen onderscheiden worden:

a. Kindermishandeling aan de AMHK's (artikel 4.1.1, lid 2, onder a, Wmo en een aangepaste nieuwe bepaling in het Besluit politiegegevens)
b. Huiselijk geweld aan de AMHK's (artikel 4.1.1, lid 2, onder a, Wmo en een nieuwe bepaling in het Besluit politiegegevens)
c. Zorgmeldingen betreffende jeugdigen waarbij er geen sprake is van kindermishandeling of huiselijk geweld aan de colleges van B&W (artikelen 2.3, lid 1 en lid 6, en 2.4, lid 1, Jeugdwet en een nieuwe bepaling in het Besluit politiegegevens)

Daarnaast zijn er nog de (zorg)meldingen betreffende AMA's aan het NIDOS. Voor wat die meldingen betreft is er geen verschil tussen de huidige en de toekomstige situatie. Zoals al is aangegeven, hebben de voorziene berichten geen betrekking op acute noodsituaties. Dergelijke meldingen gescheiden bijvoorbeeld per telefoon en vinden in die zin plaats buiten de CORV om.

De huidige en de toekomstige situatie wordt hieronder weergegeven.

	Huidige situatie	Toekomstige situatie
Zorgmeldingen jeugdigen (geen kindermishandeling)	Aan BJZ als toeleider jeugdzorg (art. 5, Wjz)	College als toeleider jeugdhulp (Jeugdwet)
Meldingen jeugdigen i.v.m. kindermishandeling of huiselijk geweld	Aan BJZ als AMK (art. 10, lid 1, onder e, Wjz)	AMHK (Wmo 2015 met specifieke regels)
Meldingen huiselijk geweld (geen jeugdigen betrokken)		AMHK (Wmo 2015 met specifieke regels)
Meldingen betreffende AMA's	Aan NIDOS	Aan NIDOS

Om ook vanaf 2015 een goede werkwijze en behandeling van politiemeldingen te borgen, is het uitgangspunt bij de betrokken partijen dat de toekomstige AMHK's als centraal loket

fungeren en een eerste beoordeling van de binnen gekomen meldingen doen. Meldingen specifiek voor de gemeentelijke toegangstaak worden daarbij doorgezonden naar de gemeenten. De betrokken partijen, in het bijzonder politie, gemeenten en AMHK's, ondernemen diverse activiteiten om de juiste afhandeling van politiemeldingen vorm te geven. Deze activiteiten zijn er onder meer op gericht om de volgende risico's te beperken.

- het risico dat bepaalde meldingen niet tijdig op de juiste plek terecht komen en mogelijk tussen organisaties (gemeenten, wijkteams, AMHK etc.) gaan 'zwerven'.
- het risico dat a) meldingen vanuit verschillende partijen over eenzelfde situatie of b) in de tijd bezien op verschillende momenten gedane meldingen over eenzelfde jeugdige of gezin niet op een juiste wijze gecombineerd worden, zodat de ernst van de situatie en de noodzaak om te handelen (onbedoeld) miskent wordt of 'onder de oppervlakte verborgen' blijft. In beide gevallen gaat het dan vooral om de optelsom van de verschillende meldingen die juist aanleiding is om te handelen en waarbij de meldingen geheel los van elkaar bezien wellicht geen aanleiding tot handelen zouden geven.

Bovenstaande risico's en de beperking daarvan hebben onder andere betrekking op de ontwikkeling van ICT systemen voor de AMHK's. Zie in dit verband met al genoemde *Programma van Eisen ICT-ondersteuning AMHK* van de VNG van 16 mei 2014. Bij de ontwikkeling van ICT systemen voor de AMHK's, kan ook gewezen worden op de ontwikkeling van het systeem WIJZ. Dit systeem wordt thans onder meer ontwikkeld voor de uitvoering van de taken en werkzaamheden van de toekomstige gecertificeerde instellingen en de AMHK's (zie hiervoor ook paragraaf 4.3)

4.3 De CORV

Voor de nieuwe ketenberichten wordt de CORV als nieuwe berichten infrastructuur (routeervoorziening) ingericht. De ontwikkeling en realisatie van de CORV valt, zoals al is aangegeven, binnen de taken van het Deelproject justitiële keteninformatisering van het project beleidsinformatie stelselherziening jeugd. De ontwikkeling en realisatie wordt uitgevoerd in samenwerking met het de VNG, KING, gemeenten, de raad voor de kinderbescherming, gecertificeerde instellingen en het ministerie van VenJ. Het beheer van CORV wordt belegd bij het ministerie van VenJ. De risico-beoordeling van dit deel van de werkzaamheden van het Deelproject komt aan de orde in paragraaf 6 over de CORV.

Bij een berichten infrastructuur zoals de CORV, wordt in deze PIA de infrastructuur bedoeld die ligt tussen de postbussen/aansluitpunten van de gebruikers. In deze PIA blijven de gegevensverwerkingen (back-offices) van de gebruikers buiten beschouwing. De gebruikers zijn geheel zelf verantwoordelijk voor de naleving van privacy wetgeving voor de eigen achterliggende gegevensverwerkingen (systemen en databases). De gebruikers zijn ook zelf verantwoordelijk voor het verwerken van persoonsgegevens door c.q. binnen de door hen gebruikte postbussen/aansluitpunten. Onverminderd deze eigen verantwoordelijkheid, ondersteunt het Deelproject justitiële keteninformatisering de aansluiting van justitiepartijen en, in samenwerking met Jeugdzorg Nederland, de gecertificeerde instellingen. De

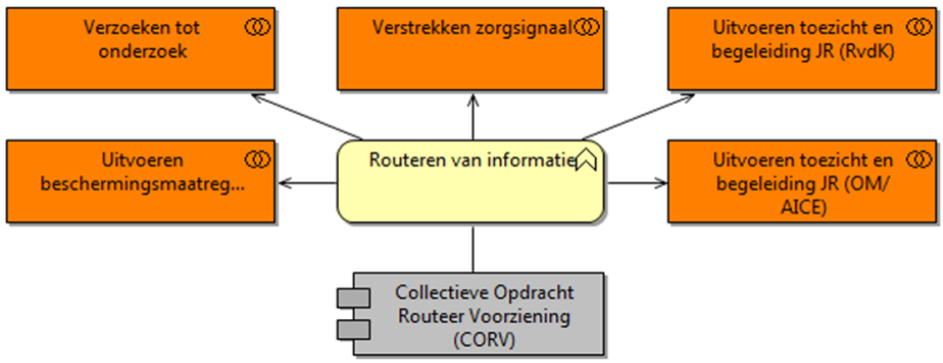
implementatieondersteuning bij gemeenten is een verantwoordelijkheid van de VNG. De VNG heeft de uitvoering hiervan belegd bij KING. Het Deelproject justitiële keteninformatisering faciliteert deze implementatieondersteuning door KING. De risicobeoordeling van dit deel van de werkzaamheden van het Deelproject komt aan de orde in paragraaf 7 over de inbedding in de informatievoorziening van verzenders en ontvangers. Vooral komen daarbij de aansluitvoorwaarden die bij het aansluiten op de CORV gehanteerd zullen worden aan de orde.

De ontwikkeling, implementatie en het beheer van de CORV en het aansluiten door gebruikers worden beschreven in o.a. de volgende documenten:

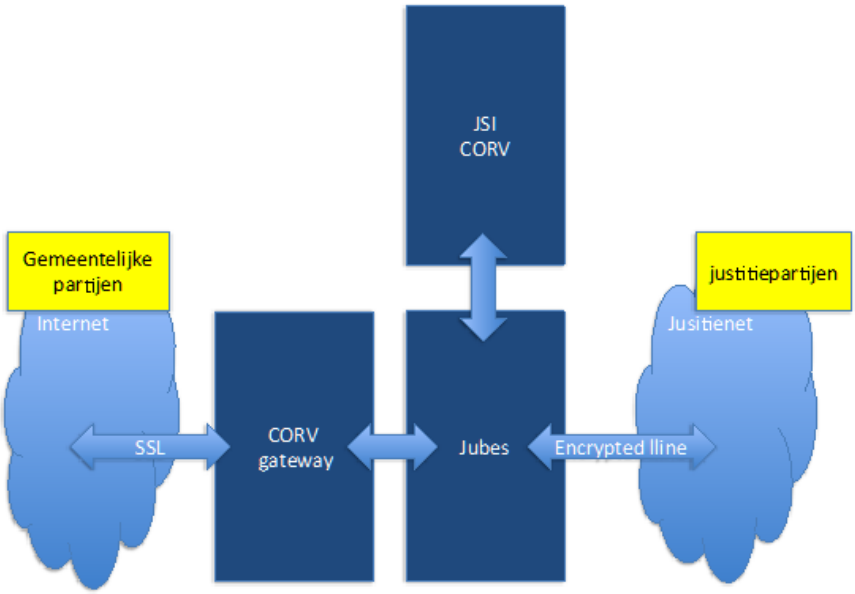
- De *PSA/Solution Architecture, Interactieproces, Koppelvlakken en de Collectieve Opdracht RouteerVoorziening justitiële jeugdketen (CORV)* van 17 juli 2013;
- Het rapport *Beheerinrichting CORV* van 10 oktober 2013;
- Het *Plan van Aanpak Ontwikkeling, implementatie en in beheer name Collectieve Opdracht en Routeer Voorziening (CORV)* van 19 november 2013;
- Het *Acceptatietestplan CORV* van 22 januari 2014 en de *Reviewrapportage* van 12 juni 2014 van de auditor;
- De *Solution Architecture CORV* van de Justitiële Informatiedienst van 11 april 2014;
-Het rapport *Aansluitproces op CORV voor gemeenten* van het projectteam van 14 maart 2014;
-De *Impact Analyse CORV* van KING van 13 mei 2014.

De CORV draagt er zorg voor dat de berichten van de verzender afgeleverd worden bij de ontvanger. Daarbij worden de berichten overgezet van het ene naar het andere berichtformaat. Er vindt geen inhoudelijke bewerking of verrijking van de berichten of de gegevens plaats. De CORV ondersteunt slechts het ontvangen, translatie en verzenden van elektronische berichten. Daarnaast ondersteunt CORV het (tijdelijk) vastleggen en ontsluiten van verkeersgegevens en foutberichten.

De onderstaande figuur geeft de positie van de CORV als routeervoorziening aan bij de verschillende soorten berichten. Deze berichten vloeien voort uit de in paragraaf 2.1 beschreven taken en werkzaamheden van de betrokken ketenpartijen.



De verschillende technische (infrastructurele) componenten van de justitiële keteninformatisering en de CORV zijn weergegeven in de onderstaande figuur. Gecertificeerde instellingen kunnen afhankelijk van hun positie tot de justitiepartijen gerekend worden als ze via jeugdzorgnet op Justitienet zijn aangesloten en tot de gemeentelijke partijen gerekend worden als ze via internet worden aangesloten.



De technische werking van de CORV is als volgt.

Gemeentelijke partijen naar justitiepartijen

1. Via internet (SSL-beveiligd) komt het bericht van een gemeente of gecertificeerde instelling aan op de CORV gateway. Deze berichten zijn opgesteld conform het gemeentelijke Standaard Uitvoerings Formaat (StUF) of de Jeugdzorg XML-standaard;
2. de CORV gateway stuurt het bericht door naar Jubes (Justitie berichten Service);
3. Jubes stuurt het bericht vervolgens naar de Justitie Service Interface JSI CORV;
4. De JSI CORV transformeert het bericht van het gemeentelijke Standaard Uitvoerings Formaat (StUF) naar de elektronische berichten standaard (EBV) van Justitie en stuurt het EBV bericht terug naar Jubes;
5. Jubes verstuurt het bericht naar de Justitiepartij via Justitienet.

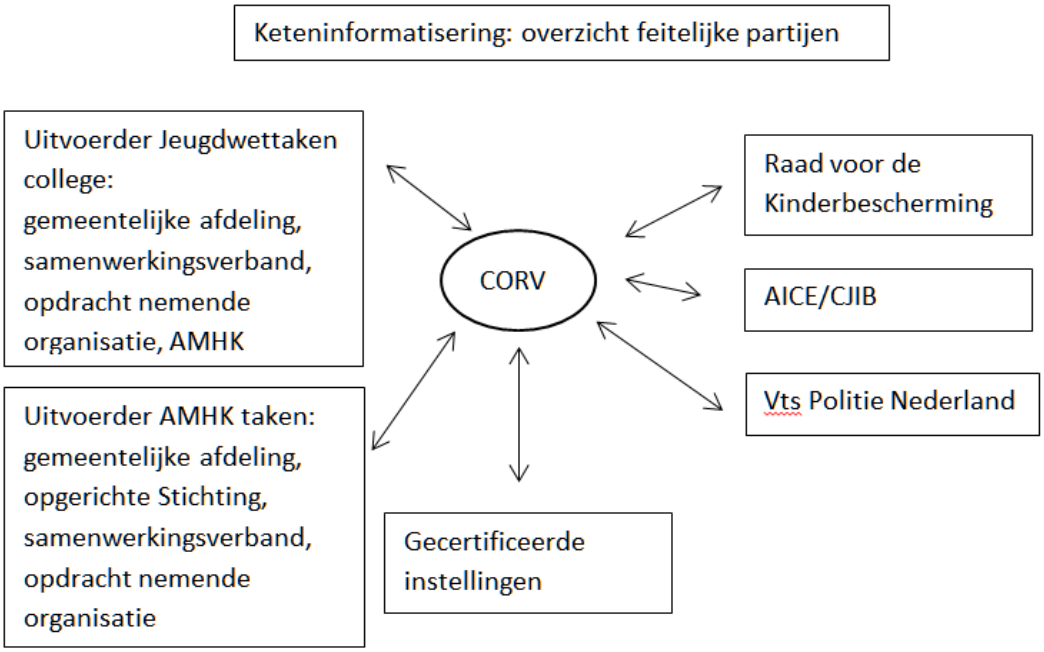
Justitiepartijen naar gemeentelijke partijen

Berichten vanuit justitiepartijen naar gemeenten volgen de omgekeerde weg en lopen als volgt.

1. Via justitienet komt het bericht van een justitiepartij of gecertificeerde instelling aan op Jubes. Deze berichten zijn opgesteld conform de elektronische berichten standaard (EBV) van Justitie) of de Jeugdzorg XML-standaard;
2. Jubes stuurt het bericht vervolgens naar de Justitie Service Interface JSI CORV;
3. De JSI CORV transformeert het bericht van de elektronische berichten standaard (EBV) van Justitie naar het gemeentelijke Standaard Uitvoerings Formaat (StUF) en stuurt het StUF bericht terug naar Jubes;
4. Jubes stuurt het bericht vervolgens naar de CORV gateway;
5. De CORV gateway verstuurt het bericht naar de gemeentelijke partij via internet (SSL-beveiligd).

Zowel de CORV gateway, Jubes, als de JSI CORV staan in de beveiligde omgeving van Jubit. Jubit is daarbij een fysiek en logisch beveiligde omgeving (donkerblauw in bovenstaande figuur).

Uiteraard staan de in paragraaf 4.1 beschreven juridische partijen in juridische zin ook centraal bij het gebruik van en het aansluiten op de CORV. In de praktijk zullen de feitelijke werkzaamheden echter niet (altijd) door de betrokken juridische partijen zelf uitgevoerd worden. Zo hebben gemeenten onder de Jeugdwet de vrijheid om taken zelf uit te laten voeren door een gemeentelijke afdeling, uit te laten voeren door een wijkteam of de uitvoering van werkzaamheden uit te besteden aan een (externe) partij. Ook zal samenwerking tussen verschillende gemeenten plaatsvinden. In het kader van berichten over door de rechter of de officier van justitie opgelegde jeugdreclassering, draagt het Administratie- en Informatie Centrum voor de Executieketen (AICE), ondergebracht bij het Centraal Justitieel Incassobureau (CJIB), zorg voor de uitvoering van de werkzaamheden. Voor wat de politie betreft zal de aansluiting op de CORV niet plaatsvinden door de verschillende politieonderdelen, maar zal vts Politie Nederland als centrale (ICT) organisatie aansluiting op de CORV realiseren. Onderstaand overzicht geeft aan met welke organisaties of samenwerkingsverbanden die de werkzaamheden uitvoeren, de CORV geconfronteerd kan worden. Vooral voor wat de werkzaamheden van gemeenten betreft, is een groot aantal diverse aansluitende partijen mogelijk. Voor een goede werking van de CORV is daarbij echter wel noodzakelijk, dat duidelijk is voor welke juridische partij (bijvoorbeeld voor welke gemeenten) een bepaalde partij die de werkzaamheden uitvoert optreedt en bevoegd is om berichten te verzenden en te ontvangen.

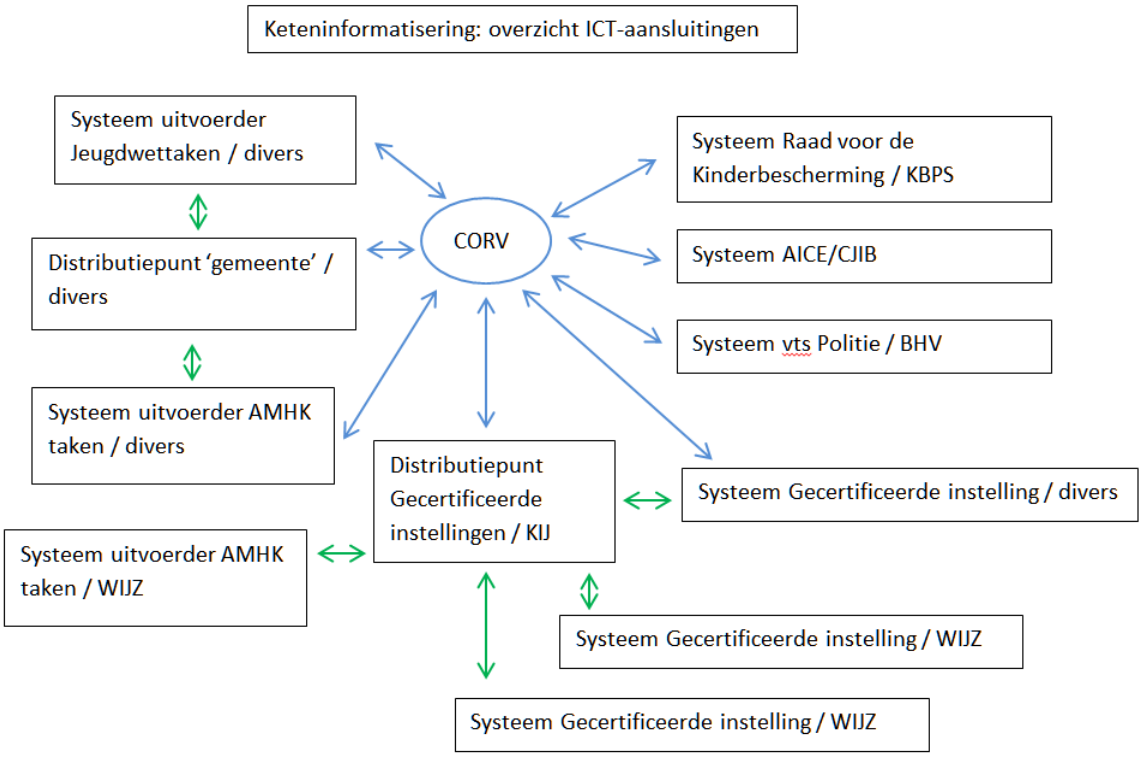


Omdat het aansluiten op de CORV technisch gezien neerkomt op het aansluiten van een 'postbus' van de organisatie die de feitelijke werkzaamheden uitvoert, is ook van belang welke 'postbussen' daarbij gebruikt worden. Bij de 'postbussen' die in technische zin op de CORV aangesloten worden, zijn twee typen te onderscheiden:

- de 'postbussen' die technisch gezien onderdeel uitmaken van de ICT die voor de uitvoering van de taken en werkzaamheden gebruikt wordt, en
- de 'postbussen' van zogenaamde distributiesystemen die voor meerdere partijen gebruikt worden of die gebruikt worden voor meerdere soorten berichten.

De verwachting is dat vooral gemeenten, de AMHK's en de gecertificeerde instelling als 'postbus' voor CORV berichten gebruik zullen maken van distributiesystemen. Daarbij kan er sprake zijn van een diversiteit aan systemen en ook kan er sprake zijn van de situatie dat 'postbussen' en distributiesystemen aangeboden en beheerd worden door externe partijen c.q. door partijen die niet belast zijn met de feitelijke (inhoudelijke) uitvoering van de werkzaamheden. Een voorbeeld van een distributiesysteem is de zogenaamde KIJ. De KIJ wordt thans ten behoeve van de BJZ en gecertificeerde instelling ontwikkeld als distributie-postbus voor instellingen die gebruik zullen maken van het systeem WIJZ. Het systeem WIJZ wordt thans onder meer ontwikkeld voor de uitvoering van de taken en werkzaamheden van de toekomstige gecertificeerde instellingen en AMHK's.
Voor een goede werking van de CORV is daarbij echter wel noodzakelijk, dat duidelijk is voor welke juridische partij (bijvoorbeeld voor welke gemeenten) en voor welke feitelijke uitvoerder een bepaalde 'postbus' zal fungeren.

In onderstaand overzicht is aangegeven met welke verschillende ‘postbussen’ en distributiepunten voor berichten de CORV geconfronteerd kan worden. De blauwe pijlen geven daarbij de communicatie tussen de CORV en de ‘postbussen’ weer. Deze behoren tot de ontwikkeling en werking van de CORV. De groene pijlen geven de verdere routering van berichten aan “achter” de verschillende distributiepunten van de verzenders en ontvangers. Deze communicatie behoort niet tot de ontwikkeling en werking van de CORV. Voor de communicatie die weergegeven wordt door de groene pijlen zijn de verzendende en ontvangende partijen zelf verantwoordelijk.



Er is een grote variëteit aan partijen die feitelijk de taken en werkzaamheden ten behoeve van de juridische partijen kunnen uitvoeren. De technische aansluiting op verschillende soorten postbussen kan ook door een grote variëteit van partijen gedaan worden en zelfs door niet-uitvoerende partijen beheerd worden. Vanwege deze complexiteit worden in deze PIA ten aanzien van het (technisch) aansluiten op de CORV en de daarbij te hanteren procedure en aansluitvoorwaarden een aantal aanbevelingen gedaan. Deze zijn opgenomen in paragraaf 4.6. Hierbij dient opgemerkt te worden dat binnen het Deelproject justitiële keteninformatisering reeds aansluitprocedures, aansluitformulieren en aansluitvoorwaarden ontwikkeld zijn die rekening houden met de grote variëteit in postbussen waarmee de CORV geconfronteerd zal worden.

4.4 Toepasselijkheid Wbp en persoonsgegevens bij de werking van de CORV

Alhoewel er bij de CORV geen inhoudelijke verwerkingen of bewerkingen van persoonsgegevens plaatsvinden, is er ook bij de werking van de CORV sprake van persoonsgegevens en dient voor de CORV een Wbp-verantwoordelijke aangewezen te (kunnen) worden. Hierbij spelen de volgende overwegingen een rol.

Als eerste dient de CORV te zorgen voor een juiste en veilige verzending van de berichten en de daarin opgenomen persoonsgegevens. Feitelijk gezien 'gaan de persoonsgegevens door de infrastructuur'. In die zin moet er sprake zijn van een afdoende informatiebeveiliging als bedoeld in artikel 13 Wbp. Inhoudelijk is er dan weliswaar geen bemoeienis met de persoonsgegevens, maar dat is bijvoorbeeld hetzelfde bij externe hosting van hardware. Een partij die dergelijke hosting doet, is een bewerker voor de verantwoordelijke (vooral gericht op informatiebeveiliging) omdat er nu eenmaal persoonsgegevens "in de hardware vastgelegd zijn".
Als tweede is er bij de CORV sprake van het vastleggen van verkeersgegevens en foutberichten. Bij foutberichten inclusief het oorspronkelijke bericht is er (zelfstandige) opslag van persoonsgegevens. Maar ook als verkeersgegevens of foutberichten enkel "meta-" of uitwendige gegevens over een bericht bevatten (bijv. wie welk bericht op welk moment aan wie verzonden heeft of bij welk bericht van wie aan wie het fout ging), zal het met die uitwendige gegevens (verzender, ontvanger, tijdstip bericht en aanduiding, bijvoorbeeld code, van het bericht) vrij eenvoudig zijn om met behulp van de verzender of de ontvanger de inhoud van het bericht te achterhalen. En, los van de vraag of men dat achterhalen ook daadwerkelijk doet, volgens de brede opvatting van persoonsgegevens gaat het ook bij dergelijke verkeersgegevens en foutberichten om persoonsgegevens omdat er sprake is van indirect identificeerbare gegevens (met behulp van informatie van bijvoorbeeld de verzender of de ontvanger te identificeren personen). Dat er sprake is van persoonsgegevens omdat de personen met behulp van informatie van andere partijen te achterhalen zijn, was bijvoorbeeld een belangrijk issue bij alle onderzoeken die het Cbp deed naar de verwerking van persoonsgegevens bij de OV-chipcard.
Als derde zijn er andere factoren die een rol spelen. Zoals bijvoorbeeld de regels over het melden van datalekken die opgenomen zijn in het wetsvoorstel 33 662 over gebruik meldplicht datalekken. Als berichten binnen CORV of justitienet kwijtraken, onverhoopt verkeerd verzonden worden of onverhoopt afgetapt worden, kan er sprake zijn van een datalek dat in de toekomst gemeld moet worden aan het Cbp. Een dergelijke melding moet dan gedaan worden door de Wbp-verantwoordelijke. Ook komt voor dat de Wbp-verantwoordelijke bij infrastructuren wettelijk wordt aangewezen. Dat is bijvoorbeeld zo bij de verwijsindex risicojongeren (VIR) en het SUWI-netwerk. En ook in het concept wetsvoorstel Wet herziening tenuitvoerlegging
strafrechtelijke beslissingen is er sprake van het wettelijk aanwijzen van de Wbp-verantwoordelijke. In artikel 6:1:10, lid 2, (567, 568, 572a Sv; nieuw) wordt de Minister van VenJ aangewezen als de verantwoordelijke (Wbp) voor de gegevensverwerking, waaronder ook het verstrekken van gegevens.

4.5 Wat is de justitiële keteninformatisering niet

Voor een juiste positionering en beoordeling van de justitiële keteninformatisering, de berichten en de werking van de CORV, kan ook aangegeven worden om welke vorm van samenwerking tussen ketenpartners en gegevensuitwisseling het niet gaat.
Er zijn binnen het justitiële domein en bij de toekomstige uitvoering van de Jeugdwet verschillende soorten samenwerking.

Gegevensuitwisseling niet met CORV

Zo valt aan de ene kant te denken aan onder andere veiligheidshuizen en casus overleggen. Bij dergelijke vormen van samenwerking is er gegevensuitwisseling in het kader van en ten behoeve van de uitvoering van werkzaamheden binnen een bepaalde fase van een geheel proces van werkzaamheden. Een voorbeeld bij de toekomstige uitvoering van de Jeugdwet zijn ook de voorziene wijkteams waarbinnen in bepaalde gevallen door verschillende organisaties samengewerkt wordt bij de uitvoering van bepaalde taken zoals de toeleiding naar jeugdhulp. Bij deze vormen van samenwerking worden gegevens verwerkt om werkzaamheden uit te voeren en om tot een (eind)resultaat van die werkzaamheden te komen. Bij samenwerking in het kader van casus overleggen kan gedacht worden aan een advies of plan van aanpak in een concreet geval. Ook kan een casusoverleg aanleiding geven om een verzoek tot onderzoek aan de Raad voor de Kinderbescherming te doen. De uitwisseling van gegevens bij bijvoorbeeld casus overleggen is sterk afhankelijk van de situatie en niet op voorhand vorm te geven in vooraf gedefinieerde berichten. Vooral bij dergelijke vromen van samenwerking spelen privacy vragen over de rechtmatigheid van gegevensuitwisseling en doelbinding. De berichten en het gebruik van de CORV zien uitdrukkelijk niet op dergelijke vormen van samenwerking en gegevensdeling binnen dergelijke samenwerkingsvormen.

Berichten wel met CORV

Aan de andere kant is er bij ketensamenwerking de overgang van werkzaamheden tussen verschillende fasen en/of organisaties. Daarbij wordt het (eind)resultaat van een bepaalde fase door de ene ketenpartner als het ware overgedragen aan een andere ketenpartner die belast is met taken en werkzaamheden in een volgende fase van de gehele keten. Bij de formele berichten die met gebruik van de CORV verzonden worden gaat het om berichten die door de verzender verstuurd worden als het sluitstuk van bepaalde werkzaamheden van de verzender. Voor de ontvanger van berichten zijn de berichten juist het startpunt voor het uitvoeren van de taken en werkzaamheden. In dergelijke situaties is er in het bijzonder spraken van het samen werken van verschillende partijen die ieder voor zich een (afzonderlijke) fase voor hun rekening nemen.

Bij de uitvoering van de Jeugdwet kunnen verschillende fasen onderscheiden worden. Het gaat daarbij, in algemene zin, om de volgende fasen:

- de fase waarbij meldingen of aanvragen gedaan worden. Bij politiemeldingen (zorgmeldingen) en verzoeken tot onderzoek (VTO) aan de Raad voor de

kinderbescherming gaat het om documenten in het kader van een melding c.q. een aanvraag. De berichten die via de CORV verzonden worden vormen het startpunt voor de ontvangende partij.

- de fase waarin aan de hand van meldingen of verzoeken bezien wordt welke voorzieningen of maatregelen aangewezen zijn en de beslissingen over maatregelen zelf. De berichten over het vervolg dat door de Raad voor de Kinderbescherming aan een verzoek tot onderzoek gegeven wordt en de berichten over beslissingen met betrekking tot het opleggen van kinderbeschermingsmaatregelen en jeugdreclassering behoren hiertoe.

- de fase van uitvoering van jeugdhulp en kinderbeschermingsmaatregelen en jeugdreclassering. De berichten over beslissingen over het opleggen van kinderbeschermingsmaatregelen en jeugdreclassering vormen voor gecertificeerde instellingen het startpunt voor de uitvoering van die maatregelen.

- de fase die betrekking heeft op financiële aspecten. Specifiek voor deze fase worden via de CORV geen afzonderlijke berichten verzonden. Er zijn ook geen CORV-berichten met betrekking tot bijvoorbeeld beleids- en managementinformatie.

Hieronder is een overzicht opgenomen van de verschillende fasen en de berichten die bij gebruik van de CORV bij de verschillende overgangsmomenten betreffen.
De positionering van de CORV berichten is aangegeven met

Intern proces ketenpartner(s) (werkzaamheden die leiden tot een resultaat)	**Overgang van werkzaamheden** (formeel bericht)
Informatieuitwisseling bij Samenwerking niet met CORV	*Informatieverstrekking bij Samen Werken*
a) Melding / aanvraag doen	Melding / signaal
	Verzoek / aanvraag
b) Beoordelen en beslissen n.a.v. een melding of aanvraag	Doorverwijzing
	Inbreng in casusoverleg
	Genomen besluit
	Mededeling over besluit
c) Uitvoeren van de beslissing	Opdracht tot uitvoering
	Bevestiging uitvoering
	Plan van Aanpak
	Behandelplan
	Tussentijdse evaluatie
e) Financieel	Contract / opdracht
	Facturering / Subsidiebetaling

4.6 Algemene bevindingen over de justitiële keteninformatisering en de CORV

Een beoordeling van de risico's in verband met de privacy van betrokkenen (jeugdigen), de gegevensverwerking bij de justitiële ketenberichten en het gebruik van de CORV vindt niet plaats in het 'luchtledige'. Aan de ene kant spelen privacy aspecten en een zorgvuldige gegevensbescherming in het belang van de jeugdogen over wie persoonsgegevens verwerkt worden. Aan de andere kant speelt het belang van de berichten en het verzenden van de berichten met behulp van de CORV voor een goede uitvoering van de Jeugdwet en het doel dat alle kinderen gezond en veilig opgroeien, hun talenten ontwikkelen en meedoen in de samenleving naar vermogen. Gebaseerd op dit doel van de Jeugdwet kunnen over de justitiële ketenberichten en de CORV een aantal algemene bevinden vermeld worden.

Algemene bevindingen t.a.v. de justitiële keteninformatisering en de CORV
Bevinding 1: uitgangspunt bij de justitiële keteninformatisering is dat de ketensamenwerking tussen de verschillende betrokken partijen eenduidige afspraken over de informatie-uitwisseling vereist. Als alle betrokken partijen separaat onderlinge afspraken over gegevensuitwisseling maken leidt dit tot extra administratieve lasten, minder overzicht, mogelijke rechtsongelijkheid bij bijvoorbeeld verzoeken tot onderzoek aan de RvdK, en meer kans op vertraging en fouten in de uitvoering. Tevens zal een goede informatiebeveiliging bij allerlei verschillende en afwijkende afspraken en methoden om gegevens te verzenden onder druk komen te staan. Bevinding 2: bij de justitiële keteninformatisering gaat het om formele berichten tussen justitiepartijen, het gemeentelijke domein en de gecertificeerde instellingen. De berichten hebben betrekking op jeugdbescherming (kinderbeschermingsmaatregelen), jeugdreclassering en zorgmeldingen door de politie. Met de term 'formeel' wordt aangegeven dat de berichten door de verzender verstuurd worden als het sluitstuk van bepaalde werkzaamheden van de verzender. Voor de ontvanger van berichten zijn de berichten juist het startpunt voor het uitvoeren van de taken en werkzaamheden. Bevinding 3: verzekerd dient te worden dat de overdracht van informatie op momenten waarbij de werkzaamheden van de verzendende partij als het ware beëindigen en vervolgens voorgezet dienen te worden door de ontvangende partij, juist, accuraat en snel plaatsvindt. Zonder een adequate informatieverstrekking van verzender aan ontvanger zou de keten c.q. het proces, van jeugdbescherming, de uitvoering van jeugdreclassering en het behandelen van zorgmeldingen gedaan door de politie onnodige vertraging op kunnen lopen en zelfs stil kunnen vallen. Bevinding 4: omdat het essentieel is dat op de momenten waarbij de werkzaamheden van de ene ketenpartner overgenomen worden door de andere ketenpartners, de informatieverstrekking juist, accuraat en snel plaatsvindt, wordt een (nieuwe) voorziening ontwikkeld en ingericht: . de Collectieve Opdracht Routeer Voorziening (CORV)

Bevinding 5: het gebruik van de CORV is cruciaal voor een efficiënte en effectieve berichten-uitwisseling tussen betrokken partijen bij een goede uitvoering van de Jeugdwet. Als voor de 'formele' justitiële ketenberichten allerlei verschillende berichtenstromen tussen de ketenpartners zouden ontstaan, kan dit onnodige risico's voor privacy, doelbinding bij gegevensverwerking en informatiebeveiliging met zich mee zal brengen.

Deze 5 bevindingen geven samengevat het belang van de CORV en de berichten aan. In die zin geven de bevindingen ook dat dat het aangewezen is om de berichten die met de CORV verzonden worden ook na 1 januari 2015 uit te breiden. Hierbij valt bijvoorbeeld te denken aan berichten over verlenging van jeugdbeschermingsmaatregelen, terugmeldingen bij politiemeldingen en berichten over jeugdreclassering opgelegd door justitiële jeugdinrichtingen etc.

Zoals in paragraaf 4.3 al is aangegeven, kunnen in verband met de grote diversiteit van aanvragers voor een aansluiting op de CORV, een aantal uitgangspunten geformuleerd worden. Deze uitgangspunten zijn verwerkt in de thans ontwikkelde aansluitprocedure en worden opgenomen in de nadere regelgeving.

De uitgangspunten zijn:

- duidelijk dient te zijn voor welke juridische partijen (en voor welke feitelijke partijen) een aansluiting op de CORV plaatsvindt;
- als een bepaalde organisatie (feitelijke partij) een aanvraag doet voor aansluiting op de CORV voor meerdere organisaties (juridische partijen), dient daarbij duidelijk te zijn voor welke organisaties (juridische partijen) dat is. Een voorbeeld is een AMHK die als feitelijke partij voor meerdere gemeenten (juridische partijen) in een regio politiemeldingen ontvangt. Dan moet duidelijk zijn voor welke gemeenten dat is. Een ander voorbeeld is de aansluiting op de CORV van KIJ (het distributiepunt voor de organisaties/gecertificeerde instellingen die het systeem WIJZ gaan gebruiken);
- als een bepaalde organisatie een aanvraag doet voor aansluiting op de CORV voor meerdere verschillende taken, dan dient ook dit duidelijk te zijn. Zo kan een AMHK als juridische partij een aansluiting aanvragen voor het ontvangen van de AMHK-meldingen als bedoeld in de Wmo (kindermishandeling en huiselijk geweld) en tevens als feitelijke partij voor het ontvangen van Jeugdwet-zorgmeldingen (geen kindermishandeling/huiselijk geweld) die tot het gemeentelijk domein van de toeleiding behoren;
- het stellen van aansluitvoorwaarden verdient een wettelijke regeling die opgenomen wordt in een ministeriele regeling ter uitwerking van artikel 7.3.11, lid 4, van de Jeugdwet.

5 DEEL II DE RISICO BEOORDELING VAN DE JUSTITIËLE KETENINFORMATISERING

5 De Berichten

5.1 Overzicht

In dit eerste deel van de risicobeoordeling wordt aandacht besteed aan:

- de positionering van de gegevensuitwisseling bij samenwerking (5.2);
- de zeggenschap over de berichten en de inhoud (5.3);
- de rechtvaardiging van de berichten en de inhoud (5.4).

5.2 De positionering van de gegevensuitwisseling bij samenwerking

In paragraaf 4.5 is aangegeven dat formele berichten die met gebruik van de CORV verzonden worden als het ware het sluitstuk zijn van bepaalde werkzaamheden van de verzender. Voor de ontvanger van berichten zijn de berichten juist het startpunt voor het uitvoeren van de taken en werkzaamheden. De berichten dienen dan ook gepositioneerd te worden bij de overgang van werkzaamheden. Uiteraard zijn daar privacy risico's aan verbonden, maar deze zijn beperkter dan bij gegevensuitwisseling ten behoeve van het uitvoeren een proces van een ketenpartner, zoals bijvoorbeeld de gegevensuitwisseling bij casus overleggen.
De positionering van de CORV berichten is aangegeven met

Intern proces ketenpartner(s) (werkzaamheden die leiden tot een resultaat)	**Overgang van werkzaamheden** (formeel bericht)
Informatieuitwisseling bij Samenwerking	*Informatieverstrekking bij Samen Werken*

a) Melding / aanvraag doen	Melding / signaal
	Verzoek / aanvraag
b) Beoordelen en beslissen n.a.v. een melding of aanvraag	Doorverwijzing
	Inbreng in casusoverleg
	Genomen besluit
	Mededeling over besluit
c) Uitvoeren van de beslissing	Opdracht tot uitvoering
	Bevestiging uitvoering
	Plan van Aanpak
	Behandelplan
	Tussentijdse evaluatie

e) Financieel	Contract / opdracht
	Facturering / Subsidiebetaling

5.3 De zeggenschap over de berichten en de inhoud

5.3.1 De berichten

Uitgangspunt is dat alle berichten die met gebruik van de CORV verzonden worden, wettelijk geregeld worden. Dit wettelijk regelen is vooral van belang als specifieke geheimhoudingsverplichtingen een rol spelen.

Een nadere regeling over de berichten is voorzien in artikel 7.3.11, lid 4, van de Jeugdwet. Hieronder is met arcering aangegeven welk deel van dit artikel van belang is voor de berichten en die in deze PIA aan de orde komen.

> Artikel 7.3.11 Jeugdwet
>
> 4. Bij regeling van Onze Minister van Volksgezondheid, Welzijn en Sport, voor zover nodig in overeenstemming met Onze Minister van Veiligheid en Justitie, *kunnen regels worden gesteld omtrent* de inhoud van het dossier en *de wijze waarop* de verwerking van gegevens *door* en *de uitwisseling van gegevens tussen het college, de jeugdhulpaanbieders, de gecertificeerde instellingen en de raad voor de kinderbescherming plaatsvindt*. Daarbij kan worden bepaald welke maatregelen moeten worden getroffen om te waarborgen dat de uitwisseling van gegevens veilig en zorgvuldig plaatsvindt.

Artikel 7.3.11, lid 4, Jeugdwet biedt echter geen basis voor berichten over door de strafrechter of de officier van justitie opgelegde jeugdreclassering.
Op dit moment is het Openbaar ministerie belast met de tenuitvoerlegging van rechterlijke beslissingen en strafbeschikkingen (art. 553 en art 572 Wetboek van Strafvordering). In de (nabije) toekomst zal de Minister van VenJ belast worden met de tenuitvoerlegging van rechterlijke beslissingen en strafbeschikkingen (artikel 6:1:1, lid 1, van het conceptwetsvoorstel Wet herziening tenuitvoerlegging strafrechtelijke beslissingen, consultatieversie van 4 november 2013). In het kader van berichten over door de rechter of de officier van justitie opgelegde jeugdreclassering, draagt het Administratie- en Informatie Centrum voor de Executieketen (AICE), ondergebracht bij het Centraal Justitieel Incassobureau (CJIB), zorg voor de uitvoering van de werkzaamheden.
Thans kunnen berichten betreffende jeugdreclassering door het Openbaar ministerie op basis van artikel 39e, lid 1, onder g, van de Wet justitiële en strafvorderlijke gegevens en op basis van de nieuwe artikelen 11aa en 17 van het Besluit justitiële en strafvorderlijke gegevens verzonden worden. In de toekomst zullen de berichten namens de Minister van VenJ verzonden worden op basis van het nieuwe artikel 6:1:10, lid 2 (567, 568, 572a Sv; nieuw) van het voorstel voor de Wet herziening tenuitvoerlegging strafrechtelijke beslissingen en op basis van de nieuwe artikelen 11aa en 17 van het Besluit justitiële en strafvorderlijke gegevens.

Artikel 7.3.11, lid 4, Jeugdwet biedt ook geen basis voor het regelen van berichten door de politie betreffende meldingen over jeugdigen. Voor wat de meldingen door de politie betreft zal artikel 4.2 van het Besluit politiegegevens aangepast worden in verband met de nieuwe Jeugdwet.

Het gebruik van het burgerservicenummer (BSN) bij de berichten geschiedt overeenkomstig artikel 7.2.1 Jeugdwet, artikel 5.2.9 Wmo 2015 of artikel 27b Wetboek van strafvordering. Het gebruik van het strafrechtketennummer (SKN) geschiedt overeenkomstig artikel 27b Wetboek van Strafvordering.

Door de berichten als hierboven is aangegeven wettelijk te regelen is het risico op onrechtmatige verstrekking van gegevens in algemene zin laag. Zie in dit verband ook de aanbevelingen in paragraaf 5.4.

Onderwerp	Risico's		
	laag	midden	hoog
Het bestaan van een specifiek bericht in relatie tot de taak waarvoor berichten verzonden en ontvangen worden	wettelijk bepaald	Deels wettelijk bepaald, deels in te vullen door de gebruikers	Geheel in te vullen door de gebruikers

5.3.2 De inhoud van berichten

Uitgangspunt is dat alle berichten die met gebruik van de CORV verzonden worden, wettelijk geregeld worden. Daarbij geldt hetzelfde als hierboven bij 5.3.1 is aangegeven. Om die reden is het risico in algemene zin laag. Omdat er bij enkele berichten, vooral verzoeken tot onderzoek aan de Raad voor de Kinderbescherming en bij meldingen door de politie sprake is van niet vooraf volledig te definiëren gegevens en er sprake kan zijn van het bijvoegen van bestanden, kan daarvoor het risico gesteld worden op "midden". Omdat gegevens in verband met een verzoek tot onderzoek en een melding door de politie niet op voorhand nauwkeurig zijn aan te geven (hangt af van de omstandigheden) en omdat er daarbij wel sprake zal zijn van professioneel handelen, is er geen aanleiding tot een extra aanbeveling op dit punt. Zie in dit verband ook paragraaf 5.4.

Onderwerp	Risico's		
	laag	midden	hoog
De inhoud van een bericht in relatie tot de taak waarvoor berichten verzonden en ontvangen worden en de mogelijkheden voor eigen inhoudelijke vulling van bericht	wettelijk bepaald	Deels wettelijk bepaald, deels in te vullen door de gebruikers *(berichten met vrije velden of bijvoegen bestanden)*	Geheel in te vullen door de gebruikers

5.3.3 Beheersbaarheid

Uitgangspunt is dat alle berichten die met gebruik van de CORV verzonden worden, wettelijk geregeld worden. Dit geldt uiteraard ook voor aanpassing of aanvulling van de berichten in de toekomst. Het is van belang dat deze (inhoudelijke) governance over de berichten duidelijk belegd wordt. Hetzelfde geldt voor eventuele aanvulling van de PIA bij wijzigingen. Zie in dit verband paragraaf 5.4 en de daar opgenomen aanbevelingen. Hierdoor is er sprake van een laag risico t.a.v. de beheersbaarheid van de berichten. In 2015 wordt een review uitgevoerd op de berichten. Door dit in het eerste jaar van het operationeel zijn van het nieuwe stelsel uit te voeren, kan direct bijgestuurd worden indien dit aangewezen is. In verband met deze review kan ook gewezen worden op de uitbreiding van berichten zoals aangegeven is in paragraaf 4.6.

Onderwerp	Risico's		
	laag	midden	hoog
De beheersbaarheid van de berichten (governance t.a.v nieuwe berichten)	wettelijk bepaald	Deels wettelijk bepaald, deels in te vullen door de gebruikers	Niet duidelijk bepaald Geheel in te vullen door de gebruikers

5.4 De rechtvaardiging van de berichten en de inhoud en Het berichtenboek

Het feit dat het verzenden van berichten en de inhoud van de berichten wettelijk geregeld wordt, geeft op zich nog niet aan of de persoonsgegevens die in de berichten opgenomen worden ook daadwerkelijk noodzakelijk zijn voor de ontvanger. Zo zal bij de omschrijving en invulling van vooral de inhoud van de berichten nadrukkelijk bezien dienen te worden of en welke gegevens inderdaad noodzakelijk zijn voor de ontvanger.

Er iseen groot aantal (concept) documenten beschikbaar die de verschillende berichten beschrijven. Zoals in paragraaf 4.2.1 al is aangegeven, gaat het om:

- Het rapport *Stelselherziening Jeugdbescherming* van de Justitiële Informatiedienst van april 2014;
- Het rapport *Ketenproces Jeugdreclassering* van de Justitiële Informatiedienst van 13 juni 2014.

Daarnaast kan ook gewezen worden op de in Bijlage 2 opgenomen overzichten over berichten aan de gemeenten.

Bevindingen t.a.v. de berichten en de inhoud van de berichten
Bevinding 6: een eerste beoordeling van de berichten die beschreven zijn in het rapport Stelselherziening Jeugdbescherming van de Justitiële Informatiedienst van april 2014, het rapport Ketenproces Jeugdreclassering van de Justitiële Informatiedienst van 13 juni 2014 en Bijlage 2 levert geen berichten op waarbij sprake is van niet toegestane verstrekking

van gegevens omdat er voor de berichten zelf geen voldoende wettelijke basis zou zijn. Hetzelfde geldt voor de berichten die per 1 januari 2015 verzonden zullen worden en die beschreven worden in de (komende) ministeriële regeling.

Bevinding 7: voor wat de inhoud van de berichten betreft, bieden de genoemde rapporten geen nauwkeuring inzicht in de persoonsgegevens per bericht. Bijlage 2 geeft wel een aanduiding van de inhoud van de berichten. In Bijlage 2 zijn geen berichten opgenomen waarbij de inhoud van het bericht (de persoonsgegevens) aangemerkt zou dienen te worden als niet voldoende noodzakelijk. Hetzelfde geldt voor de berichten die per 1 januari 2015 verzonden zullen worden en die beschreven worden in de (komende) ministeriële regeling. Daarbij blijkt uit de diverse projectdocumenten dat beperking van de te verstrekken gegevens tot de noodzakelijke gegevens en een goede wettelijke onderbouwing van de te verstrekken persoonsgegevens leidend zijn bij de ontwikkeling van berichten betreffende kinderbescherming en jeugdreclassering.

Voor een volledig overzicht en beschrijving van alle te verzenden berichten, de inhoud van de berichten en de zeggenschap over de inhoud van die berichten, worden hieronder een aantal aanbevelingen gedaan.

Aanbevelingen t.a.v. de wettelijke regeling over de te verzenden berichten (5.3.1), de inhoud van de berichten (5.3.2), de zeggenschap (5.3.3) en een beoordeling van de noodzakelijk van de te verstrekken gegevens (5.4)

Aanbeveling 1: Aanbevolen wordt om op basis van de reeds bestaande documenten over de berichten een Berichtenboek op te stellen. Daarmee kan bereikt worden dat alle informatie over alle berichten samengebracht wordt in één document. In onderstaand voorstel voor een dergelijk berichtenboek wordt als basis daarvoor uitgegaan van:

- Het rapport *Stelselherziening Jeugdbescherming* van de Justitiële Informatiedienst van april 2014;
- Het rapport *Ketenproces Jeugdreclassering* van de Justitiële Informatiedienst van 13 juni 2014;
- Bijlage 2;
- de berichten per 1 januari 2015 zoals deze geregeld zullen worden in de ministeriële regeling;
- de reeds ontworpen berichten die door de executieverantwoordelijke bij jeugdreclassering verzonden worden;
- de zorgmeldingen die door de politie verzonden worden.

Voor wat het Berichtenboek betreft, wordt het volgende voorgesteld.

A) Het berichtenboek zodanig vorm te geven en te redigeren dat:

A1) Aandacht besteed wordt aan de berichten tussen en door het college, waaronder het AMHK, de gecertificeerde instellingen en de raad voor de kinderbescherming betreffende VTO's, kinderbeschermingsmaatregelen, jeugdreclassering, vrijwillige begeleiding en (doorzenden van) meldingen gedaan door de politie of door het college, waaronder het AMHK aan bijvoorbeeld de politie over het vervolg op een van de politie ontvangen melding;

A2) Aandacht besteed wordt aan de berichten over jeugdreclassering die door AICE verzonden zullen worden namens het Openbaar ministerie op basis van artikel 39e, lid 1, onder g, van de Wet justitiële en strafvorderlijke gegevens en op basis van de nieuwe artikelen 11aa en 17 van het Besluit justitiële en strafvorderlijke gegevens. In de toekomst zullen de berichten namens de Minister van VenJ verzonden worden op basis van het nieuwe artikel 6:1:10, lid 2 (567, 568, 572a Sv; nieuw) van het voorstel voor de Wet herziening tenuitvoerlegging strafrechtelijke beslissingen en op basis van de nieuwe artikelen 11aa en 17 van het Besluit justitiële en strafvorderlijke gegevens.

A3) Aandacht besteed wordt aan de (zorg)meldingen door de politie op basis van het nieuwe artikel 4:2, eerste lid, van het Besluit politiegegevens.

B) Bij de indeling van het berichtenboek een drietal indelingsprincipes te hanteren.

B1) In het berichtenboek een onderverdeling te maken in:
- berichten betreffende jeugdbescherming;
- berichten betreffende jeugdreclassering;
- berichten betreffende meldingen door de politie.

B2) Bij de verschillende soorten berichten een onderdeel op te nemen dat een beschrijving geeft van de werking van jeugdbescherming, jeugdreclassering , de AMHK, respectievelijk de meldingen door de politie. Een dergelijke beschrijving geeft inzicht in de verschillende processen, de rol die verschillende partijen hebben en de taken en werkzaamheden die verschillende partijen uitvoeren. Ook de verschillende zogenaamde 'praatplaten' die reeds door het projectteam opgesteld zijn, kunnen daarbij een toegevoegde waarde hebben.

B3) Een onderscheid aan te brengen tussen enerzijds de primaire inhoudelijke berichten (Dé ketenberichten) en anderzijds de secundaire (afgeleide) retourberichten en foutmeldingen.

C) Bij de beschrijving van de berichten ook aandacht te besteden aan de volgende aspecten.

C1) De juridische basis voor zowel de verzender als de ontvanger waarop de berichten gebaseerd zijn te vermelden. Zie hierbij paragraaf 4.1 voor de taken van de betrokken partijen en paragraaf 5.3.1 voor de meer specifieke juridische grondslag van de berichten.

C2) Bij de verzender van berichten de volgende uitgangspunten te hanteren:
- De politie is de verzender van meldingen aan gemeenten en/of de AMHK's
- De gemeenten, gecertificeerde instellingen en de AMHK's zijn de verzenders van VTO's;
- De RvdK is de verzender van alle berichten betreffende kinderbeschermingsmaatregelen (uitgezonderd de VTO's, maar inclusief de beslissingen van de rechter);
- AICE is namens het Openbaar ministerie (en in de toekomst namens de Minister van VenJ) de verzender van berichten betreffende jeugdreclassering opgelegd door de jeugdstrafrechter of door het Openbaar Ministerie;
- De RvdK is de verzender van door de RvdK in het vrijwillig kader aangewezen toezicht en begeleiding als vorm van jeugdreclassering.

C3) De in een bericht opgenomen persoonsgegevens te vermelden. Zie hiervoor bijvoorbeeld Bijlage 2 en de komende ministeriële regeling.

6 De centrale berichteninfrastructuur (CORV)

6.1 Overzicht

In dit tweede deel van de risicobeoordeling wordt aandacht besteed aan:

- de werking en functies van de berichteninfrastructuur (6.2);
- de beheersbaarheid van de berichten infrastructuur (6.3).

6.2 De werking en functies van de berichteninfrastructuur (CORV)

6.2.1 Nauwkeurigheid adressering

Bij de adressering van de berichten wordt het OIN (overheids identificatienummer) gebruikt of een ander specifiek nummer voor bijvoorbeeld de gecertificeerde instellingen. Indien een beheerder van een aansluitpunt/distributiepunt werkzaamheden voor meerdere gemeenten of bijvoorbeeld AMHK's verricht, dient die bij de aansluiting aangegeven te worden. Daarnaast hebben alle berichten een eigen unieke codering. Deze vorm van adressering maakt het mogelijk om alle berichten, zonder dat distributiepunt kennis dient te nemen van de inhoud, bezorgd kan worden bij de juiste organisatie én bij het juiste organisatieonderdeel. Bij de adressering van de berichten is er daardoor een laag risico op verkeerde bezorging door de CORV.

Onderwerp	Risico's		
	laag	midden	hoog
Nauwkeurigheid adressering bericht	Specifieke inhoudelijke codering van het bericht	Domein-gerichte codering van het bericht	Geen inhoudelijke gerichte codering

6.2.2 Toegang tot gegevens van de verzender (inkijk)

De collectieve opdracht routeervoorziening (CORV) is een 'postkantoor ofwel -routeer' voorziening. De CORV ontvangt berichten van een verzender en stuurt deze door naar de ontvanger. Dit vindt, mede ter beveiliging en afscherming, plaats in een (volstrekt) afgesloten systeem zonder menselijke toegang. De CORV is er dan ook geen voorziening waarbij raadpleging van de gegevens bij de verzender (inkijk) door gebruikers/ontvangers mogelijk is. Daardoor is er een laag risico (n feite geen risico).

Onderwerp	Risico's		
	laag	midden	hoog
toegang tot de gegevens van de verzender (bijv. inkijk-functie)	geen	Gestructureerde toegang	'Vrije' toegang

6.2.3 Centrale gegevensopslag

De CORV wordt enkel gebruikt voor de routering van justitiële ketenberichten in het kader van de Jeugdwet. Dit vindt, mede ter beveiliging en afscherming, plaats in een (volstrekt) afgesloten systeem zonder menselijke toegang. De persoonsgegevens (in de berichten) worden niet opgeslagen. De gemiddelde verblijfsduur van persoonsgegevens in de JSI CORV zal enkele seconden bedragen in geval van gelijktijdige uitval van meerdere delen van het (redundant uitgevoerde) netwerk kan dit oplopen tot een aantal uur. Na afleveren van bericht is het bericht niet meer voor/in de CORV beschikbaar, maar enkel in het bronsysteem van de ontvanger. Door het ontbreken van centrale opslag van inhoudelijke berichten of gegevens, is er sprake van een laag risico (in feite geen risico).

Onderwerp	Risico's		
	laag	midden	hoog
Centrale gegevensopslag van berichten/gegevens met toegang	geen	Centrale opslag met gestructureerde bevraging	Centrale opslag met 'vrije' bevraging

6.2.4. Afslag van gegevens

De CORV wordt enkel gebruikt voor de routering van justitiële ketenberichten in het kader van de Jeugdwet. Dit vindt, mede ter beveiliging en afscherming, plaats in een (volstrekt) afgesloten systeem zonder menselijke toegang. Er is geen afslag van de berichten voor bijvoorbeeld het samenstellen van managementinformatie of voor beleidsinformatie. Er zijn overigens ook geen berichten voor de ontvangers die betrekking hebben op beleids- of managementinformatie. Of en in welke mate verzenders en ontvangers van berichten hun eigen berichten gebruiken voor interne managementrapportages, valt buiten het bestek van deze PIA. Dat is immers de eigenverantwoordelijkheid van verzenders en ontvangers van berichten en zal betrekking hebben op de eigen werkzaamheden in plaats van dat dit betrekking zal hebben op de werking van de CORV zelf.
Door het ontbreken van een afslag van (inhoudelijke) gegevens of berichten voor bijvoorbeeld managementinformatiecentrale, is er sprake van een laag risico. Hierbij past wel nadrukkelijk de kanttekening dat ook zonder een afslag van de berichten, de verkeersgegevens gebruikt zouden kunnen worden voor managementrapportages over de werking van de CORV. Zie daarvoor onderdeel 6.2.5.

Onderwerp	Risico's		
	laag	midden	hoog
Afslag van gegevens voor bijvoorbeeld managementinformatie	geen	(centrale) Opslag met gestructureerde bevraging	Decentrale opslag met decentrale bevraging

6.2.5 Centrale vastlegging van verkeersgegevens en foutmeldingen

De CORV slaat verkeersgegevens (niet de inhoud) van de berichten die verstuurd zijn op, zodat hiervan een overzicht ontstaat. Bij verkeersgegevens gaat het (enkel) om informatie welke organisatie op een bepaald moment een bepaald bericht verzonden heeft en wie daarvan de ontvanger was. Met deze informatie kan de juiste werking van de CORV gecontroleerd worden en kunnen eventuele verbeteringen doorgevoerd worden. Ook kunnen verkeersgegevens bijdragen in geval er onduidelijkheid is of een bepaald bericht wel of niet verzonden c.q. ontvangen is. Tevens wordt gebruik gemaakt van foutmeldingen. Ook deze worden tijdelijk opgeslagen. De foutberichten bevatten geen kopie van het oorspronkelijk inhoudelijke bericht. Bij de verkeersgegevens en de foutberichten is er sprake van persoonsgegevens (zie paragraaf 4.4).

Onderwerp	Risico's		
	laag	midden	hoog
Centrale vastlegging van verkeersgegevens en foutmeldingen	Vastlegging foutmeldingen / verkeersgegevens enkel tot het moment dat een herhaalbericht juist is afgeleverd	Geen foutmeldingen Vastlegging zonder inhoud van het bericht	Geen foutmeldingen Vastlegging met inhoud van het bericht

6.3 De beheersbaarheid van de berichteninfrastructuur

6.3.1 Beheer van de centrale componenten van de infrastructuur en de juiste werking

In vooral het rapport *Beheerinrichting CORV* van het projectteam van 10 oktober 2013 wordt ingegaan op het beheer van de CORV. Voor wat de inhoudelijke aspecten betreft, wordt als systeem en proceseigenaar uitgegaan van de Directeur DJJ. De feitelijke uitvoering van de werkzaamheden wordt uitgevoerd door de Justitiële Informatiedienst. Daarmee zijn de beheersmatige aspecten duidelijk belegd. Weliswaar ziet de huidige belegging op de meer op de ontwikkelfase, maar een permanente belegging is ook voorzien. Dit leidt wat het beheer van de CORV betreft tot een laag risico.

Onderwerp	Risico's		
	laag	midden	hoog
Beheer van de centrale componenten van de infrastructuur en de juiste werking	Duidelijk belegd op het niveau van uitvoering	Duidelijk belegd, maar meer "op papier" dan bij de uitvoering	Niet belegd of belegd bij meerdere partijen zonder duidelijkheid "wie wat doet"

6.3.2 Zeggenschap / invloed van de voor de gegevensverwerking verantwoordelijke organisatie

Het voornemen is om de Minister van Veiligheid en Justitie aan te wijzen als de Wbp-verantwoordelijke voor de persoonsgegevens die met de CORV verwerkt worden. Ook dit is aangegeven is het rapport *Beheerinrichting CORV* van het projectteam van 10 oktober 2013.

De juridische basis voor het aanwijzen van de minister is opgenomen in artikel 7.3.11, lid 4 van de Jeugdwet is de laatste zinsnede "*Daarbij kan worden bepaald welke maatregelen moeten worden getroffen om te waarborgen dat de uitwisseling van gegevens veilig en zorgvuldig plaatsvindt."*.

In de Memorie van Toelichting bij de Jeugdwet wordt specifiek over de verantwoordelijke voor de CORV vermeld: *"Om de uniformiteit te bevorderen bij de uitwisseling van gegevens tussen de ketenpartners zal daarnaast een voorziening voor de uitwisseling van deze gegevens worden ingericht. Het gaat om de Collectieve opdracht routeervoorziening (CORV)."* Tevens wordt vermeld: *"Vooral omdat er bij de berichten tussen ketenpartners ook sprake is van bijzondere gegevens als bedoeld in art. 16 Wbp, dient er een afdoende basis te zijn dat de verantwoordelijke voor de voorziening dergelijke bijzondere gegevens inderdaad tijdens het transport van de berichten en de opdrachten mag verwerken. Daartoe biedt het vierde lid een grondslag."*

Aanwijzing van één Wbp-verantwoordelijke draagt ertoe bij dat er ten aanzien van de zeggenschap en invloed over de te verwerken persoonsgegevens een laag risico is.

Onderwerp	Risico's		
	laag	midden	hoog
Zeggenschap / invloed van de voor de gegevensverwerking verantwoordelijke organisaties	1 verantwoordelijke	enkele verantwoordelijken met expliciete rolverdeling	Vele verantwoordelijken Geen expliciete rolverdeling bij enkele verantwoordelijken

6.3.3 Toepasselijk normenkader informatiebeveiliging

In onderdeel 8.1 van de *PSA/Solution Architecture, Interactieproces, Koppelvlakken en de Collectieve Opdracht RouteerVoorziening justitiële jeugdketen (CORV)* van het projectteam van 17 juli 2013 wordt het toepasselijk normenkader voor informatiebeveiliging van de CORV als volgt opgesomd.

Voor de CORV gelden de volgende eisen:

- Voorschrift Informatiebeveiliging Rijksdienst 2007

In VIR 2007 is op strategisch niveau aangegeven hoe een rijksdienst aan het informatiebeveiligingsbeleid en de verbetercyclus invulling dient te geven.

- Beveiligingsvoorschrift Rijksdienst 2005
  In BVR 2005 zijn de taken en verantwoordelijkheden van de Beveiligingsambtenaar en de Beveiligingscoördinator beschreven.
- Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie
  VIR-BI schrijft voor hoe om te gaan met gerubriceerde informatie.
- Baseline Informatiebeveiliging Rijksdienst – Tactisch Normenkader & Operationele Baseline
  Deze rijksbrede baseline is gebaseerd op ISO27001 en toereikend voor de verwerking van vertrouwelijke gegevens tot en met Departementaal Vertrouwelijk en persoonsgegevens tot en met risicoklasse II. Voor systemen die hogere betrouwbaarheidsniveaus vereisen dan de BIR biedt dienen risicoanalyses te worden uitgevoerd. Ook kan een risicoanalyse op een systeem nodig zijn om te toetsen of BIR toereikend is (baselinetoets).

Gelet op deze opsomming is er sprake van een toereikend en eenduidig normenkader voor de informatiebeveiliging van de CORV. Daardoor is er een laag risico.

Onderwerp	Risico's		
	laag	midden	hoog
Toepasselijk normenkader informatiebeveiliging	1 toereikend normenkader	Meerdere normenkaders of onduidelijkheid over de toereikendheid	Geen normenkader vastgesteld c.q. bepaald

6.3.4 Afscherming (deel)domeinen bij meervoudig gebruik infrastructuur

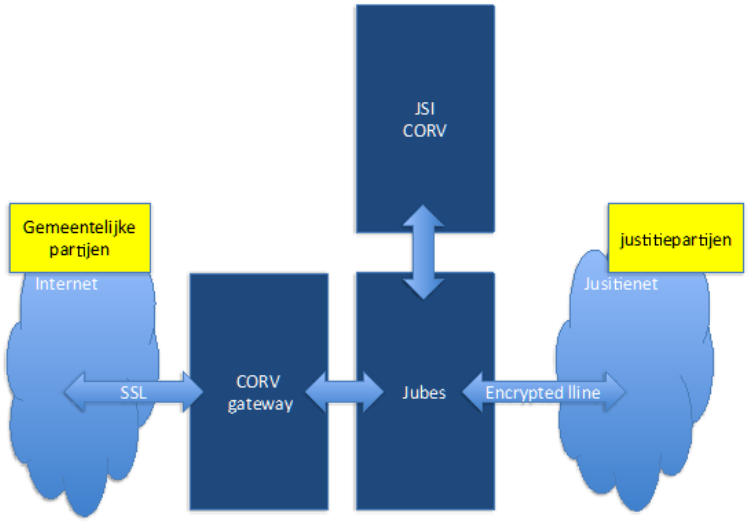
De CORV wordt enkel gebruikt voor de routering van berichten in het kader van de Jeugdwet en, voor zover betreft de AMHK's, de Wmo 2015. Dit vindt, mede ter beveiliging en afscherming, plaats in een (volstrekt) afgesloten systeem zonder menselijke toegang. Bij de CORV is er (op dit moment) geen sprake van meervoudig gebruik van de infrastructuur voor inhoudelijk andere domeinen. Daardoor is er sprake van een laag risico.
Ingeval de CORV in de toekomst ook voor andere soorten berichten gebruikt zou worden, is daarvoor een (aanvullende) beoordeling nodig

Onderwerp	Risico's		
	laag	midden	hoog
Afscherming (deel)domeinen bij meervoudig gebruik infrastructuur	Geen meervoudig gebruik (CORV)	Meervoudig gebruik met afgescheiden informatiestromen (Justitienet)	Meervoudig gebruik zonder afscheiding van informatiestromen

6.3.5 Informatiebeveiliging (risico-inventarisatie en maatregelen)

Voor de CORV is een QuickScan BIR uitgevoerd (de *CORV Quick scan BIR* van het deelproject Justitiële Keteninformatisering van 13 juni 2014). De Quickscan is bedoeld als instrument om te bepalen of de risico's voor een proces met ondersteunende systemen voldoende door de BIR worden afgedekt. Als dit niet het geval is dan moet met een aanvullende risicoanalyse vastgesteld worden welke extra beveiligingsmaatregelen nodig zijn.

De Quickscan BIR is uitgevoerd voor de donkerblauwe elementen (CORV Gateway, Jubes en JSI CORV) zoals weergegeven in onderstaande figuur. De uitgevoerde Quickscan BIR heeft geen betrekking op de SSL verbinding met gemeentelijke partijen en Justitienet.



Op basis van de analyse is in de Quickscan BIR de conclusie getrokken dat het bij de CORV om risicoklasse II gegevens gaat. Daarbij is onderstaand overzicht gebruikt.

Aard van de persoonsgegevens:		Persoonsgegevens	Bijzondere persoonsgegevens	Financieel en / of economische persoonsgegevens
Hoeveelheid persoonsgegevens (aard en omvang)	*Aard van de verwerking*		Conform artikel 16 WBP	
Weinig persoonsgegevens	Lage complexiteit van verwerking	**Risicoklasse** 0	**Risicoklasse** II	**Risicoklasse** II
Veel persoonsgegevens	Hoge complexiteit van verwerking	**Risicoklasse** I	**Risicoklasse** III	

De QuickScan BIR CORV leidt tot de conclusie dat geen aanvullende maatregelen op de BIR nodig zijn. Er hoeft geen aanvullende risico-analyse te worden uitgevoerd. Conclusie is dat de BIR Baseline volstaat.

Zoals in de Quickscan BIR ook benadrukt wordt, is niet onderzocht of de BIR Baseline maatregelen ook daadwerkelijk genomen zijn en gecontroleerd worden. Wel wordt in de Quickscan het advies gegeven om dat te doen.

Zoals reeds is aangegeven, heeft de Quickscan BIR geen betrekking op de SSL verbinding met gemeentelijke partijen en Justitienet. Voor wat justitienet betreft is in ieder geval in 2010 een risico-analyse uitgevoerd.

Voor wat het gebruik van Digikoppeling en SSL met tweezijdige authenticatie betreft, kan opgemerkt worden dat dit een veilige manier is om binnen de digikoppeling standaard berichten uit te wisselen. Zie bijvoorbeeld http://www.logius.nl/producten/gegevensuitwisseling/digikoppeling/.
Het (vereiste) gebruik van SSL komt ook aan de orde in het rapport van het Cbp van 10 juli 2013 over *Onderzoek naar de beveiliging van het online aanvragen van herhaalrecepten bij huisarts en apotheek.* Het Cbp verwijst t.a.v. het gebruik van SSL om berichtenverkeer te beveiliging in de rapportage naar de *ICT-Beveiligingsrichtlijnen voor webapplicaties Deel 2 (januari 2012). Nationaal Cyber Security Centrum (NCSC)*.

Omdat nog geen beoordeling plaatsgevonden heeft of de te nemen BIR Baseline maatregelen voor de CORV reeds genomen zijn, geen specifieke (nieuwe) risico-analyse voor het gebruik van justitienet en SSL is uitgevoerd en bijvoorbeeld nog geen kwetsbaarheids-test (penetratietest) voor de gehele infrastructuur is uitgevoerd, wordt het risico aangemerkt als “midden” en worden een aantal aanbevelingen gedaan.

Onderwerp	Risico’s		
	laag	midden	hoog
Informatiebeveiliging (risico-inventarisatie en maatregelen)	Risico-inventarisatie uitgevoerd en maatregelen getroffen	Risico-inventarisatie uitgevoerd en onduidelijkheid over de getroffen maatregelen (CORV , Justitienet, SSL)	Geen risico-inventarisatie uitgevoerd

Aanbeveling t.a.v. informatiebeveiliging
Aanbeveling 2: Voor wat de informatiebeveiliging en het treffen van de benodigde maatrelen betreft, worden de volgende acties aanbevolen:

CORV: besteed, bijvoorbeeld in het kader van de voorziene praktijkproef CORV, aandacht aan de vraag of de BIR- Baseline maatregelen daadwerkelijk getroffen zijn;
Digikoppeling en SSL: beleg de verantwoordelijkheid voor het zorgvuldig en juist gebruik van SSL en bepaal met name welke organisatie belast is met het signaleren van en attenderen op eventuele problemen bij het gebruik van SSL;
Justitienet: stem de informatiebeveiliging en de resultaten van de Quick Scan BIR voor de CORV af met de beheerder c.q. de proceseigenaar van Justitienet.

6.3.6 Toezicht en controle

De Minister van Veiligheid en Justitie wordt aangewezen als de Wbp-verantwoordelijke voor de CORV (zie paragraaf 6.3.2). Dit betekent dat de functionaris voor de gegevensbescherming van het ministerie toezicht houdt op de naleving. T.a.v. het toezicht is het risico daardoor laag.

Omdat nog geen beoordeling plaatsgevonden heeft of de te nemen BIR Baseline maatregelen voor de CORV reeds genomen zijn, wordt het risico t.a.v. controle aangemerkt als “midden”. Hierbij gaat het om een nadere uitwerking van de aanbevelingen die t.a.v. informatiebeveiliging al gedaan zijn.

Onderwerp	Risico’s		
	laag	midden	hoog
Toezicht en controle	Toezicht: belegd bij de functionaris gegevensbescherming	Controle: duidelijk belegd, maar wellicht meer “op papier” dan bij de uitvoering (CORV, Justitienet, SSL)	Niet belegd

7 De inbedding in de informatiehuishouding van verzenders en ontvangers

7.1 Overzicht

In het derde, en laatste, onderdeel van de risicobeoordeling wordt kort aandacht besteed aan aandachtspunten voor de inbedding in de informatiehuishouding van verzenders en ontvangers. Het gaat over:

- aandachtspunten voor gebruikers in verband met aansluiting op de CORV;
- elementen die bij aansluiting een rol kunnen spelen.

7.2 Verplichting tot aansluiten op de CORV

Uitgangspunt is dat aansluiten op de CORV verplicht is. Deze verplichting zal opgenomen worden in de ministeriele regeling ter uitwerking van artikel 7.3.11, lid 4, Jeugdwet.

7.3 Stand van zaken bij de gebruikers t.a.v. aansluiting en informatiebeveiliging

De CORV en de berichten infrastructuur ziet op de centrale componenten gelegen tussen de ‘’postbussen’ c.q. aansluitpunten van de gebruikers. In die zin wordt ook wel aangegeven dat de CORV werkt van ‘deurmat tot deurmat’. De aansluitende partijen zijn zelf verantwoordelijk verantwoordelijk voor zijn aansluiting en de benodigde aanpassing van de processen.

In paragraaf 4.6 is aandacht besteed aan de voor de CORV op te stellen aansluitvoorwaarden o.a. betreffende de informatiebeveiliging van het aansluitpunt van de gebruiker. Aansluitende partijen dienen zelf te beoordelen en aan te geven welke activiteiten voor aansluiting verricht zijn en welke informatiebeveiliging reeds plaatsvindt. Daarbij kunnen aansluitende partijen gebruik maken van onderstaand overzicht om een inzicht te verkrijgen in de risico’s die bij de aansluitende partijen spelen en voor welke onderwerpen nog nadere aandacht nodig is.

Onderwerp	Risico’s		
	laag	midden	hoog
Inspanningen van de gebruikers voor implementatie	Maatregelen worden getroffen (bij aansluiting van een ‘postbus’ op CORV in het bijzonder maatregelen over een juiste verdere interne distributie van berichten)	Aandacht voor het treffen van maatregelen (bij aansluiting van een ‘postbus’ op CORV in het bijzonder maatregelen over een juiste verdere interne distributie van berichten)	Geen aandacht
Informatiebeveiliging (risico-	Risico-inventarisatie	Risico-inventarisatie	Geen risico-

inventarisatie en maatregelen)	uitgevoerd en maatregelen getroffen	uitgevoerd en onduidelijkheid over de getroffen maatregelen	inventarisatie uitgevoerd
Toezicht en controle	Duidelijk belegd op het niveau van uitvoering	Duidelijk belegd, maar meer “op papier” dan bij de uitvoering	Niet belegd

BIJLAGE 1 | Overzicht basisdocumenten

Het *Projectplan Beleidsinformatie Stelselherziening Jeugd* van 8 november 2012

Het *Beslisdocument Interacties tussen gemeenten, gecertificeerde instellingen en de justitiële jeugdketens in het nieuwe jeugdstelsel* van het projectteam van 11 april 2013.

De *PSA/Solution Architecture, Interactieproces, Koppelvlakken en de Collectieve Opdracht RouteerVoorziening justitiële jeugdketen (CORV)* van 17 juli 2013

Het rapport *Beheerinrichting CORV* van het projectteam van 10 oktober 2013

Het *Plan van Aanpak Ontwikkeling, implementatie en in beheer name Collectieve Opdracht en Routeer Voorziening (CORV)* van het projectteam van 19 november 2013

Het *Acceptatietestplan CORV* van het projectteam van 22 januari 2014 en de *Reviewrapportage* van 12 juni 2014 van de auditor;

De *Factsheet Collectieve Opdracht RouteerVoorziening* van februari 2014

Het rapport *Aansluitproces op CORV voor gemeenten* van het projectteam van 14 maart 2014

De *CORV Quick scan BIR* van het deelproject Justitiële Keteninformatisering van 13 juni 2014

De *Solution Architecture CORV* van de Justitiële Informatiedienst van 11 april 2014

Het rapport *Stelselherziening Jeugdbescherming* van de Justitiële Informatiedienst van april 2014

Het rapport *Ketenproces Jeugdreclassering* van de Justitiële Informatiedienst van 13 juni 2014

Diverse zogenaamde '*Praatplaten*' van het projectteam over de diverse onderdelen en onderwerpen bij de justitiële keteninformatisering en de ontwikkeling van de CORV.

De *Impact Analyse CORV* van KING van 13 mei 2014

De Factsheet *Zorgmeldingen Jeugd* van de VNG van juni 2014

Het *Programma van Eisen ICT-ondersteuning AMHK* van de VNG van 16 mei 2014

Het Concept *Model Handelingsprotocol voor het AMHK* van de VNG van 4 juni 2014

Het *Logisch ontwerp formulier Zorgmeldingen jeugdige* van vts Politie Nederland van 29 oktober 2012

Het *Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst* van 24 juni 2013, Bijlage bij TK, 26 643, nr. 282

De Brief van de minister voor Wonen en Rijksdienst en van de staatssecretaris van VenJ van 21 juni 2013 over het *verplicht gebruik van het Toetsmodel PIA Rijksdienst* (TK, 26 643, nr. 282)

Het advies van het Cbp van 5 maart 2103, z2012-00847, over het concept Toetsmodel Privacy Impact Assessment

Het rapport van het Cbp van 10 juli 2013 over *Onderzoek naar de beveiliging van het online aanvragen van herhaalrecepten bij huisarts en apotheek*

Het advies van het Cbp van 7 augustus 2014, kenmerk z2014-00487 over *het ontwerpbesluit Jeugdwet (wijziging Besluit justitiële en strafvorderlijke gegevens*

de *ICT-Beveiligingsrichtlijnen voor webapplicaties Deel 2 (januari 2012). Nationaal Cyber Security Centrum (NCSC)* .

De Motie Franken van 17 mei 2011 over *het uitvoeren van een PIA in het kader van wetgeving* (EK, 31 051, nr. D)

De Motie Elissen en Gesthuizen van 13 oktober 2011 over *privacy by design en safety by design bij de ontwikkeling van nieuwe ICT-projecten* (TK, 26 643, nr. 203)

De Motie Bergkamp van 4 april 2013 over een PIA betreffende *de uitwisseling van gegevens over cliënten tussen partijen als provincies, gemeenten en Bureau Jeugdzorg* (TK, 31 839, nr. 279)

BIJLAGE 2 | Voorbeeld Overzicht berichten CORV / Gemeenten

ROL, TAAK EN BERICHTEN CORV TBV DE GEMEENTE PER 28 MEI 2015 (*)								
Nr	Bericht en Betekenis	Berichtcode	Van	Rol/Wettelijke taak	Naar	Rol/Wettelijke taak	Inhoud bericht	Taken en acties gemeente
JEUGDBESCHERMING **Indienen verzoek tot onderzoek**								
JB1	Verzoek tot onderzoek (VTO): Fomele bericht voor aanvraag onderzoek noodzaak kinderbeschermingsmaatregel	StUF: vtoDi01 EBV: BD-050001 Gemeente ==> RvdK, en GI ==> RvdK, en AMHK ==> RvdK	Gemeente (of gemandateerde) NB. Dit bericht kan ook worden ingestuurd door AMHK en GI. Spoedzaken kunnen door professionals ook rechtstreeks (telefoon/mail) bij de RvdK worden gemeld	Verzoeker: Indienen van het verzoek (JW 2.4 lid 1 en 3.1 lid 1) Regisseur: op vroeghulp gedwongen kader en nazorg (JW MvT)	Landelijke RvdK NB. Vanuit landelijke RvdK wordt RvdK regio betrokken	Onderzoeker: Onderzoeken noodzaak kinderbeschermings-maatregel (JW 3.1 lid 1)	Casusnummer verzoeker (bijv. zaaknummer gemeente); Gegevens verzoeker; Gegevens kind(eren); Gegevens ouder(s); Gezagsgegevens; Kindfactoren/omstandigheden die hebben geleid tot verzoek; Evt toe te voegen bijlagen	Ouders/verzorgers informeren omtrent VTO; Ingediend VTO registreren; Monitoren voortgang; Eventueel ketenoverleg in het kader van regie en voorkomen dubbelingen; Continueren benodigde hulp gedurende het lopende verzoek en onderzoek; Veiligheidsplan (Zie ook handreiking JB JR)
JB2	Acceptatiesignaal Verzoek tot onderzoek: Bevestiging dat VTO in goed orde is ontvangen	StUF: Bv01 EBV: BD-050004 RvdK ==> Verzoekende Gemeente	Landelijke RvdK	Onderzoeker	Verzoekende gemeente (of gemandateerde)	Verzoeker Regisseur	Identificatiecode (=Identificatiecode van het oorspronkelijke bericht Verzoek tot onderzoek waar dit een antwoordbericht op is)	Voortgang registreren en verder monitoren
JB3	Foutbericht Verzoek tot onderzoek: Bericht van afkeuring van ontvangen foutief VTO	StUF: Fo01 EBV: BD-050005 RvdK ==> Verzoekende Gemeente	Landelijke RvdK	Onderzoeker	Verzoekende gemeente (of gemandateerde)	Verzoeker Regisseur	Foutcode, Foutniveau, Foutomschrijving NB. Inhoudelijke informatie betreffende de fout wordt bepaald door de ontvangende partij van het VTO (de RvdK).	Kan softwarefout of procesfout betreffen. Fout analyseren en herstellen. Het betreffende VTO bericht wordt door de RvdK niet in behandeling genomen
Notificatie intake								
JB4	Notificatie Intake: Notificatie of de RvdK al dan niet een onderzoek zal instellen na ontvangst en intake verzoek tot onderzoek	StUF: notificatieDi01 EBV: BD-050002 (Type "01") RvdK ==> Verzoekende Gemeente	Landelijke RvdK	Onderzoeker	Verzoekende gemeente (of gemandateerde)	Verzoeker Regisseur	Type notificatie (=01); Casusnummer RvdK (leeg in geval van afwijzing); Status casus, Gegevens kind; Casusnummer verzoeker; Indicatie verzoek toegewezen of afgewezen NB. Er wordt per kind in het oorspronkelijke verzoek tot onderzoek een aparte notificatie verzonden	Notificatie registreren; Vervolgactie afhankelijk van toewijzen of afwijzen van het verzoek
JB5	Foutbericht Notificatie intake: Bericht van afkeuring van ontvangen foutieve Notificatie intake	StUF: Fo01 EBV: BD-050005 Verzoekende ==> RvdK NB. Deze foutmelding is alleen bedoeld om technische fouten in de ontvangen notificatie terug te melden	Verzoekende gemeente (of gemandateerde)	Verzoeker Regisseur	Landelijke RvdK	Onderzoeker	Foutcode, Foutniveau, Foutomschrijving NB. Inhoudelijke informatie betreffende de fout wordt bepaald door de ontvangende partij van de Notificatie (Gemeente)	Monitoren vervolg; Eventueel contact met RvdK

ROL, TAAK EN BERICHTEN CORV TBV DE GEMEENTE PER 28 MEI 2015 (*)								
Nr	Bericht en Betekenis	Berichtcode	Van	Rol/Wettelijke taak	Naar	Rol/Wettelijke taak	Inhoud bericht	Taken en acties gemeente
Notificatie uitkomst onderzoek								
JB6	Notificatie uitkomst onderzoek: Notificatie omtrent resultaat uitgevoerd onderzoek door RvdK	StUF: notificatieDi01 EBV: BD-050002 (Type "02") RvdK ==> Verzoekende Gemeente	Landelijke RvdK	Onderzoeker Rekwestreerder (BW 255 lid 2)	Verzoekende gemeente (of gemandateerde)	Verzoeker Regisseur	Type notificatie (=02); Casusnummer RvdK; Status casus; Beslissing (wel/geen rekest); Gegevens kind; Casusnummer verzoeker; uitkomst onderzoek en voorgestelde maatregel (rekest) NB. Er wordt per kind in het oorspronkelijke verzoek tot onderzoek een aparte notificatie verzonden	Notificatie registreren; Vervolgactie afhankelijk van uitkomst onderzoek; In geval van rekest overleg over in te zetten GI met de RvdK (JW 3.1 lid 6) NB. Wet herziene kinderbeschermingsmaatregelen (nu in voorbereiding) geeft de burgemeester mogelijkheid om, in geval van negatieve beslissing van de RvdK, een zaak alsnog voor te leggen aan de rechtbank
JB7	Foutbericht Uitkomst onderzoek: Bericht van afkeuring van ontvangen foutieve Notificatie intake	BD-050005 Verzoekende Gemeente ==> RvdK NB. Deze foutmelding is alleen bedoeld om technische fouten in de ontvangen notificatie terug te melden	Verzoekende gemeente (of gemandateerde)	Verzoeker Regisseur	Landelijke RvdK	Onderzoeker Rekwestreerder	Foutcode, Foutniveau, Foutomschrijving NB. Inhoudelijke informatie betreffende de fout wordt bepaald door de ontvangende partij van de Notificatie (Gemeente)	Monitoren vervolg; Eventueel contact met RvdK
Notificatie ambtshalve onderzoek								
JB8	Notificatie Ambtshalve onderzoek: Notificatie dat RvdK ambtshalve onderzoek zal starten	StUF: notificatieDi01 EBV: BD-050002 (Type "03") RvdK ==> Verzoekende Gemeente	Landelijke RvdK	Onderzoeker (3.1, lid 2 en 3)	Verantwoordelijke gemeente, conform woonplaatsbeginsel (of gemandateerde)	Regisseur	Type notificatie (=03). Casusnummer RvdK; Status casus; Gegevens kind; Gegevens ouder(s); Gezagsgegevens	Notificatie registreren; Monitoren vervolg;
JB9	Foutbericht Notificatie Ambtshalve onderzoek	StUF: Fo01 EBV: BD-050005 Verzoekende Gemeente ==> RvdK NB. Deze foutmelding is alleen bedoeld om technische fouten in de ontvangen notificatie terug te melden	Verantwoordelijke gemeente (of gemandateerde)	Regisseur	Landelijke RvdK	Onderzoeker	Foutcode, Foutniveau, Foutomschrijving NB. Inhoudelijke informatie betreffende de fout wordt bepaald door de ontvangende partij van de Notificatie (Gemeente)	Monitoren vervolg; Eventueel contact met RvdK; Indien notificatie bij verkeerde gemeente afgeleverd contact opnemen met de RvdK
Notificatie uitkomst ambtshalve onderzoek								
JB10	Notificatie Uitkomst Ambtshalve onderzoek: Notificatie omtrent resultaat uitgevoerd ambtshalve onderzoek door RvdK	StUF: notificatieDi01 EBV: BD-050002 (Type "04") RvdK ==> Verzoekende Gemeente	Landelijke RvdK	Onderzoeker Rekwestreerder	Verantwoordelijke gemeente, conform woonplaatsbeginsel (of gemandateerde)	Regisseur	Type notificatie (=04); Casusnummer RvdK; Status casus; Beslissing (wel/geen rekest); Gegevens kind; Uitkomst onderzoek en voorgestelde maatregel (rekest)	Notificatie opnemen in dossier; Vervolgactie afhankelijk van uitkomst onderzoek; In geval van rekest overleg over in te zetten GI met de RvdK (JW 3.1 lid 6) NB. Wet herziene kinderbeschermingsmaatregelen (nu in voorbereiding) geeft de burgemeester mogelijkheid om, in geval van negatieve beslissing van de RvdK, een zaak alsnog voor te leggen aan de rechtbank

ROL, TAAK EN BERICHTEN CORV TBV DE GEMEENTE PER 28 MEI 2015 (*)								
Nr	Bericht en Betekenis	Berichtcode	Van	Rol/Wettelijke taak	Naar	Rol/Wettelijke taak	Inhoud bericht	Taken en acties gemeente
JB11	Foutbericht Notificatie Uitkomst Ambtshalve onderzoek	StUF: Fo01 EBV: BD-050005 Verzoekende Gemeente ==> RvdK NB. Deze foutmelding is alleen bedoeld om technische fouten in de ontvangen notificatie terug te melden	Verantwoordelijke gemeente (of gemandateerde)	Regisseur	Landelijke RvdK	Onderzoeker Rekwestreerder	Foutcode, Foutniveau, Foutomschrijving NB. Inhoudelijke informatie betreffende de fout wordt bepaald door de ontvangende partij van de Notificatie (Gemeente)	Monitoren vervolg; Eventueel contact met RvdK
Notificatie Beschikking rechtbank inzake kinderbeschermingsmaatregel (Let op: implementatie wel voorzien maar nog niet gepland)								
JB12	Notificatie Beschikking rechtbank inzake kinderbeschermingsmaatregel: Notificatie met uitspraak rechtbank ten aanzien van voorgelegde kinderbeschermingsmaatregel	StUF: notificatieDi01 EBV: BD-050002 (Type "05") NB. Inregeling en inhoud van dit bericht wordt nog nader bepaald	?????	?????	Verantwoordelijke gemeente (of gemandateerde)	Regisseur	Type notificatie (=05)	Notificatie registreren. Eventueel ketenoverleg in het kader van regie. Overleg met uitvoerende GI
JB13	Foutbericht Notificatie Beschikking rechtbank inzake kinderbeschermingsmaatregel	StUF: Fo01 EBV: BD-050005 NB. Inregeling en inhoud van dit bericht wordt nog nader bepaald	Verantwoordelijke gemeente (of gemandateerde)	Regisseur	?????	?????	Foutcode, Foutniveau, Foutomschrijving	Monitoren vervolg; Eventueel contact met verzender; Indien notificatie bij verkeerde gemeente afgeleverd contact opnemen met de verzender

JEUGDRECLASSERING								
Notificatie Reclassering opdracht								
JR1	Notificatie omtrent reclasseringsopdracht, betreffende een jeugdige, die is toegestuurd aan een gecertificeerde instelling	StUF: notificatieDi01 EBV: BD-050002 (Type "06") NB. Inregeling en inhoud van dit bericht wordt nog nader bepaald	AICE (=Administratief Informatie en Coördinatie Centrum)	Executie verantwoordelijke	Verantwoordelijke gemeente (of gemandateerde)	Regisseur	Type notificatie (=06)	Notificatie registreren. Eventueel ketenoverleg in het kader van regie. Overleg met uitvoerende GI
JR2	Foutbericht Notificatie Reclassering opdracht	StUF: Fo01 EBV: BD-050005 NB. Inregeling en inhoud van dit bericht wordt nog nader bepaald	Verantwoordelijke gemeente (of gemandateerde)	Regisseur	AICE (=Administratief Informatie en Coördinatie Centrum)	Executie verantwoordelijke	Foutcode, Foutniveau, Foutomschrijving	Monitoren vervolg; Eventueel contact met RvdK, bijvoorbeeld indien notificatie bij verkeerde gemeente is afgeleverd
Notificatie Toezicht en begeleiding door de RvdK								
JR3	Notificatie Toezicht en begeleiding door de RvdK	nnb RvdK ==> Gemeente NB. Inregeling en inhoud van dit bericht wordt nog nader bepaald	Landelijke RvdK	Opdrachtverstrekker (JW MvT)	Verantwoordelijke gemeente (of gemandateerde)	Regisseur	nnb	Notificatie registreren. Eventueel ketenoverleg in het kader van regie. Overleg met uitvoerende GI
JR4	Foutbericht Notificatie Toezicht en begeleiding door de RvdK	StUF: Fo01 EBV: BD-050005 NB. Inregeling ven inhoud aan dit bericht wordt nog nader bepaald	Verantwoordelijke gemeente (of gemandateerde)	Regisseur	Landelijke RvdK	Opdrachtverstrekker (JW MvT)	Foutcode, Foutniveau, Foutomschrijving	Monitoren vervolg; Eventueel contact met RvdK, bijvoorbeeld indien de notificatie bij verkeerde gemeente is afgeleverd

ROL, TAAK EN BERICHTEN CORV TBV DE GEMEENTE PER 28 MEI 2015 (*)								
Nr	Bericht en Betekenis	Berichtcode	Van	Rol/Wettelijke taak	Naar	Rol/Wettelijke taak	Inhoud bericht	Taken en acties gemeente
Zorgmelding Politie								
ZM1	Zorgmelding Politie: In geval van gconstateerde zorgen omtrent jeugdige, op basis van signalen of onderzoek, stuurt Politie een zorgmelding met daarin opgenomen een zorgformulier	StUF: EBV: BD-050016 Politie ==> Gemeente NB. Inregeling, inhoud en aflevering van dit bericht wordt nog nader bepaald	Politie	Vroegsignaleren en doorverwijzen	Gemeente (of gemandateerde, bijv AMHK)	Toeleider/Beslisser (JW 2.3 lid 1) Regisseur	Gegevens indiener; Gegevens kind; Gegevens ouder(s), verzorgers en betrokkenen; Kindfactoren/omstandigheden/leefgebieden die hebben geleid tot het zorgformulier; Evt toe te voegen bijlagen	Registreren zogformulier; Vervolgbeslissing toeleiden naar jeugdhulp; Eventueel overleg met (en/of overdragen naar) andere gemeente indien andere gemeente verantwoordelijk is voor deze jeugdige
ZM2	Acceptatiesignaal Zorgmelding Politie: Bevestiging dat Zorgmelding in goede orde is ontvangen	StUF: Bv01 EBV: BD-050004 Gemeente ==> Politie NB. Inregeling en inhoud van dit bericht wordt nog nader bepaald	Gemeente (of gemandateerde, bijv AMHK)	Toeleider/Beslisser (JW 2.3 lid 1) Regisseur	Politie	Vroegsignaleren en doorverwijzen	Identificatiecode (=Identificatiecode van het oorspronkelijke bericht Verzoek tot onderzoek waar dit een antwoordbericht op is)	Voortgang registreren en verder monitoren
ZM3	Foutbericht Zorgmelding Politie: Bericht van afkeuring van ontvangen foutief Zorgformulier Politie	StUF: Fo01 EBV: BD-050005 Gemeente ==> Politie NB. Inregeling en inhoud van dit bericht wordt nog nader bepaald	Gemeente (of gemandateerde, bijv AMHK)	Toeleider/Beslisser (JW 2.3 lid 1) Regisseur	Politie	Vroegsignaleren en doorverwijzen	Foutcode, Foutniveau, Foutomschrijving NB. Inhoudelijke informatie betreffende de fout wordt bepaald door de ontvangende partij	Monitoren vervolg; Eventueel contact met Politie

BIJLAGE 3 | Ingevulde vragenlijst PIA Rijksdienst

De vragenlijst van het *Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst van 24 juni 2013* (Bijlage bij TK, 26 643, nr. 282) . Het Toetsmodel dient vanaf 1 september 2013 standaard te worden toegepast bij ontwikkeling van nieuwe wetgeving en beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien.

I. Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/gegevensminimalisering

I.1. Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?

> Ja, er worden bij en in de berichten persoonsgegevens verwerkt.
> De CORV als berichten-infrastructuur heeft geen inhoudelijke bemoeienis met de inhoud van de berichten zelf.
> De CORV legt wel zelfstandig verkeersgegevens en foutberichten vast. Ook dat zijn persoonsgegevens.

I.2. Andere specifieke persoonsgegevens?

I.2a. Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?

> Ja, voor wat betreft de inhoud van de berichten (niet t.a.v. de verkeersgegevens en de foutberichten / foutberichten bevatten geen kopie van het oorspronkelijke bericht).
> Alleen al het feit dat jeugdreclassering opgelegd is kan een stigmatiserende werking hebben. Bij nagenoeg alle berichten is er sprake van bijzondere persoonsgegevens, met name bij politiemeldingen en VTO's aan de RvdK.

I.2b. Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?

> Ja, voor wat betreft de inhoud van de berichten (niet t.a.v. de verkeersgegevens en de foutberichten / foutberichten bevatten geen kopie van het oorspronkelijke bericht).

Het gaat bij de berichten over alle jeugdigen die te maken krijgen met het gedwongen kader

I.2c. Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?

Neen, bij de CORV niet omdat er sprake is van enkel routeren en machine-machine koppelingen

I.2d. Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?

Neen

I. 2e. Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken?

Ja, voor wat betreft de inhoud van de berichten (niet t.a.v. de verkeersgegevens en de foutberichten / foutberichten bevatten geen kopie van het oorspronkelijke bericht). In de berichten (inhoud) zijn het BSN en bij bepaalde berichten het SKN opgenomen. Opname van BSN is gebaseerd op artikel 7.2.1 Jeugdwet, artikel 5.2.9 Wmo 2015 of artikel 27b Wetboek van strafvordering. Opname van het SKN is gebaseerd op artikel 27b Wetboek van Strafvordering.

I. 3. Kan van elk van de onder vraag I.1 en vraag I.2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegeven toe.

Ten aanzien van de inhoud van de berichten: ja, verbonden met de taken ter uitvoering van de jeugdwet van de verzenders en ontvangers van berichten Ten aanzien van de verkeersgegevens en foutberichten: ja

I.4. Kan als het gaat om gevoelige persoonsgegevens hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?

Ten aanzien van de inhoud van de berichten: neen Ten aanzien van de verkeersgegevens en foutberichten: neen / nvt.

I.5. In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject? Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen?

Ten aanzien van de berichten: uitvoering door gemeenten en veldpartijen van de Jeugdwet en ook de uitvoering van jeugdreclassering. Zie de aanbeveling over het Berichtenboek en de beschrijving over welke taken en artikelen van de Jeugdwet die een rol spelen bij de berichten. Ten aanzien van de CORV: vastleggen verkeersgegevens en foutberichten voor een juiste werking van de CORV

II. Doelbinding, koppeling, kwaliteit en profilering

Doeleinden/doelbinding en koppeling
II.1. Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?

Zie I.5

II. 2. Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen? (scenario toevoeging nieuwe persoonsgegevens).

Zie I.5

II. 3. Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden). Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?

Zie I.5

II.4. Indien u positief hebt geantwoord op vragen II.2 of II.3, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) het Cbp indien er geen FG is?

De CORV-verwerkingen (routeren, verkeersgegevens en foutberichten) worden gemeld bij de FG van VenJ.
De verkeersgegevens en foutberichten vallen (in beginsel) binnen artikel 33 van het Vrijstellingbesluit Wbp.

Artikel 33. Computersystemen

1. Artikel 27 van de wet is niet van toepassing op verwerkingen die uitsluitend zijn gericht op het onderhoud, het beheer, de beveiliging, het gebruik en de goede werking van computersystemen of computerprogramma's binnen de organisatie van de verantwoordelijke, voor zover deze verwerkingen voldoen aan de in dit artikel vermelde eisen.
2. De verwerking geschiedt slechts voor:
    a. de controle op en de beveiliging van de computersystemen of computerprogramma's;
    b. de ondersteuning van de goede werking van de computersystemen of computerprogramma's;
    c. het sorteren en herstellen van (tussen)bestanden;
    d. het aanmaken van reservekopieën van (tussen)bestanden;
    e. het beheer van de systemen of programma's.
3. Geen andere persoonsgegevens worden verwerkt dan:
    a. gegevens met betrekking tot het gebruik van de programmatuur;
    b. technische en besturingsgegevens;
    c. gegevens ter bevordering van een goede werking;

d. historische gegevens;
e. gebruikersgegevens.

4. De persoonsgegevens worden slechts verstrekt aan:
a. degenen, waaronder begrepen derden, die zijn belast met of leiding geven aan het systeem-, gegevensbeheer of applicatiebeheer of die daarbij noodzakelijk zijn betrokken;
b. anderen, in de gevallen bedoeld in artikel 8, onder a, c en d, en artikel 9, derde lid, van de wet.

5. De persoonsgegevens worden verwijderd uiterlijk 6 maanden nadat zij zijn verkregen, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht.

II.5. Indien u positief geantwoord hebt op vragen II.2 of II.3, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?

Zie de aanbeveling om in 2015 een review op de berichten te doen.

II.6. Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het beleidsvoorstel, wetsvoorstel op overheidsICT-systeem verwerkte persoonsgegevens na te gaan?

Speelt t.a.v. de inhoud van de berichten. Die worden allemaal gedetailleerd beschreven en in een ministeriel regeling geregeld. Uiteraard blijven de gebruikers van de berichten verantwoordelijkheid voor de juistheid van de gegevens. De CORV toetst die inhoudelijke juistheid niet.

II.7. Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen? Zijn de betrokkenen daarvan op de hoogte? Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld?

Neen / Nvt.

II.8. Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?

Neen / Nvt.

III. Betrokken instanties/systemen en verantwoordelijkheid

III.1. Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder I.5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?

Zie paragraaf 6 van de PIA.

III.2. Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?

Zie paragraaf 6 van de PIA.

III. 3. Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens? Bestaat de kans dat bij het gebruik ervan de gegevens ter beschikking komen van onbevoegden?

Zie paragraaf 6 van de PIA.

III.4. Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?

Zie paragraaf 6 van de PIA.

III.5. Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?

Zie paragraaf 6 van de PIA.

III.6. Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?

Zie paragraaf 6 van de PIA.

III. 7. Is er sprake van overdracht van persoonsgegevens naar een (overheids-)instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven?

Zie paragraaf 6 van de PIA. Er worden geen gegevens buiten Nederland verwerkt.

IV. Beveiliging en bewaring/vernietiging

Beveiliging
IV.1. Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging?

Zie voor informatiebeveiliging van de CORV paragraaf 6 en zie paragraaf 7 t.a.v. de gebruikers van de berichten en hun eigen ICT.

IV.2. Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker?

Zie voor informatiebeveiliging van de CORV paragraaf 6 en zie paragraaf 7 t.a.v. de gebruikers van de berichten en hun eigen ICT.

IV. 3. Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bv. wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend bv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen?

Zie voor informatiebeveiliging van de CORV paragraaf 6 en zie paragraaf 7 t.a.v. de gebruikers van de berichten en hun eigen ICT.

IV.4. Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen?

Zie voor informatiebeveiliging van de CORV paragraaf 6 en zie paragraaf 7 t.a.v. de gebruikers van de berichten en hun eigen ICT.

IV.5. Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?

Zie voor informatiebeveiliging van de CORV paragraaf 6 en zie paragraaf 7 t.a.v. de

gebruikers van de berichten en hun eigen ICT.

IV.6. Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?

Zie voor informatiebeveiliging van de CORV paragraaf 6 en zie paragraaf 7 t.a.v. de gebruikers van de berichten en hun eigen ICT.

IV.7. Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief log-gegevens, vernietigd? Is er controle op de vernietiging, en door wie?

Zie voor informatiebeveiliging van de CORV paragraaf 6 en zie paragraaf 7 7 t.a.v. de gebruikers van de berichten en hun eigen ICT.

V. Transparantie en rechten van betrokkenen

V.1. Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden? Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens?

Speelt in feite niet bij de CORV. Veel berichten worden wettelijk verplicht. Daarnaast: alle berichten vloeien voort uit de taken en werkzaamheden van partijen voortvloeien en daarover zal informatie gegevens worden aan de betrokkenen. Voor wat de rechten op kennisneming etc. t.a.v. de inhoud van de berichten betreft vallen deze gegevens onder de reguliere verwerkingen van de verzenders en ontvangers van de berichten.

V. 2. Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?

Zie V.1

V. 3. Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?

Zie V.1

V.4. Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?

Zie V.1

V.5. Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?

Zie V.1

6. Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?

Zie V.1