Harmonisatie maatregelen informatiebeveiliging Wvggz

Routering

		Geplande datum/ werkelijk datum	Geplande versie/ Werkelijke versie
BKR	Ter vaststelling	12 dec 2018	Versie 6
LKO	Voor advies BKR	15 nov 2018	Versie 5
CIO-overleg	Voor advies BKR	7 nov 2018	Versie 5
Werkgroep IB	Laatste review	22 okt 2018	Versie 4

Versie historie

Versie	Datum	Wijzigingen
Versie 2	12 juli 2018	Eerste versie opgesteld op basis van analyse en bilateraal overleg. Ter bespreking in en ter review door werkgroep.
Versie 3	-	Interne versie
Versie 4	15-10-2018	Aangepaste versie op basis van uitwerking van de resultaten van de review.
Versie 5	26-10-2018	Aangepaste versie op basis van bespreking in het overleg werkgroep IB, dd. 22-10-2018.
Versie 6	20-11-2018	Aangepaste versie op basis van inhoudelijke bespreking in CIO-overleg, dd. 7-11-2018 en laatste opmerkingen vanuit JenV.
Versie 1.0, Definitief	12-12-2018	Vaststelling door BKR, dd. 12-12-2018

Programma Wvggz

Frank Hendriksen en Theo Heinsbroek

15 december 2018

Versie 1.0, Definitief

Inhoud

Inleiding

Het programma Wvggz, is in opdracht van de bij de uitvoering van de wet Verplichte GGZ[1] betrokken partijen[2], de voorbereidingen aan het treffen voor de uitvoering van deze wet. Onderdeel hiervan is het voorbereiden van de informatievoorziening van en tussen deze partijen en verdere betrokkenen.

Onder deze wet wordt op specifieke momenten in de samenwerking informatie uitgewisseld, waaronder gevoelige medische, justitiële- en politiegegevens. Het betreft hier bijzondere persoonsgegevens van toch al kwetsbare jeugdigen en volwassenen. Verlies, ongeoorloofd of onrechtmatig gebruik kan grote impact hebben op de persoonlijke levenssfeer van betrokkenen. Denk hierbij o.a. aan stigmatisering. Beveiliging samen op orde hebben, is niet alleen een vereiste, maar ook van groot maatschappelijk en sociaal belang. Informatie wordt bij de uitvoering van deze wet op diverse manieren uitgewisseld variërend van mondeling tot verregaand geautomatiseerd.

Iedere organisatie die betrokken is bij de uitvoering van de Wvggz heeft een eigen wettelijke taak en is zelfverantwoordelijk voor de bijbehorende informatiebeveiliging. Informatiebeveiliging gaat over drie zaken:

- Beschikbaarheid (ook wel continuïteit)
  Zorgen dat de informatie beschikbaar en toegankelijk is zodat de wettelijke of opgedragen taak kan worden uitgevoerd. Daaronder vallen dus ook continuïteitsmaatregelen om bij het uitvallen van een informatiesysteem uit te kunnen wijken naar een andere manier om de wettelijke of opgedragen taak uit te kunnen voeren.
- Integriteit
  Zorgen dat de informatie juist en volledig is en de juiste actualiteit heeft.
- Vertrouwelijkheid (ook wel exclusiviteit) inclusief privacy
  Zorgen dat alleen de juiste personen bij de informatie kunnen inclusief zorgen dat hierbij niet de privacy van iemand geschonden wordt.

De wettelijke taak van elke organisatie kan effectief worden uitgevoerd met in achtneming van de bescherming van de persoonlijke levenssfeer als de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie is geborgd. Elke organisatie is echter afhankelijk van andere organisaties die die informatie moet verstrekken. Als een andere organisatie de benodigde informatie niet of niet op tijd of met onvoldoende kwaliteit levert, kan men simpelweg de wettelijke taak niet uitvoeren. Andersom moet iedere organisatie die informatie moet verstrekken het vertrouwen hebben dat ze deze informatie mag verstrekken en dat de ontvanger deze gegevens betrouwbaar verwerkt. Twijfel hieraan kan de samenwerking laten haperen met soms verstrekkende risico's tot gevolg. Om die reden moeten organisaties hierover dus afspraken maken met elkaar.

In dit document worden de eerste afspraken geformuleerd. Hiertoe doen partijen een geharmoniseerde uitspraak over de te hanteren principes voor veilige informatie-uitwisseling, het vereiste informatiebeveiligingsniveau en de belangrijkste beveiligingsmaatregelen.

Het is van belang, met name gezien de AVG eisen, om duidelijk te zijn over wanneer de verwerkingsverantwoordelijkheid van elke partij begint, zodat altijd duidelijk is waar gegevens verwerkt worden en namens wie.

[1] https://www.dwangindezorg.nl/nieuwe-wetgeving/wet-verplichte-ggz

[2] GGZ-sector, Gemeenten, Openbaar Ministerie, Rechtspraak, Politie, IGJ, ministerie VWS, ministerie JenV en vertegenwoordiging patiënten

De Gemeenten, de GGZ-zorgleveranciers, de IGJ, het Openbaar Ministerie en de rechtspraak hebben besloten samen tot deze beveiligingsmaatregelen te willen komen. De Stichting PVP en de Politie hebben aangegeven dat ze zullen aansluiten op deze keus. Het ministerie JenV heeft laten weten dat hun betrokkenheid beperkt kan blijven tot toetsing en advisering indien nodig. Het ministerie van VWS (directie I) heeft aangegeven geen actieve rol voor zichzelf te zien maar wil wel graag geïnformeerd blijven over de voortgang en de resultaten.

Deze notitie schetst deze geharmoniseerde beveiligingsmaatregelen op basis van de principes, geldende normenkaders, gegevens classificatie en overleg met verantwoordelijken van genoemde partijen.

Besluitvorming

Deze notitie wordt ter vaststelling aangeboden aan het bestuurlijk overleg (BKR) van het programma Wvggz. Hiertoe vindt eerst afstemming plaats met de contactpersonen (zie bijlage A) per organisatie, deze zullen daarvoor ook hun achterban moeten raadplegen. Ook zullen de partijen die niet actief medeopstellers zijn worden gevraagd deze notitie van commentaar te voorzien. Aanvullend zal afgestemd worden met de projectleiders en architecten en leden van de programma specifieke overleggen LKO en CIO-overleg.

Het vaststellen van deze notitie staat los van de zelfstandige verantwoordelijkheid voor informatiebeveiliging en privacy van elke organisatie. Deze exercitie kan deze niet vervangen.

De mogelijke schade die door een dreiging kan worden toegebracht aan bepaalde informatie en de kans dat het optreedt, kan formeel met een risicoanalyse worden geëvalueerd. In de vigerende normenkaders voor informatiebeveiliging wordt de methode classificatie als alternatief voor een risicoanalyse genoemd. Het uitgangspunt is dat deze vorm van risicoanalyse als afdoende wordt beschouwd. Het staat ketenpartners uiteraard vrij om alsnog een risicoanalyse te gebruiken en de classificatievoorstellen aan te passen.

De afspraken moet echter voldoende zijn om als uitgangspunt te dienen voor de verdere uitwerking van ketenafspraken en keten IV-voorzieningen. Mocht later blijken dat een partij alsnog wil besluiten tot een afwijkend beveiligingsniveau of maatregel dan zal hiervoor binnen de ketensamenwerking een oplossing gezocht moeten worden.

Voor alle hier genoemde maatregelen geldt dat uiteindelijk in de uitwerking moet worden afgewogen of de betreffende maatregelen proportioneel en uitvoerbaar en werkbaar zijn. Met name in die situaties van samenwerking waar sprake is van bijzondere omstandigheden moet dit goed worden afgewogen. Bijvoorbeeld bij het toepassen van de wet in crisissituaties. Mocht dit leiden tot bijstelling van de maatregelen dan vereist dit afstemming tussen de betrokken partijen via het programma Wvggz.

Principes voor informatiebeveiliging samenwerking Wvggz

Om tot een geharmoniseerde set aan beheersmaatregelen te komen moeten de partijen het eens zijn over de te hanteren principes. Alle partijen onderschrijven de volgende principes:

1. **Organisaties zijn zelfverantwoordelijk voor informatiebeveiliging en privacy en stemmen af in ketenverband.**
   Elke organisatie is zelfverantwoordelijk voor het classificeren van bedrijfsvoering processen en het bepalen en toepassen van de maatregelen rondom informatiebeveiliging inclusief privacy. Om te zorgen dat dit het functioneren van de samenwerking niet in de weg zit stemmen we deze af in ketenverband. De organisaties zullen actief transparant communiceren over hun werkwijze[3]. Indien nodig vindt bijstelling plaats van de afspraken rondom de beveiligingsmaatregelen.

2. **Afspraken gaan eerst over informatieverstrekking tussen mensen in hun organisatorische rol binnen de Wvggz, afspraken over informatie- en communicatiemiddelen zijn een afgeleide daarvan.**
   We maken afspraken over informatiebeveiliging binnen het samenwerkingsproces tussen mensen in hun rol binnen de Wvggz, dat is dus ongeacht de wijze van communiceren die ze daarbij gebruiken. De eisen aan de informatievoorziening en communicatiemiddelen volgen daaruit maar zijn niet noodzakelijk identiek, aangezien zowel organisatorische en technische maatregelen genomen kunnen worden om de afspraken na te komen.

3. **Informatiebeveiliging wordt situationeel afgewogen tegen andere risico's.**
   Van het afgesproken vereiste informatiebeveiligingsniveau op het samenwerkingsproces kan situationeel worden afgeweken indien deze (nog) niet haalbaar is of keuzes gemaakt moeten worden tussen conflicterende kwaliteitseisen en risico's (bijvoorbeeld beschikbaarheid versus privacy). Afwijkingen worden vastgelegd als (rest)risico in het kader van de bedrijfsvoering en voorgelegd ter goedkeuring aan de eigenaar van het bedrijfsproces binnen de betreffende organisatie.

4. **De informatiebeveiliging gaat uit van een federatieve benadering.**
   We gaan zoveel als mogelijk uit van een federatieve benadering. Dat wil zeggen dat we afspraken maken op organisatieniveau die het mogelijk maken dat toegang tot systemen en gegevens zoveel mogelijk beheerd worden door de gebruikende organisatie. Dit vereist afspraken en vertrouwen in elkaars informatiebeveiligingsprocessen[4],

5. **Organisaties maken onderling afspraken over gegevensverwerking en maken zelf afspraken met hun eigen gegevensverwerkers.**
   De verantwoordelijken voor gegevensverwerking maken afspraken met elkaar over informatie-uitwisseling (horizontale afspraken), elke organisatie maakt dan afspraken met

[3] Actieve en transparante communicatie is bijvoorbeeld van belang bij het delen van incident informatie aan andere ketenpartners, als daar een aanleiding voor is. Dit geldt bijvoorbeeld ook voor andere beveiligingsafspraken zoals het (actief) monitoren van in- en uitgaande verkeersstromen en het beschikbaar hebben van relevante loginformatie en het verstrekken van loginformatie in het geval van een data lek.

[4] Met informatiebeveiligingsprocessen bedoelen we vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging conform NEN-ISO/IEC 27001:2013.

zijn eigen gegevensverwerkers (verticale afspraken conform o.a. AVG). Organisaties maken geen afspraken direct met de gegevensverwerker van een andere organisatie.

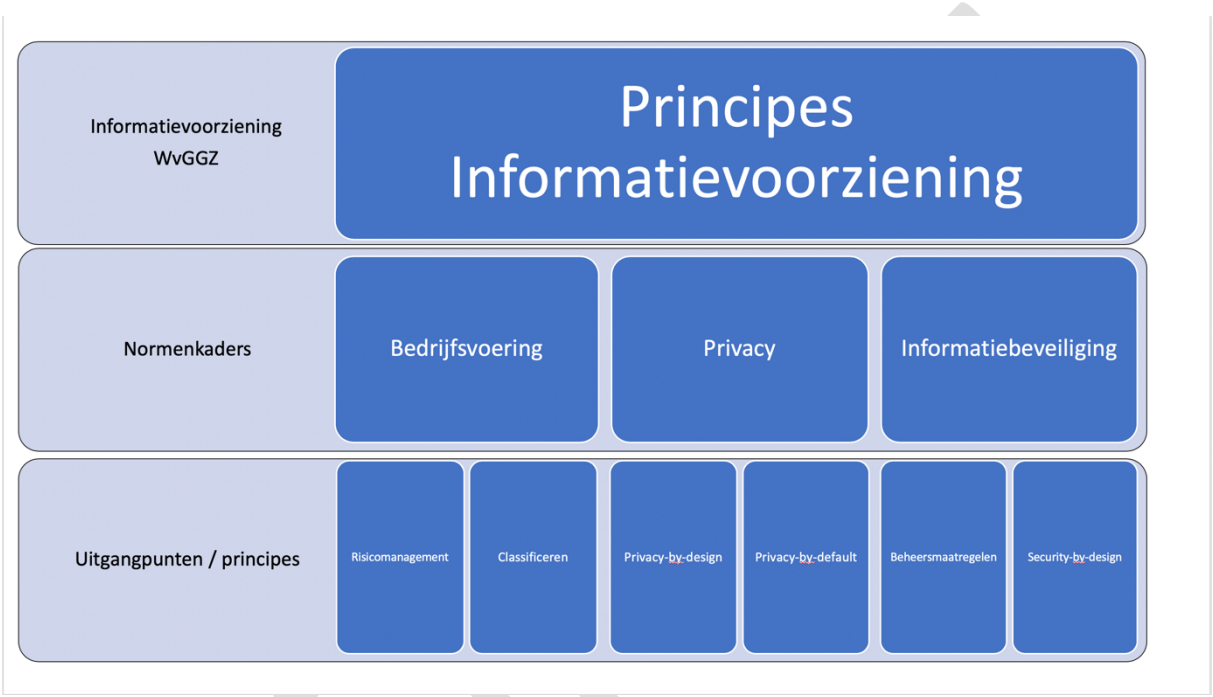
6. **Afspraken over compliance hergebruiken bestaande compliance eisen en processen.**
   We maken afspraken over het toezicht op elkaars beveiligingsmaatregelen en -processen door zoveel mogelijk gebruik te maken van bestaande compliance eisen en processen, zodat er bij voorkeur geen extra compliance belasting komt voor de organisaties.

7. **Van elke verstrekking is exact afgesproken op welke moment de verwerking van de ontvanger start.**
   Het is van belang, met name gezien de AVG eisen, om duidelijk te zijn over wanneer de verwerkingsverantwoordelijkheid van elke partij begint, zodat altijd duidelijk is waar gegevens verwerkt worden en namens wie.
   We gaan ervan uit dat in alle gevallen van communicatie er sprake is van communicatie tussen actoren die een eigen taak hebben in het kader van de Wvggz of andere betrokkenen die recht hebben op het krijgen van de gegevens en dus al deze actoren en betrokkenen zelfverantwoordelijk zijn voor de verwerking van de ontvangen gegevens conform het doel waarvoor zij het hebben ontvangen. Hierdoor voorzien we dus dat er geen situaties zullen zijn waarbij de een actor van een organisatie gegevens verwerkt onder de verantwoordelijkheid van een andere organisatie.

8. **Verwerking van ontvangen informatie is altijd tot een natuurlijk persoon traceerbaar.**
   Ontvangende organisaties zorgen dat de (al dan niet geautomatiseerde) verwerking van aan hun verstrekte informatie inzichtelijk is tot op de persoon.

9. **De organisaties hebben aantoonbaar hun (bedrijf)proces en informatie geclassificeerd voordat informatie gedeeld wordt met ketenpartners.**
   Het toekennen van classificatieniveaus aan het bedrijfsproces en aan de te delen informatie is van groot belang, omdat daarmee het (vereiste) beschermingsniveau van het (bedrijf)proces en de te delen informatie kenbaar gemaakt wordt, zodat weloverwogen informatie gedeeld kan worden met ketenpartners.

De overeengekomen principes voor informatievoorziening binnen de ketensamenwerking zijn de grondslag voor de samenwerking en voor het maken van ketenafspraken. Deze principes zijn ontstaan uit de wens tot samenwerking tussen de ketenpartners en worden gekoppeld aan de verplichte normenkaders voor bedrijfsvoering, informatiebeveiliging en privacy. De bij de ketenpartners verplichte gestelde normenkaders voor bedrijfsvoering, informatiebeveiliging en privacy zijn de nadere specificatie en invulling van de principes (conform pas-toe of leg-uit principe) in de vorm van toe te passen uitgangspunten die ketenpartijen zelfstandig moeten treffen als invulling voor het waarborgen van de principes en aantoonbaar voldoen aan de geldende normenkaders.



Geldende normenkaders

De vijf organisaties die tot een geharmoniseerde uitspraak willen komen hanteren vier verschillende normenkaders voor beveiliging. Sommige normenkaders beschrijven een minimum beveiligingsniveau met maatregelen die toch al genomen moeten zijn. Dit is het basisniveau.

De Politie en de Stichting PVP kennen geen specifieke baselines als normenkader voor informatiebeveiliging, maar hanteren een risicomanagement aanpak. Beide organisaties zijn gedurende de ontwikkeling van dit normenkader voor ketensamenwerking geconsulteerd en actief betrokken. Beide organisaties hebben aangegeven in te stemmen met dit normenkader.

Vooral waar de Wvggz specifieke beveiligingseisen tot gevolg heeft die hoger zijn dan dit basisniveau zullen extra maatregelen nodig zijn. De volgende tabel laat zien welke organisatie aan welke beveiligingsnorm moet voldoen en wat het basisniveau van beveiliging is volgens die norm.

	Gemeenten	GGZ	OM	IGJ	Rechtspraak
Beveiligings-norm	BIG:2014	NEN7510	BIR:2017	BIR:2017	Rechtspraak specifiek (gebaseerd op BIR)
Basisniveau waar organisaties al aan (moeten) voldoen	Beschikbaarheid (1-belangrijk) Integriteit (2-hoog) Vertrouwelijkheid (2-vertrouwelijk)	Zekerheidsniveau Laag	Basisbeveiligings-niveau 1 (BBN1)	Basisbeveiligings-niveau 1 (BBN1)	Dep V (Vertrouwelijk) *(Geen basisniveau voor beschikbaarheid en integriteit)*
Noot: **Voor overheidsorganisaties geldt dat per 1-1-2020 de Baseline Informatiebeveiliging Overheid (BIO) opgenomen wordt als standaard voor informatiebeveiliging.**					

Alle genoemde normenkader bevatten een zogenaamde good practices voor (gegevens)classificatie. Classificatie van gegevens maakt het mogelijk om die bepaalde gegevens adequaat te beschermen en impliciet voor te schrijven welke beheersmaatregelen (bijv. ten aanzien van identificatie en authenticatie) moeten worden genomen. In het volgende hoofdstuk wordt het principe voor classificeren nader uitgewerkt.

Classificeren is een vorm van een risicoafweging, daarbij wordt een inschatting gemaakt van mogelijke schade als gegevens (bijv. in een bedrijfsproces of binnen een informatiesystemen) (tijdelijk) niet beschikbaar zijn, de gegevens niet integer is en/of deze in verkeerde handen vallen. In een risicoafweging wordt normaliter ook een inschatting gemaakt van de dreigingen waartegen beschermd moet worden. De inschatting van mogelijke schade en dreigingen leidt tot beveiligingseisen om het risico te beperken. Om deze eisen af te dekken worden passende beheersmaatregelen getroffen of wordt het (rest)risico geaccepteerd door de eigenaar van de gegevens.

Classificeren en authenticeren

Classificeren geeft een goede indicatie van het belang van de informatie (in processen en informatiesystemen) en is daarmee de basis voor het (vereiste) beveiligingsniveau.

De mogelijke schade die door een dreiging toegebracht kan worden aan bepaalde informatie en de kans dat het optreedt, kan met een risicoanalyse worden geëvalueerd. Risicoanalyses zijn vaak tijdrovend en een abstract traject. In de eerdergenoemde normenkaders wordt classificatie als alternatief genoemd voor een risicoanalyse. Het staat ketenpartners vrij om alsnog een risicoanalyse uit te voeren.

Het toekennen van classificatieniveaus aan gegevens en/of informatiesystemen is van groot belang, omdat daarmee het (vereiste) beveiligingsniveau kenbaar gemaakt wordt. Aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke beheersmaatregelen moeten worden genomen. Classificeren is ook aanwezig als instrument in de handreiking betrouwbaarheidsniveaus digitale dienstverlening[5]. Generiek genomen geldt dat op basis van deze handreiking de classificatie van de gegevens strikt genomen eIDAS “hoog” is.

De classificatie eIDAS “hoog” hoeft echter niet op elk proces- en of ketenniveau doorgevoerd te worden door het implementeren van alle beheersmaatregelen. Voor de classificatie eIDAS “hoog” geldt immers nog steeds de gedoogsituatie van de Autoriteit Persoonsgegevens (AP), mede omdat nog niet alle middelen voor authenticatie beschikbaar zijn en doordat er beperkingen zijn die ervoor zorgen dat niet alle middelen beschikbaar kunnen zijn.

Tijdens de verdere verwerking van persoonsgegevens komen gegevens of documenten voor die, los van de (eigen) dienst, bewijzen dat de gebruiker echt betrokken is bij de dienst en er toestemming voor heeft gegeven. Door deze risicoverlaging kan het eIDAS “hoog” niveau verlaagd worden naar eIDAS “substantieel” [6].

Conclusie: de classificatie van de gegevens is inderdaad eIDAS “hoog”, maar kan op basis van de Handreiking betrouwbaarheidsniveaus digitale dienstverlening verlaagd worden naar “substantieel[7][8]”.

Het is de eigenaar van de gegevens die uiteindelijk bepaalt of de classificatie juist is, maar ook of het restrisico acceptabel is. Als dit het geval is, kan beargumenteerd worden afgeweken van de aan de classificatie gekoppelde maatregelen. Het beschermingsniveau van gegevens wordt uitgedrukt in een classificatie ten aanzien van de beschikbaarheid, integriteit en vertrouwelijkheid. Hierbij wordt onderscheid gemaakt tussen reguliere werkprocessen en crisis werkprocessen. In het volgende hoofdstuk wordt het (vereiste) beveiligingsniveau uitgewerkt.

---

[5] https://www.forumstandaardisatie.nl/nieuws/lancering-regelhulp-betrouwbaarheidsniveaus-voor-digitale-dienstverlening

[6] Op basis van handreiking betrouwbaarheidsniveaus digitale dienstverlening, Forum Standaardisatie, april 2017. Uitkomst regelhulp komt uit op niveau Hoog met een risico verlagende factor. Namelijk: In het vervolgproces komen gegevens of documenten voor die, los van uw dienst, bewijzen dat de gebruiker echt betrokken is bij uw dienst en er toestemming voor heeft gegeven. Hierdoor komt het niveau uit op Substantieel.

[7] eIDAS “substantieel” is gelijkgesteld met niveau 3 van e-Herkenning. Voor authenticatie geldt dus dat naast een userID en wachtwoord een extra authenticatiemiddel nodig is.

[8] Het BKR heeft, bij de vaststelling van dit document, afgesproken dat beveiligingsniveau 4 voor de keten in zijn geheel op termijn wordt nagestreefd.

Vereiste beveiligingsniveau informatie Wvggz

Vanuit de analyse van de wet en de afgeleide ketenwerkprocessen met de partijen zijn ca. 130 uitwisselingsmomenten van informatie geïdentificeerd. Dit is nog exclusief een aantal te verwachten detail afstemmingen tussen partijen die nodig zullen zijn maar nog niet concreet zijn gemaakt.

Omdat het in dit stadium nog niet mogelijk is om elk uitwisselingsmoment individueel te classificeren voor beveiligingseisen doen we dit globaler. Daarvoor zijn in onderstaande kruistabel (zie ook bijlage B) de overdrachtsmomenten samengevat in 31 bilaterale informatiestromen tussen partijen.

We constateren dat in elk van deze informatiestromen gegevens worden uitgewisseld met persoonsgegevens en zeer vaak bijzondere persoonsgegevens[9]. Deze laatste categorie mag alleen gebruikt worden als daarvoor een wettelijke grondslag is. Dat is voor de Wvggz het geval maar dit stelt hoge eisen aan met name de vertrouwelijkheid.

Voor integriteit en vertrouwelijkheid (op werkproces niveau) gaan we uit van één niveau voor alle informatiestromen.

Voordat een partij (organisatie of burger) daadwerkelijk toegang krijgt tot systemen en/of informatie binnen de ketensamenwerking geldt dat de identificatie van die partij eenduidig vastgesteld is.

Voor beschikbaarheid (proces niveau) gelden hogere eisen voor de informatiestromen die nodig zijn in het kader van werkprocessen met een hoge urgentie (essentieel). Dit is namelijk bij de samenwerking in het kader van de (verlenging van de) crisismaatregel. De overige werkprocessen stellen lagere eisen aan de beschikbaarheid (noodzakelijk) van de informatiestromen. In bijlage B is aangegeven welke informatiestromen nodig zijn bij de uitvoering van de werkprocessen met een hoge urgentie.

De volgende kruistabel laat zien welke informatiestromen nodig zijn, wie aan wie informatie moet verstrekken. Alle rood omkaderde aangegeven informatiestromen zijn essentieel om de wettelijke taken in het kader van de (verlenging van de) crisismaatregel te kunnen uitvoeren en vereisen beschikbaarheid Essentieel.

Naar/ Ontvangen Van/ Verstrekken	Gemeente	GGZ	OM	Rechtspraak	IGJ	St PVP	Politie	Overig	Min JenV
Gemeente	-	X[1]	X[3]	-	X[2]	X[5]	-	X[4]	-
GGZ	X[10]	X[7]	X[6]	X[12]	X[11]	X[9]	-	X[8]	X[13]
OM	X[17]	X[14]	-	X[15]	-	-	X[18]	X[16]	-
Rechtspraak	X[23]	X[20]	X[21]	-	X[19]	-	-	X[22]	-
IGJ	-	-	-	-	-	-	-	-	-
StPVP	-	-	-	-	X[24]	-	-	-	-
Politie	-	-	X[31]	-	-	-	-	-	-
Overig	X[27]	X[28]	X[26]	X[29]	X[25]	-	-	-	-
Min JenV	-	X[30]	-	-	-	-	-	-	-

[9] https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens

In dit stadium is nog niet bekend met welke communicatiemiddelen de informatie wordt uitgewisseld/ verstrekt. Dat kan dus zijn telefonisch, fysieke post, fax, veilige e-mail, toegang via website/portaal, systeem koppelingen tussen systemen, etc. De principes en beveiligingsmaatregelen zijn soms echter specifiek gericht op digitale communicatiemiddelen; een aantal is ook van toepassing op andere vormen van communicatie.

Op basis van de nu beschikbare uitwerking van de ketenprocessen en de daarin uitgewisselde informatie komen we tot de volgende vereiste beveiligingsniveaus.

Vereiste classificatie Integriteit en Vertrouwelijkheid[10]					
	Gemeenten	GGZ	OM	IGJ	Rechtspraak
Voor alle ketenprocessen	Integriteit (2-hoog) Vertrouwelijkheid (2-vertrouwelijk)	Hoog Maatregelen op zekerheidsniveau Hoog	BBN2, wellicht extra maatregelen nodig op Integriteit	BBN2, wellicht extra maatregelen nodig op Integriteit en Vertrouwelijkheid, vergelijkbaar met WGBO	Dep V (Vertrouwelijk), deels Dep V (Hoog Vertrouwelijk) *Geen classificatie voor Integriteit*

Vereiste classificatie Beschikbaarheid					
	Gemeenten	GGZ	OM	IGJ	Rechtspraak
Ketenprocessen Crisismaatregel en Verlenging Crisismaatregel = Beschikbaarheid Essentieel	Essentieel	Hoog	BBN2	BBN2	*Geen classificatie voor beschikbaarheid)*
Overige ketenprocessen = Beschikbaarheid Noodzakelijk	Noodzakelijk	Hoog	BBN2	BBN2	*Geen classificatie voor beschikbaarheid*
Noot: **Voor overheidsorganisaties geldt dat per 1-1-2020 de Baseline Informatiebeveiliging Overheid (BIO) opgenomen wordt als standaard voor informatiebeveiliging.**					

Hierbij dienen ook aantoonbaar de (eigen) wettelijke verplichtingen[11] gevolgd te worden, zoals de eisen vanuit de AVG en eisen rond archiveren voor de ketenpartijen.

De AVG en eisen rond archiveren moeten dus in onderlinge samenhang bekeken worden. Dit geldt met name voor het bewaren en vernietigen van persoonsgegevens. Voor het bewaren van persoonsgegevens gelden soms vaste bewaartermijnen in specifieke wetgeving zoals bijvoorbeeld de Wet justitiële en strafvorderlijke gegevens. Als er geen specifieke wetgeving met een bewaartermijn aanwezig is, stelt de AVG dat persoonsgegevens slechts bewaard mogen worden voor zolang dat noodzakelijk is. Het belang van archivering kan blijvende bewaring van archiefbescheiden met persoonsgegevens noodzakelijk maken.

[10] Als hogere classificaties dan de hiergenoemde niveaus voorkomen dan moeten de specifieke classificatieprocessen voor die hogere classificatie niveaus gevolgd worden.
[11] https://www.nationaalarchief.nl/archiveren/kennisbank/vastgestelde-selectielijsten

De eisen rond archiveren bevatten zelf geen concrete bewaartermijnen, maar de verplichting om deze voor archiefbescheiden vast te leggen. De eisen rond archiveren schrijven voor dat een selectielijst moet worden opgesteld met bewaartermijnen. Bij het bepalen van deze termijnen moet een belangenafweging plaatsvinden en onder meer gemotiveerd worden waarom bepaalde archiefbescheiden permanent bewaard worden. Daarbij moet ook rekening worden gehouden met persoonsgegevens die onderdeel zijn van archiefbescheiden. Deze belangenafweging, waarvan de AVG dus onderdeel uitmaakt, moet zijn neerslag vinden in de selectielijst.

Als in het kader van de AVG wordt besloten tot aangepaste – bijvoorbeeld kortere - bewaartermijnen vanwege in archiefbescheiden aanwezige persoonsgegevens, moeten deze ook worden vastgesteld in een selectielijst.

Geharmoniseerde maatregelen

Op basis van bovenstaande normen en classificaties stellen we de volgende geharmoniseerde maatregelen voor.

Authenticatie en identificatie organisaties

1. **De volgende organisaties worden in het licht van deze afspraken erkend als organisaties die vanuit hun wettelijke rol informatie uitwisselen in het kader van de Wvggz: het Openbaar Ministerie, alle rechtbanken, de Hoge Raad, alle gemeenten, de Nationale Politie, de stichting PVP, de landelijke stichting Familievertrouwenspersonen (LSFVP), de Raad voor Rechtsbijstand (RvR).**
2. **Zorgaanbieders zijn rechtspersonen en worden in het licht van deze afspraken erkend als organisaties die vanuit hun wettelijke rol informatie uitwisselen in het kader van de Wvggz zolang ze correct geregistreerd staan in het openbaar register conform artikel 1:2 Wvggz.**

Toelichting:

De organisaties die uitvoering geven aan de Wvggz zijn vrijwel allemaal vooraf bekend bij alle partijen. De partijen gaan er vanuit dat artikel 1:2 Wvggz uitgelegd moet worden als of registratie van organisaties vooraf plaats gevonden heeft, voorafgaand aan het vervullen van een rol in het kader van de Wvggz. Om deze reden wordt hier afgesproken dat alleen als die registratie actueel en correct is de informatie-uitwisseling met die geregistreerde rechtspersoon kan worden ingericht volgens deze afspraken. Het sluit niet uit dat een zorgaanbieder toch een rol heeft in de Wvggz en dat andere organisaties daarmee informatie moeten kunnen uitwisselen.

Uitschrijving van een deelnemer uit het register moet leiden tot het staken van de (geautomatiseerde) informatie-uitwisseling.

Authenticatie bij toegang

3. **Authenticatie van personen voor het toegang krijgen tot gegevens geschiedt op het niveau eHerkenning - niveau 3/ eIDAS substantieel.**
4. **Het middel voor authenticatie om personen namens een rechtspersoon toegang te geven tot gegevens is eHerkenning indien mogelijk.**
5. **Medewerkers toegang geven tot gegevens mag ingericht worden met single sign-on mits gebaseerd op SAML[12] en wordt aangevuld worden met two-factor authenticatie.**

Toelichting:

De afspraken 3 en 4 gaan over de wijze waarop personen toegang kunnen krijgen tot applicaties/ website/ portalen van erkende organisaties en waar het van belang is dat de identiteit van de persoon en zijn relatie met zijn organisatie met voldoende zekerheid moet worden vastgesteld. Voor authenticatie van medewerkers tussen erkende organisaties kan, indien betrokken organisaties dat met elkaar overeenkomen, single sign-on oplossingen worden ingezet en is gebaseerd op SAML. Toegang tot gegevens is voor interne en externe medewerkers op het niveau eIDAS “substantieel”, of eHerkenning-3. Afwijkingen hiervan zijn

[12] https://www.forumstandaardisatie.nl/standaard/saml, SAML is momenteel opgenomen op de pas-toe of leg-uit lijst van het forum. Nieuwe standaarden zoals bijv. REST/JSON en OAUTH mogen gebruikt worden als deze geen afbreuk doen aan het gevraagde betrouwbaarheidsniveau.

toegestaan, mits toegepast conform het principe pas-toe of leg-uit, en vastgelegd en goedgekeurd tussen de betrokken ketenpartijen.

6. **Tussen partijen worden afspraken gemaakt over de wijze van identificatie van communicerende entiteiten. Waar mogelijk en nuttig wordt afgesproken bestaande landelijke registers te gebruiken (Basisregistratie Personen (BRP), Handelsregister (HR), Beroepen in de Individuele Gezondheidszorg (BIG), AGB-register). Waar mogelijk worden afspraken gemaakt over vertrouwde identiteitsbronnen[13].**

   Toelichting:

   Bij het uitwisselen van informatie wordt veelvuldig verwezen naar personen en organisaties, locaties die informatie verstrekken of moeten ontvangen. Bijvoorbeeld de betrokkene, de geneesheer-directeur, de officier van justitie, de instelling, de gemeente, etc. Om de informatieverwerking soepel te laten verlopen zullen afspraken gemaakt moeten worden over de wijze waarop naar dergelijke communicerende entiteiten wordt verwezen. Waar mogelijk wordt gebruik gemaakt van vertrouwde registraties.

Digitaal transport

7. **Communicatie over niet-vertrouwde netwerken (o.a. internet) verloopt alleen via beveiligde verbindingen (voor alle vormen van digitale communicatie o.a. berichten, e-mail en website toegang).**
8. **Beveiligde verbindingen worden gerealiseerd op basis van authenticatie van de betreffende organisatie met minimaal een middel op het niveau eIDAS substantieel.**
9. **De besloten netwerken Justitienet (van justitie: Openbaar Ministerie, rechtspraak) en Politienet (Nationale Politie) en GGI-Netwerk (gemeenten) gelden als vertrouwde netwerken.**

   Toelichting:

   Een bericht wordt altijd beveiligd getransporteerd tussen de ontvangende en verzendende partij[14]. Het betreft hier een berichtuitwisseling conform technische standaarden van het forum voor standaardisatie. Voor transportbeveiliging gelden minimaal de beveiligingseisen uit de reguliere normenkaders voor informatiebeveiliging en privacy. Om de vertrouwelijkheid van de inhoud te garanderen, worden aanvullende contractafspraken gemaakt met de intermediairs, die zich bevinden in het pad tussen die twee ketenpartners.

Toegangsautorisatie

10. **Toegang tot systemen wordt federatief beheerd.**
11. **Toegang op groepsniveau zijn mogelijk, voor specifieke informatieverstrekkingen, waarbij altijd geldt dat toegang tot een informatieobject/ zaakdossier/etc. aantoonbaar herleidbaar is naar een natuurlijk persoon**
12. **Toegangsautorisaties mogen gebruikt worden voor toegang tot een informatieobject/ zaakdossier/etc. of voor toegang tot een applicatie/ website/ portaal**

    Toelichting:

[13] Vervolguitwerking nodig om te bepalen welke identiteitsbronnen worden gehanteerd.
[14] Adressering vindt plaats aan de hand van het OIN-nummer. VECOZO adresseert op basis van de AGB-code.

Toegangsautorisatie betreft de toegang kunnen krijgen tot een applicatie die gegevens bevat. Dit gaat vooraf aan de autorisatie die dan binnen de applicatie nog nodig is. Toegang geven tot een systeem aan medewerkers van een andere organisatie geschiedt federatief. De betreffende organisatie wijst minimaal één beheerder aan die vervolgens de verantwoordelijkheid draagt om de toegang te beheren voor andere medewerkers. Een medewerker toevoegen aan de groep is dan de manier om hem de autorisatie te geven.

Autorisatie

13. **Iedere organisatie heeft een formele aanvraag-, goedkeurings- en intrekkingsprocedure voor toewijzing en intrekking van toegangsrechten, incl. logging daarvan.**
14. **Groepsaccounts zijn toegestaan in deze processen. Uitgezonderd specifieke gegevens die alleen op combinatie van persoon en casus toegankelijk mogen zijn.**

    Toelichting:

    Autorisatie betreft de toegang kunnen krijgen tot de gegevens in een applicatie. Autoriseren binnen een systeem aan medewerkers van een andere organisatie geschiedt federatief indien de eigenaar van dat systeem dat wenst. De betreffende organisatie wijst minimaal één beheerder aan die vervolgens de verantwoordelijkheid draagt om de autorisaties te beheren voor andere medewerkers binnen dat systeem. Toegang tot gegevens mag indien nodig geregeld worden op groepsniveau. Een medewerker toevoegen aan de groep is dan de manier om hem de autorisatie te geven. De procedures voor aanvragen, goedkeuren en intrekken van autorisaties moeten beschreven zijn en er moet worden toegezien op naleving.

15. **Toegang kan casus gerelateerd zijn op basis van in het proces bepaalde betrokkenheid op aangeven van een communicatiepartij.**

    Toelichting:

    In de samenwerkingsprocessen in het kader van de Wvggz moet het soms mogelijk zijn om toegang af te schermen als de persoon niet betrokken is bij een specifieke casus (bijvoorbeeld een aanvraag voor een zorgmachtiging). In veel gevallen kan en mag dit organisatorisch worden opgelost en aangezien iedere toegang tot gegevens achteraf kan worden herleid tot een persoon. Voor machtiging geldt dat deze toegestaan zijn. De inrichting hiervan is minimaal gelijk aan afspraak 3.

Beschikbaarheid

16. **In ketenwerkprocessen met de beschikbaarheidsclassificatie “Essentieel” is de procesbeschikbaarheid gegarandeerd met een maximale uitval van 30 minuten, met aan maximum van 2 keer uitval per maand.**
17. **In ketenwerkprocessen met de beschikbaarheidsclassificatie “Noodzakelijk” is de procesbeschikbaarheid gegarandeerd met een maximale uitval van 60 minuten gedurende kantoortijden, met aan maximum van 2 keer uitval per maand.**

    Toelichting:

    De informatieverstrekkingen in het kader van de samenwerking in de keten zijn geclassificeerd op basis van de beschikbaarheidseisen in het werkproces. Bij de processen met classificatie Essentieel is het noodzakelijk dat de informatie 24/7 beschikbaar is. Bij de processen met classificatie Noodzakelijk is kantooruren voldoende. In bijlage B is die classificatie opgenomen.

Logging

18. **Partijen geven elkaar op verzoek binnen twee weken inzage in logging.**

    Toelichting:

    Organisaties moeten met vertrouwen de informatie kunnen delen die nodig is voor de samenwerking i.k.v. de WvGGZ zonder dat technische beveiligingsmaatregelen tot diep in elkaars organisaties moeten worden toegepast. Met name de afspraken om op afdelings- en groepsniveau te kunnen verstrekken vereisen wel aanvullende afspraken om er op te kunnen vertrouwen dat de verwerking van die verstrekte gegevens ook van voldoende maatregelen is voorzien. Hiertoe is het een vereiste dat elke aangesloten organisatie de logging bijhoudt conform de eisen uit de eigen normenkaders voor informatiebeveiliging en privacy.

Mobiele apparatuur

19. **Voor mobiele apparaten geldt het Zero-footprint-concept**
20. **Verplichte beveiliging en op afstand wissen.**

    Toelichting:

    Toegang tot informatie met mobiele apparatuur is kwetsbaarder vanwege het ontbreken van fysieke toegang afscherming die normaal wel bij apparatuur op kantoorlocatie wel aanwezig is. Om die reden mogen er geen gegevens op een mobiel apparaat worden opgeslagen tenzij deze versleuteld zijn, conform de eisen voor mobiele apparatuur uit de normenkaders voor informatiebeveiliging en privacy. Als extra maatregel moet het mogelijk zijn om het apparaat op afstand te kunnen wissen mocht die kwijt zijn.

Bijlage A – Contactpersonen per organisatie

In de volgende tabel staan de personen die de contactpersonen zijn bij het opstellen van dit advies.

Vertegenwoordiging van Organisatie/ Branche	Deelnemer	Werkzaam bij	Functie	Contact	Betrokken adviseur
Gemeenten	Bas Nieuwesteeg	VNG Realisatie/ Informatie Beveiligingsdienst	Team Coördinator IBD	bas.nieuwesteeg@vng.nl	Jule Hintzbergen
GGZ-Zorgleveranciers	Jaap Schrieke	GGZ-NL	Beleids-adviseur	JSchrieke@ggznederland.nl	
IGJ	Martijn van Oosten	IGJ	CISO / Privacy Officer	mc.v.oosten@igj.nl	
Openbaar Ministerie	Marcel Hoeke	Openbaar Ministerie	CISO	m.hoeke@om.nl	
Rechtspraak	Arjan Deij	Raad voor de rechtspraak	CISO / plv. landelijk Beveiligings-ambtenaar	a.deij@rechtspraak.nl	Harro Kremer

Bijlage B – Overzicht informatiestromen Wvggz

Afgeleid uit de wet en uitgewerkte werkprocessen waarin samenwerking nodig is tussen de ketenpartners en overige betrokkenen kunnen we de bilaterale informatiestromen (verstrekkingen) identificeren. De onderstaande tabel zijn deze informatiestromen aangegeven (X). De cijfers verwijzen naar de tabel eronder met voorbeelden van de informatie die in die informatiestroom wordt verstrekt. Daar waar een (-) staat is (nog) geen noodzaak tot informatieverstrekking geïdentificeerd.

Naar/ Ontvangen Van/ Verstrekken	Gemeente	GGZ	OM	Rechtspraak	IGJ	St PVP	Politie	Overig	Min JenV
Gemeente	-	X[1]	X[3]	-	X[2]	X[5]	-	X[4]	-
GGZ	X[10]	X[7]	X[6]	X[12]	X[11]	X[9]	-	X[8]	X[13]
OM	X[17]	X[14]	-	X[15]	-	-	X[18]	X[16]	-
Rechtspraak	X[23]	X[20]	X[21]	-	X[19]	-	-	X[22]	-
IGJ	-	-	-	-	-	-	-	-	-
StPVP	-	-	-	-	X[24]	-	-	-	-
Politie	-	-	X[31]	-	-	-	-	-	-
Overig	X[27]	X[28]	X[26]	X[29]	X[25]	-	-	-	-
Min JenV	-	X[30]	-	-	-	-	-	-	-

Toelichting op de in de vorige tabel genummerde informatiestromen.

Nr	Van	Naar	LET OP! Slechts voorbeelden, hier worden niet alle uit te wisselen informatieproducten genoemd!
1.	Gemeente	GGZ	Afgegeven CM, Medische verklaring
2.	Gemeente	IGJ	Afgegeven CM, Medische verklaring (Art 7:2 lid 2)
3.	Gemeente	OM	Afgegeven CM, opvragen Historie, aanvragen verlenging, resultaat verkennend onderzoek
4.	Gemeente	Overig betrokkenen	Resultaat verkennend onderzoek, beslissing OvJ (melder) Afschrift CM (advocaat, gezinsvoogdij, vertegenwoordiger) Verzoek bijstand (RvdRechtsbijstand)
5.	Gemeente	St PVP	Contactgegevens van betrokkene
6.	GGZ	OM	Aanvraag en bescheiden ZM, medische verklaring, Aanvraag politie/justitie gegevens bij CM
7.	GGZ	GGZ	Beslissing wilsonbekwaam, zelfbindingsverklaring, aanwijzing zorgverantwoordelijke, Medische verklaring, zorgkaart, zorgplan
8.	GGZ	Overig betrokkenen	Zelfbindingsverklaring (betrokkene, gezinsvoogdij, vertegenwoordiger) Informatie voorbereiding ZM (advocaat) Besluit schorsing (betrokkene, vertegenwoordiger) Beëindigen verplichte zorg (familie, naasten) Aanwijzing zorgverantwoordelijke (ouders, partner, huisarts)

Nr	Van	Naar	LET OP! Slechts voorbeelden, hier worden niet alle uit te wisselen informatieproducten genoemd!
9.	GGZ	St PVP	Contactgegevens van betrokkene
10.	GGZ	Gemeente	Aanvraag CM, Informatie m.b.t. crisismaatregel, besluit overplaatsing, …
11.	GGZ	IGJ	Besluit overplaatsing
12.	GGZ	Rechtbank	Besluit overplaatsing
13.	GGZ	Min JenV	Verzoek toestemming tijdelijke onderbreking
14.	OM	GGZ	Politie/justitie informatie, aanwijzing GD, historie WvGGZ/BOPZ, politiegegevens, justitiële gegevens
15.	OM	Rechtspraak	Verzoekschrift ZM, verzoekschrift beëindiging ZM
16.	OM	Overig betrokkenen	Besluit geen verzoekschrift (aanvrager, betrokkene, vertegenwoordiger, advocaat)
17.	OM	Gemeente	Historie WvGGZ/BOPZ
18.	OM	Politie	Aanvraag politiegegevens
19.	Rechtspraak	IGJ	Afschrift besluit ZM, uitspraak beëindiging verplichte zorg
20.	Rechtspraak	GGZ	Afschriften uitspraken en besluiten
21.	Rechtspraak	OM	Afschriften uitspraken en besluiten
22.	Rechtspraak	Overig betrokkenen	Verzoek bijstand (RvdRechtsbijstand) Afschrift uitspraak (betrokkene, vertegenwoordiger, advocaat, ouders, partner, gezinsvoogdij-mdw, aanvrager, huisarts)
23.	Rechtspraak	Gemeente	Afschrift beslissing beroep, uitspraak beëindiging verplichte zorg
24.	St PVP	IGJ	Melding tekortkomingen in de zorg
25.	Overige betrokkenen	IGJ	Melding tekortkomingen in de zorg (FVP)
26.	Overige betrokkenen	OM	Aanvraag alsnog verzoekschrift (aanvrager, melder) Aanvraag indienen verzoekschrift beëindiging verplichte zorg (aanvrager)
27.	Overige betrokkenen	Gemeente	Melding crisissituatie (melder) Toestemming verstrekken persoonsinfo(betrokkene) Informatie m.b.t. maatregel (ambulancezorg, door minister aangewezen deskundigen)
28.	Overige betrokkenen	GGZ	Informatie m.b.t. maatregel (ambulancezorg, door minister aangewezen deskundigen) Persoonsgegevens, (kennisgeving) plan van aanpak (betrokkene)
29.	Overig betrokkenen	Rechtspraak	Verzoek beroep CM (betrokkene)
30.	Min JenV	GGZ	Toestemming beëindiging
31.	Politie	OM	Politiegegevens

In de volgende tabel is aangegeven welke informatiestromen cruciaal zijn voor het kunnen uitvoeren van de werkprocessen met een hoge urgentie.

	Van	Naar	Cruciaal voor (verlenging) crisismaatregel?
1.	Gemeente	GGZ	Ja
2.	Gemeente	IGJ	Nee
3.	Gemeente	OM	Ja
4.	Gemeente	Overig betrokkenen	Ja
5.	Gemeente	St PVP	Nee
6.	GGZ	OM	Ja
7.	GGZ	GGZ	Ja
8.	GGZ	Overig betrokkenen	Ja
9.	GGZ	St PVP	Nee
10.	GGZ	Gemeente	Ja
11.	GGZ	IGJ	Nee
12.	GGZ	Rechtbank	Ja (alleen verlenging)
13.	GGZ	Min JenV	Nee
14.	OM	GGZ	Ja
15.	OM	Rechtspraak	Ja (alleen verlenging)
16.	OM	Overig betrokkenen	Nee
17.	OM	Gemeente	Ja
18.	OM	Politie	Ja
19.	Rechtspraak	IGJ	Nee
20.	Rechtspraak	GGZ	Ja (alleen verlenging)
21.	Rechtspraak	OM	Nee
22.	Rechtspraak	Overig betrokkenen	Ja (alleen verlenging)
23.	Rechtspraak	Gemeente	Nee
24.	St PVP	IGJ	Nee
25.	Overige betrokkenen	IGJ	Nee
26.	Overige betrokkenen	OM	Nee
27.	Overige betrokkenen	Gemeente	Nee
28.	Overige betrokkenen	GGZ	Ja
29.	Overig betrokkenen	Rechtspraak	Nee
30.	Min JenV	GGZ	Nee
31.	Politie	OM	Ja