



Privacyprotocol Zorg- en Veiligheidshuis IJsselland

Voor de Integrale Veiligheid en Complexe Multi-problematiek
van zorg- en veiligheidshuis
IJsselland

Ingaande november 2019

CONTEXT

Met dit Privacy Protocol worden afspraken rondom de uitwisseling en het verdere gebruik van persoonsgegevens door en tussen verschillende partijen in het zorg- en veiligheidshuis IJsselland geformaliseerd en vastgelegd. In dit Privacy Protocol ligt vast met welk doel persoonsgegevens worden verwerkt, wie voor welke acties met betrekking tot persoonsgegevens verantwoordelijk is, wanneer er sprake is van gezamenlijke verantwoordelijkheid en hoe invulling wordt gegeven aan de materiële vereisten uit de privacy wet- en regelgeving zoals de informatieplicht, de rechten van de betrokkene, beveiliging en het bewaren en vernietigen van persoonsgegevens.

In dit Privacy Protocol zijn de standaard onderdelen van een samenwerkingsovereenkomst opgenomen, behoudens hetgeen al is geregeld in het bijbehorende Convenant. De precieze verdeling van verantwoordelijkheden, rechten en plichten is uiteindelijk aan partijen zelf in te vullen, tenzij de wet hier een dwingende bepaling over heeft, en dient aan te sluiten op de verdeling van rollen en bevoegdheden zoals belegd in het Convenant.

Formuleringen, begrippen en andere specifieke zorg- en veiligheidshuis-gerelateerde termen zijn afgeleid uit het Handvat “Gegevensuitwisseling in het zorg- en veiligheidsdomein – een juridisch handvat voor zorg- en veiligheidshuizen”, versie 2 van maart 2019 en het Landelijk Kader Veiligheidshuizen. Ook wordt aangesloten bij de werkwijze zoals in het Handvat beschreven. Daarnaast is geput uit een aantal reeds bestaande samenwerkingsconvenanten voor wat betreft onder meer de structuur van het zorg- en veiligheidshuis.

Dit Privacyprotocol en de daarin gehanteerde terminologie is gebaseerd op Algemene Verordening gegevensbescherming, alsook de Wet politiegegevens en de Wet justitiële strafvorderlijke gegevens. Het is tot stand gekomen in samenwerking tussen (privacy)adviseurs van verschillende landelijke partijen, Considerati en het Ministerie van Justitie en Veiligheid.

Privacyprotocol tussen ketenpartners zorg- en veiligheidshuis IJsselland

De ondergetekenden:

De gemeenten,

- Dalfsen, te dezen vertegenwoordigd door de burgemeester
- Deventer, te dezen vertegenwoordigd door de burgemeester
- Hardenberg, te dezen vertegenwoordigd door de burgemeester
- Kampen, te dezen vertegenwoordigd door de burgemeester
- Olst-Wijhe, te dezen vertegenwoordigd door de burgemeester
- Ommen, te dezen vertegenwoordigd door de burgemeester
- Raalte, te dezen vertegenwoordigd door de burgemeester
- Staphorst, te dezen vertegenwoordigd door de burgemeester
- Steenwijkerland, te dezen vertegenwoordigd door de burgemeester
- Zwartewaterland, te dezen vertegenwoordigd door de burgemeester
- Zwolle, te dezen vertegenwoordigd door de burgemeester

verder afzonderlijk aangeduid als 'Partij' of 'Gemeente' en gezamenlijk als 'Gemeenten',

en de bevoegde vertegenwoordigers van:

- Politie Regionale Eenheid Oost-Nederland
- Openbaar Ministerie Arrondissementsparket Oost-Nederland
- Dienst Justitiële Inrichtingen
- GGD IJsselland (waaronder Team VIA)
- Veilig Thuis
- HALT
- Iriszorg
- Trajectum
- Stichting Dimence
- Stichting Transfore
- Leger des Heils
- Reclassering Nederland
- Tactus
- Humanitas
- MEE IJsselland
- Raad voor de Kinderbescherming
- RIBW Groep Overijssel
- Jeugdbescherming Overijssel
- Slachtofferhulp Nederland
- Pactum
- Raster
- Limor
- Trias
- Vitree
- WSG
- Creating Balance
- Stichting De Kern

hierna afzonderlijk te noemen 'Partij' en gezamenlijk, inclusief Gemeente[n], te noemen 'Partijen',

Overwegende dat:

- Partijen in het kader van samenwerking op het gebied van integrale veiligheid en complexe casuïstiek zoals beschreven in het Landelijke Kader het zorg- en veiligheidshuis IJsselland (hierna: 'het zorg- en veiligheidshuis') hebben opgezet;
- Partijen voor deze samenwerking afspraken vastleggen in het Convenant 'Samenwerking tussen ketenpartners in zorg- en veiligheidshuis IJsselland' (verder: het Convenant), welke gelijktijdig met dit Privacyprotocol vastgesteld wordt en waar dit Privacy Protocol deel van uitmaakt;
- voor de samenwerking in het zorg- en veiligheidshuis de uitwisseling van (bijzondere) (persoons-) gegevens tussen de Partijen noodzakelijk is;
- in het door Partijen opgezette zorg- en veiligheidshuis Persoonsgegevens worden verwerkt ten dienste en onder verantwoordelijkheid van Partijen;
- Partijen slechts die Persoonsgegevens binnen het zorg- en veiligheidshuis delen die noodzakelijk zijn voor het doel van de samenwerking;
- op de samenwerking wet- en regelgeving met betrekking tot de bescherming van Persoonsgegevens van toepassing is waarbij Partijen conform deze wet- en regelgeving willen samenwerken;
- dit Privacyprotocol (verder aangeduid als: 'het Protocol') de gedragsregels omschrijft bij het verstrekken en verder Verwerken van Persoonsgegevens door Partijen in het kader van de samenwerking op het gebied van integrale veiligheid en complexe multi-problematiek, alsook de verschillende verantwoordelijkheden met het oog op de rechten en plichten uit toepasselijke privacy wet- en regelgeving, belegd;
- met dit Protocol invulling wordt gegeven aan de in Artikel 26 van de Algemene verordening gegevensbescherming neergelegde verplichting voor Partijen om op een transparante wijze hun samenwerkingsafspraken en hun verantwoordelijkheden jegens elkaar en jegens Betrokkene vast te leggen;
- dit Protocol aansluit bij het bepaalde in het 'Landelijk Kader Veiligheidshuizen' van het Ministerie van Veiligheid en Justitie, vastgesteld in januari 2013 (verder aangeduid als: 'het Landelijk Kader') en het 'Handvat Gegevensuitwisseling in het zorg en veiligheidsdomein – een juridisch handvat voor zorg- en veiligheidshuizen', versie 2.0 van maart 2019, (verder aangeduid als: 'het Handvat'), alsmede bij de in het Handvat en het Landelijk Kader gebezigde terminologie;
- dit privacy protocol verder wordt aangehaald als 'het Protocol'.

verklaren te zijn overeengekomen als volgt:

Artikel 1. Definities

In dit Protocol en de daarbij behorende bijlage(n) wordt verstaan onder:

- 1.1. Persoonsgegevens: de definitie zoals is opgenomen in artikel 4 onder 1 AVG;
- 1.2. Politiegegevens: elk Persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt (artikel 1, sub a, Wet Politiegegevens (verder Wpg));
- 1.3. Strafvorderlijke gegevens: Persoonsgegevens of gegevens over een rechtspersoon die zijn verkregen in het kader van een strafforderlijk onderzoek en die het openbaar ministerie in een straf dossier of langs geautomatiseerde weg verwerkt in een gegevensbestand (artikel 1 sub b Wet justitiële en strafforderlijke gegevens (verder Wjsg));

- 1.4. Justitiële gegevens: bij algemene maatregel van bestuur omschreven Persoonsgegevens of gegevens over een rechtspersoon inzake de toepassing van het strafrecht of de strafbepaling, die in een bestand worden Verwerkt (artikel 1 sub a Wjsg, respectievelijk Besluit Justitiële strafbepalingen (verder Bjsj));
- 1.5. Tenuitvoerleggingsgegevens: persoonsgegevens of gegevens over een rechtspersoon inzake de tenuitvoerlegging van strafrechtelijke beslissingen, die in een dossier of een ander gegevensbestand zijn of worden verwerkt;
- 1.6. Bijzondere Persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 van de Algemene Verordening Gegevensbescherming (verder AVG);
- 1.7. Strafrechtelijke persoonsgegevens: Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (zoals bedoeld in artikel 10 AVG);
- 1.8. Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens (artikel 4 onder 2 AVG);
- 1.9. Betrokkene: de natuurlijke persoon op wie informatie, waaronder Persoonsgegevens, betrekking heeft (artikel 4 onder 1 AVG);
- 1.10. Derde: een natuurlijk persoon of rechtspersoon, niet zijnde de betrokkene, noch één der Partijen van dit protocol;
- 1.11. Verwerkingsverantwoordelijke(n): een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze Verwerking in het Unierecht of het lidstatelijke recht is vastgesteld, kan daarin reeds zijn bepaald wie de Verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen (artikel 4 onder 7 AVG);
- 1.12. Afzonderlijke Verwerkingsverantwoordelijken: Partijen zijn Afzonderlijke Verwerkingsverantwoordelijke voor zelfstandige Verwerkingen en wanneer verschillende Verwerkingen min of meer geïntegreerd zijn, maar geen sprake is van Gezamenlijke Verwerkingsverantwoordelijken;
- 1.13. Gezamenlijke Verwerkingsverantwoordelijken: Van Gezamenlijke Verwerkingsverantwoordelijkheid is sprake wanneer Verwerkingen zijn geïntegreerd, en niet één Partij als Verwerkingsverantwoordelijke kan worden aangemerkt voor de geïntegreerde Verwerkingen. In dat geval zijn de Partijen Verwerkingsverantwoordelijken voor het geheel van de Verwerking;
- 1.14. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt (artikel 4 onder 8 AVG);

- 1.15. Casusregie: het uitvoeren van werkzaamheden gericht het bewaren van de onderlinge samenhang bij het uitvoeren van het gezamenlijk opgestelde plan van aanpak bij het behandelen van één specifieke Casus;
- 1.16. Procesregie: het uitvoeren van werkzaamheden gericht op de totstandkoming van samenwerking tussen Partijen bij het behandelen van één specifieke Casus en de ondersteuning van de Casusregisseur bij de uitvoering van het gezamenlijk opgestelde plan van aanpak;
- 1.17. Casus: een geval of situatie dat of die voldoet aan de criteria voor complexe casuïstiek zoals geformuleerd in Bijlage 2 van het Convenant, en die is Aangemeld bij het zorg- en veiligheidshuis ter beoordeling en eventuele bespreking in het Regionale Casustafel;
- 1.18. Aanmelding: het voordragen van een Casus door één der Partijen en het uitwisselen van informatie, waaronder Persoonsgegevens, tussen de Procesregisseur van het zorg- en veiligheidshuis en de aanmeldende Partij ter toetsing of de Casus in aanmerking komt voor behandeling in het zorg- en veiligheidshuis;
- 1.19. Triage: het proces waarbij relevante Partijen worden bevraagd om te komen tot een nadere afweging ten aanzien van de routing van de casus, tot een bepaling van het doel en de thema's van een eventuele Regionale Casustafel, en tot een afweging welke Partijen relevant zijn om te betrekken bij een Regionale Casustafel;
- 1.20. Regionale Casustafel: fase waarin overleg plaats vindt door Partijen gericht op de totstandkoming van een plan van aanpak, afstemming tijdens de uitvoering daarvan, en het beoordelen of Casus kan worden afgeschaald;
- 1.21. GCOS: Generiek Casusoverleg Onderhoud Systeem;
- 1.22. Multi disciplinair overleg: fase waarin gezamenlijk het plan van aanpak wordt opgesteld;
- 1.23. Afschaling: fases die volgen op het besluit in de Regionale Casustafel dat de betrokkenheid van het zorg- en veiligheidshuis niet langer nodig is, waarin het dossier dat in het systeem van het zorg- en veiligheidshuis is aangelegd ten behoeve van procesregie, geschoond wordt van alle niet langer noodzakelijke informatie, en uiteindelijk verdwijnt uit het systeem van het zorg- en veiligheidshuis;
- 1.24. Procesregisseur: de medewerker van het zorg- veiligheidshuis die namens een van de Partijen is belast met de werkzaamheden in artikel 12 van het Convenant;
- 1.25. Casusregisseur: de medewerker van een van de Partijen die is belast met de taken in artikel 13 van het Convenant;
- 1.26. Manager: de persoon die is belast met de taken zoals geformuleerd in Artikel 11 van het Convenant;
- 1.27. Informatiecoördinator: de persoon die is belast met de taken zoals geformuleerd in Artikel 14 van het Convenant;
- 1.28. Ondersteuner Regionale Casustafels: de persoon die is belast met de taken zoals geformuleerd in Artikel 15 van het Convenant;
- 1.29. Stuurgroep: het verband van afgevaardigden van Partijen zoals geformuleerd in Artikel 4 van het Convenant;
- 1.30. Kerngroepoverleg: het verband van afgevaardigden van Partijen zoals geformuleerd in Artikel 6 van het Convenant;
- 1.31. Privacy adviseur: Ieder zorg- en veiligheidshuis heeft een medewerker die belast is met privacy advisering of kan gebruik maken van een privacy adviseur van een gemeente. Deze

persoon is ook belast met beleidsontwikkeling over gegevensverwerking en helpt mee met de voorbereiding van audits;

- 1.32. Jaarplan: het door de Stuurgroep op grond van Artikel 4.4 van het Convenant vastgestelde plan betreffende de operationele en inhoudelijke kaders en het financieel en inhoudelijk beleid van het zorg- en veiligheidshuis;
- 1.33. Werkprocessen: de door het Kerngroepoverleg op grond van Artikel 6 van het Convenant vastgestelde processen voor samenwerking in het zorg- en veiligheidshuis, waaronder het proces omtrent en het delen van informatie en het Afschalen van een Casus;
- 1.34. AVG: Algemene verordening gegevensbescherming (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG;

Artikel 2. Afzonderlijke en Gezamenlijke Verwerkingsverantwoordelijken

- 2.1. Partijen in het zorg- en veiligheidshuis zijn Afzonderlijk Verwerkingsverantwoordelijke voor de Persoonsgegevens die zij verstrekken aan de Procesregisseur ten behoeve van de Aanmelding en Intake en aan Partijen in het kader van Triage, Regionale Casustafel en Afschaling.
- 2.2. Partijen in het zorg- en veiligheidshuis zijn conform artikel 26 AVG Gezamenlijk Verwerkingsverantwoordelijken voor de Persoonsgegevens die zij, anders dan de verstrekking zoals bedoeld in artikel 2.1, Verwerken op locatie of in de informatiesystemen van het zorg- en veiligheidshuis in het kader van de samenwerking voor de doeleinden zoals omschreven in artikel 3.
- 2.3. Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis door personeel van het zorg- en veiligheidshuis geschiedt onder gezag van de Partij die de betreffende Persoonsgegevens heeft verstrekt. Deze Partij wordt voor die Verwerking aangeduid als Verwerkingsverantwoordelijke.
- 2.4. Wanneer twee of meer Verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de Verwerking bepalen, zijn ze gezamenlijk verantwoordelijk voor die Verwerking in overeenstemming met artikel 26 AVG.

Artikel 3. Doel Verwerking Persoonsgegevens

- 3.1. Dit Protocol ziet toe op alle Verwerkingen van Persoonsgegevens door Partijen in het kader van de uitvoering van artikel 2.2 en 2.3 van het Convenant.
- 3.2. Het verwerken van Persoonsgegevens in het zorg- en veiligheidshuis vindt plaats met als doel het gezamenlijk door Partijen bijdragen aan de veiligheid als onderdeel van het integrale zorg- en veiligheidsbeleid van de Gemeente(n). De samenwerking is meer specifiek gericht op het bijdragen aan de algemene veiligheid, het verbeteren van de persoonlijke situatie, het voorkomen en verminderen van recidive, (ernstige) overlast, criminaliteit, maatschappelijke onrust en maatschappelijke uitval bij complexe problemen, door een combinatie van repressie, bestuurlijke interventie én zorg, hetgeen gezien moet worden als een zwaarwegende taak van algemeen belang. Meer specifiek is het doel van de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis:

- a. het oplossen van complexe multi-problematiek; problematiek waarbij personen die het subject zijn in de casuïstiek te maken hebben met meerdere problemen die op meer dan één leefgebied spelen;
 - b. het voorkomen van (verder) crimineel en/of overlast gevend gedrag of verder afglijden van die personen;
 - c. het oplossen van ernstige lokale of gebiedsgebonden veiligheidsproblematiek; en
 - d. het mogelijk maken van samenwerking met het oog op de hierboven geformuleerde doeleinden, ter voorkoming van maatschappelijke onrust of openbare orde verstoring.
- 3.3. Om het onder artikel 3.2 geformuleerde doel te bereiken Verwerken Partijen gezamenlijk Persoonsgegevens in het kader van Aanmelding, Triage, Regionale Casustafel, MDO en Afschaling. Voor elk van deze fasen in het werkproces zijn specifieke doelen voor de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis van toepassing. Deze doelen zijn gespecificeerd in Bijlage 2.
- 3.4. Partijen Verwerken de Persoonsgegevens die zij in het kader van de samenwerking onder dit Protocol hebben verkregen niet voor andere doeleinden dan de doelen omschreven in artikel 3.2.
- 3.5. Bij het Verwerken van Persoonsgegevens in het zorg- en veiligheidshuis worden de volgende uitgangspunten in acht genomen:
- a. Er is sprake van een strikte doelbinding per fase voor de te Verwerken Persoonsgegevens; en alleen de voor het doel van die fase noodzakelijke persoonsgegevens worden verwerkt;
 - b. Als het doel van de Verwerking van Persoonsgegevens wijzigt, of, de casus gaat door naar een volgende fase, wordt als eerste opnieuw beoordeeld of de eerder verwerkte gegevens ook daarvoor noodzakelijk zijn en vervolgens of de gegevens daarvoor ook (verder) gebruikt mogen worden;
 - c. Een partner die in een bepaalde fase Persoonsgegevens verstrekt behoudt de zeggenschap over het verdere gebruik van die gegevens en of die voor een andere fase en/of andere doelen gebruikt mogen worden;
 - d. Partners die bij de behandeling van een casus kennisnemen van Persoonsgegevens afkomstig van een andere partner mogen deze gegevens enkel verder gebruiken voor hun eigen taken in het kader van de casusbehandeling, als de partner die de gegevens heeft ingebracht, dit afzonderlijk accordeert.

Artikel 4. Categorieën Persoonsgegevens

- 4.1. In het kader van de samenwerking worden door Partijen van de in Bijlage 4 categorieën Betrokkenen de daarin genoemde categorieën Persoonsgegevens Verwerkt:

Toelichting:

Persoonsgegevens betreft informatie die direct of indirect herleidbaar is tot een natuurlijk persoon, zoals geformuleerd in de definities. Dat kan een naam, adres of telefoonnummer zijn, maar ook gegevens over gezondheid, gewoonten, voorkeuren of (strafrechtelijke) verleden. De kring van Betrokkenen kan breder zijn dan één specifieke natuurlijke persoon.

- 4.2. Partijen Verwerken Persoonsgegevens, inclusief Bijzondere en Strafrechtelijke Persoonsgegevens, binnen de wettelijke kaders van de voor iedere Partij toepasselijke wet- en regelgeving.

- 4.3. Partijen Verwerken Persoonsgegevens voor de onder artikel 3.2 geformuleerde doeleinden enkel in de informatiesystemen van het zorg- en veiligheidshuis, of in de door de Stuurgroep aangewezen informatiesystemen en conform het beveiligingsbeleid zoals opgenomen in Bijlage 3 bij dit Protocol.

Toelichting:

Door het Ministerie van Justitie en Veiligheid is voor onder andere overleggen in het zorg- en veiligheidshuis het systeem GCOS ontwikkeld. Indien GCOS door Partijen ook voor andere werkprocessen/ samenwerkingsverbanden dan het zorg- en veiligheidshuis beschreven, wordt gebruikt, dienen deze Partijen er rekening mee te houden dat die gegevensverwerking en de toegangs-autorisaties volstrekt gescheiden dienen te zijn van de Gegevensverwerking van het zorg- en veiligheidshuis in GCOS.

Artikel 5. Verwerkingen en verstrekkingen van persoonsgegevens ten behoeve van het behandelen van een casus

5.1 Verwerking van persoonsgegevens door de procesregisseur

- 5.1.1 De procesregisseur verwerkt persoonsgegevens ten behoeve van de procesregie in het kader van de doelstellingen van de samenwerking zoals verwoord in artikel 3.2 slechts voor zover dit noodzakelijk is voor het bewerkstelligen van de in de desbetreffende fase aan de orde zijnde doelen voor gegevensverwerking als verwoord in artikel 3.3 en bijlage 2.
- 5.1.2 De procesregisseur verwerkt de in het eerste lid bedoelde persoonsgegevens ten behoeve van een goede taakuitoefening van de aanmeldende partij, dan wel de goede taakuitoefening van de partij onder wiens verantwoordelijkheid de casusregisseur zoals verwoord in artikel 12 en 13 van het convenant valt.
- 5.1.3 Voor de verwerking van persoonsgegevens als bedoeld in artikel 5.1.1 zijn van toepassing de grondslag conform de AVG en/of andere wettelijke grondslag, en de wettelijke bepalingen op grond waarvan de aanmeldende partij, dan wel de partij onder wiens verantwoordelijkheid de casusregisseur valt, de casus heeft aangemeld respectievelijk de casusregie voert.
- 5.1.4 De verantwoordelijke voor de verwerking van persoonsgegevens zoals bedoeld in artikel 5.1.1 betreft de verantwoordelijke zoals bedoeld in artikel 2 van dit protocol.

5.2 Verstrekken van persoonsgegevens ten behoeve van aanmelding, triage en Regionale Casustafel en MDO

- 5.2.1 Partijen kunnen persoonsgegevens inbrengen in het kader van de doelstellingen van de samenwerking zoals verwoord in artikel 3.2 slechts voor zover dit noodzakelijk is voor het bewerkstelligen van de in de desbetreffende fasen aan de orde zijnde doelen voor gegevensverwerking als verwoord in artikel 3.3 en bijlage 2.
- 5.2.2 Persoonsgegevens als bedoeld in artikel 5.2.1 worden slechts ingebracht indien dit noodzakelijk is voor de goede vervulling van de eigen taak, en/of de goede uitvoering van de taak van de partij ten behoeve waarvan de werkzaamheden in het kader van aanmelding en intake, screening en weging, of Regionale Casustafel worden uitgevoerd.
- 5.2.3 De grondslag conform de AVG voor het inbrengen van persoonsgegevens als bedoeld in artikel 5.2.1 wordt ontleend aan de eigen taak, en/of de taak van de partij ten behoeve waarvan de werkzaamheden in het kader van aanmelding en intake, screening en weging, of Regionale Casustafel worden uitgevoerd.

- 5.2.4 De verantwoordelijke voor de verstrekking van persoonsgegevens als bedoeld in artikel 5.2.1 betreft de verantwoordelijke zoals bedoeld in artikel 2.1 van dit protocol.

5.3 Verstrekken van gegevens bij het uitvoering geven aan afspraken uit de Regionale Casustafel en MDO

- 5.3.1 Onverminderd het bepaalde in artikel 6 en 7, kunnen partijen persoonsgegevens verstrekken aan een andere partij in het kader van de doelstellingen van de samenwerking zoals verwoord in artikel 3.2 voor zover deze noodzakelijk zijn voor deze partij bij:
- a. het uitvoering geven aan interventies en acties die in de Regionale Casustafel zijn afgesproken
 - b. het voeren van de casusregie op het plan van aanpak als dat in de Regionale Casustafel is afgesproken
 - c. het toedelen van de casus aan een specifieke partij ten behoeve van verdere afhandeling, zoals het adviseren van de aanmelder of het aanbrengen van de casus bij een andere overlegtafel.
- 5.3.2 De grondslag conform de AVG voor het verstrekken van persoonsgegevens als verwoord in artikel 5.3.1 wordt ontleend aan de eigen taak en/of de taak van de partij die de activiteiten onder artikel 5.3.1 a t/m c uitvoert.
- 5.3.3 De verantwoordelijke voor de verstrekking van persoonsgegevens als bedoeld in artikel 5.3.1 betreft de verantwoordelijke zoals bedoeld in artikel 2.1.

Artikel 6 Grondslag voor het verwerken en verstrekken van persoonsgegevens ten behoeve van het behandelen van een casus en de van toepassing zijnde taken van partijen

- 6.1 De grondslag voor de verwerking van persoonsgegevens als bedoeld in artikel 5.1.1, is artikel 6 AVG lid 1 sub e, voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de aanmeldende partner, dan wel de partner onder wiens verantwoordelijkheid de casusregisseur valt. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens (verstrekking aan derden structureel voor samenwerkingsverbanden). Voor gegevens afkomstig van het Openbaar Ministerie, is de grondslag gelegen in de artikel 8a, 39f en 51c Wjsg.
- 6.2 De grondslag voor het inbrengen van persoonsgegevens als bedoeld in artikel 5.2.1, is artikel 6 AVG lid 1 sub e, voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de aanmeldende partner, dan wel de partner onder wiens verantwoordelijkheid de casusregisseur valt, en/of de verstrekken partij. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens. De grondslag voor het verstrekken van justitiële, strafvorderlijke en/of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.
- 6.3 De grondslag voor de verstrekking van persoonsgegevens als bedoeld in artikel 5.3.1, is artikel 6 AVG lid 1 sub e, voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de ontvangende partij en/of de verstrekken partij. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens. De grondslag voor het verstrekken van justitiële, strafvorderlijke en/of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.
- 6.4 De onder 6.1, 6.2 en 6.3 bedoelde grondslag kan bij casussen slechts van toepassing zijn indien dit voortvloeit uit de goede uitvoering van de taken en werkzaamheden van partijen, en de

verwerking plaats vindt namens of de verstrekking plaats vindt aan een van de hieronder a t/m m genoemde partijen en voorwaarden:

- a. het bestuursorgaan de burgemeester: de goede uitvoering van taken en de uitoefening van bevoegdheden van de burgemeester, waaronder in het bijzonder taken en bevoegdheden op het gebied van Openbare Orde en Veiligheid zoals neergelegd in de Gemeentewet artikel 172 lid 3 ter voorkoming van grootschalige maatschappelijke onrust.
- b. het bestuursorgaan het College van B&W: de goede uitvoering van taken van het College van B&W, waaronder in het bijzonder taken in het sociaal domein zoals bedoeld in de WMO artikel 2.3.1 t/m 2.3.5, de Jeugdwet artikel 2,3 en 2.4, de Participatiewet artikel 7.1, en de Wet schuldhulpverlening artikel 3.
- c. het Openbaar Ministerie: voor de strafrechtelijke handhaving van de rechtsorde alsmede andere bij de wet vastgestelde taken (artikel 124 Wet op de Rechterlijke organisatie (verder Wro)). De grondslag voor het verstrekken van justitiële, strafvorderlijke of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.
- d. de politie: vervulling van taken zoals bedoeld in de Politiewet artikel 3, te weten taken op het gebied van opsporing, handhaving van de rechtsorde en hulp aan hen die dat behoeven. De grondslag voor het verstrekken van persoonsgegevens inclusief politiegegevens is gelegen in artikel 20 Wpg. Deze verstrekkingen dienen nader te zijn vastgelegd in de onlosmakelijk bij dit Privacy-protocol behorende en ondertekende Artikel 20 Wpg Beslissing, waarin staat vermeld dat er alleen conform artikel 8 en 13 Politiegegevens worden verstrekt. De Artikel 20 Beslissing wordt ondertekend door de gemandateerde politiechef van de Eenheid, en het gezag te weten de Burgemeesters en de Officier van Justitie. In artikel 7 van de Wpg zijn nadere voorwaarden benoemd die van toepassing zijn op gegevens die in het kader van deze taken worden verstrekt.
- e. de Raad voor de Kinderbescherming: de goede uitvoering van de taken van de Raad voor de Kinderbescherming, waaronder in het bijzonder taken zoals bedoeld in boek 1 afdeling 3 van het Burgerlijk Wetboek, waaronder de art. 1:240 BW en de art. 1:255 juncto 1:257 BW, de art. 77o en 77hh van het Wetboek van Strafrecht, de art. 126 nd en 491 van het Wetboek van Strafvordering alsmede art. 28 van het Besluit Tenuitvoerlegging Jeugdstrafrecht 1994, de Algemene Wet Bestuursrecht, de art. 2.4, 3.1 en 3.2 van de Jeugdwet alsmede art. 7.3.11 lid 4 van de Jeugdwet en art. 4 onder c, lid 1 van de Wet Opneming Buitenlandse Kinderen ter Adoptie (verder Wobka). Met inachtneming van het Kwaliteitskader 2016 van de Raad voor de Kinderbescherming.
- f. Veilig Thuis: de goede uitvoering van de taken van het AMHK, waaronder in het bijzonder taken zoals bedoeld in de Wmo artikel 4.1.1, met inachtneming van het handelingsprotocol Veilig Thuis.
- g. een Reclasseringsinstelling: de goede uitvoering van taken van de reclasseringsinstelling, waaronder in het bijzonder taken zoals bedoeld in de Reclasseringsregeling 1995 artikel 8 lid 1.
- h. een Gecertificeerde Instelling zoals bedoeld in de Jeugdwet artikel 1.1: de goede uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering zoals bedoeld in de Jeugdwet artikel 1.1.
- i. een instelling voor Geestelijke Gezondheidszorg: de uitvoering van de taken bij behandeling, verpleging, verzorging en bejegening van personen met een psychische

stoornis, inclusief verslaving met of zonder verblijf in het kader van de WGBO of de Wet bopz, per 1-1-2020 Wvvgz of Wzd.

- j. een instelling voor gehandicaptenzorg: de uitvoering van de taken bij behandeling, verpleging, verzorging en bejegening van personen met een handicap, inclusief verslaving met of zonder verblijf
 - k. een GGD: de uitvoering van de taken in het kader van de OGGZ op grond van artikel 1.2.1. sub a Wmo 2015.
 - l. de Dienst Justitiële Inrichtingen: de Dienst Justitiële Inrichtingen: voor de uitvoering van taken van de Minister van Justitie en Veiligheid, de selectiefunctionaris en de directeur van een justitiële inrichting op grond van de Beginselenwet justitiële jeugdinrichtingen, de Beginselenwet verpleging ter beschikking gestelden, de Penitentiaire beginselenwet en het Interimbesluit forensische zorg (per 1-1-2019 de wet Forensische zorg). De wettelijke grondslag voor de verwerking en verstrekking van persoonsgegevens is na inwerkingtreding van de wijziging van de Wet justitiële en strafvorderlijke gegevens (Wjsg) ter implementatie van de Europese richtlijn gegevensbescherming opsporing en vervolging gelegen in de Wjsg.
 - m. Slachtofferhulp Nederland: voor de uitvoering van de taken zoals genoemd in artikel 6 en 7 Wet Justitie subsidies jo. de Aanwijzing rechtspersoon slachtofferhulp [1], en artikel 51aa Wetboek van Strafvordering jo Besluit slachtoffers van strafbare feiten artikel 1^e en 3. De wettelijke grondslag voor de gegevensverwerking is mede gelegen in artikel 9 en/ of artikel 10 AVG jo art. 33 lid1a en art. 30 lid 3a en lid 4 UAVG]. Met dien verstande dat gegevens aan de deelnemende partijen van het convenant alleen verstrekt kunnen worden met de uitdrukkelijke toestemming van de betrokkene.
 - n. Een aanbieder zoals bedoeld in de Wmo artikel 1.1.1, zorgaanbieder zoals bedoeld in de Wlz artikel 1.1.1, dan wel een jeugdhulpaanbieder zoals bedoeld in de Jeugdwet artikel 1.1: voor de verlening van voorzieningen en/of de uitvoering van zorg- dan wel hulpverleningstaken en voor zover dit noodzakelijk is in het kader van de behandeling of hulpverlening.
- 6.5 Op de persoonsgegevens die worden verwerkt, ingebracht, en/of verstrekt zoals bedoeld in artikel 5 zijn uitdrukkelijk de uitgangspunten van artikel 3.5 van toepassing en het bepaalde in artikel 7.

Toelichting:

Zie voor een nadere toelichting op de juridische basis voor de Verwerking van Persoonsgegevens door de Gemeente §5.4 van het Handvat.

Zie voor een nadere toelichting op de juridische basis voor de Verwerking van Persoonsgegevens door het Openbaar Ministerie §5.3 van het Handvat.

De Artikel 20 Wpg Beslissing wordt ondertekend door de gemandateerde politiechef van de betreffende eenheid en het bevoegd gezag, te weten de Burgemeesters en de Officier van Justitie.

Zie voor een nadere toelichting op de juridische basis voor de Verwerking van Persoonsgegevens door de Politie §5.2 van het Handvat.

Zie voor een nadere toelichting op de juridische basis voor de Verwerking van Persoonsgegevens door de Reclassering §5.8 van het Handvat.

Zie voor een nadere toelichting op de juridische basis voor de Verwerking van Persoonsgegevens door de GGZ §5.5 van het Handvat.

Zie voor een nadere toelichting op de juridische basis voor de Verwerking van Persoonsgegevens door de GGD §5.5 van het Handvat.

Partijen dienen ieder voor zich vast te stellen op grond van welke wettelijke grondslag zij Persoonsgegevens in het kader van de samenwerking van het zorg- en veiligheidshuis Verwerken. Wanneer deze grondslag is gekoppeld aan materiewetgeving, bijvoorbeeld omdat de betreffende Verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang, dient de betreffende materie-wetgeving waarin dit algemeen belang is beschreven, te worden benoemd. In artikel 6.4 a t/m m van dit protocol zijn voor een groot deel van de vaste partners in het zorg- en veiligheidshuis de taken die aan de orde kunnen zijn benoemd. Hoofdstuk 5 van het Handvat voorziet in nadere invulling hiervan.

Publieke instellingen dienen de Verwerking van Persoonsgegevens in het zorg - veiligheidshuis voor de in Artikel 3 genoemde doeleinden een grondslag in de wet te kunnen aanwijzen (artikel 6, lid 1 onder e, AVG). Private partijen dienen te onderzoeken of zij (uitdrukkelijke) toestemming kunnen krijgen voor de Verwerking (artikel 6, lid 1 onder a, AVG), danwel dat de Verwerking noodzakelijk is voor hun gerechtvaardigd belang en de belangen van de Betrokkene hier niet tegen opwegen (artikel 6, lid 1 onder f, AVG).

Artikel 7. Doorverwerking geheimhoudingsbepalingen en toepassing toestemmingsvereiste

- 7.1 De geheimhoudingsbepaling van artikel 7 Wpg blijven rusten op de verstrekte gegevens. Dit geldt voor de ontvanger maar ook voor de tweede en derde ontvanger. Wanneer er over betrokkene in een eerder stadium op grond van artikel 16 lid 1b onder 2 Wpg politiegegevens zijn verstrekt aan de burgemeester óf op grond van artikel 15 Wpg politiegegevens ter beschikking zijn gesteld aan een Buitengewone Opsporingsambtenaar van een gemeente óf op grond van het Besluit politiegegevens (Bpg), voor een ander doel politiegegevens zijn verstrekt aan een van de convenantpartijen, dan worden deze gegevens door de desbetreffende ontvanger in principe niet als persoonsgegevens verstrekt aan de procesregisseur van het Zorg- en Veiligheidshuis. Bij voorkeur worden door de politie op grond van artikel 20 Wpg opnieuw actuele politiegegevens verstrekt aan de procesregisseur van het zorg- en veiligheidshuis voor de doelen zoals genoemd in artikel 3.2, 3.3 en bijlage 2. De politie kan in uitzonderingsgevallen ook toestemming geven aan de ontvanger voor doorverstrekking aan de procesregisseur van het zorg- en veiligheidshuis maar legt deze toestemming vast in haar systemen.
- 7.2 Indien voor het inbrengen en/of verstrekken van persoonsgegevens zoals bedoeld in de artikelen 5.2 en 5.3 toestemming noodzakelijk is voor doorbreken geheimhoudingsbepalingen zoals bijvoorbeeld verwoord in de WGBO (artikel 7:457 BW) en artikel 88 Wet BIG, de beroepscode van de Jeugdzorgwerker artikel J, beroepscode NIP artikel 71 t/m 87

(psycholoog), of beroepscode NVO artikel 8 (pedagoog), de Reclasseringsregeling 1995 artikel 37, dan:

- a. wordt deze gevraagd op het moment dat duidelijk is dat het inbrengen of verstrekken noodzakelijk is t.b.v. van de in de betreffende fase aan de orde zijnde doelen, of de uitvoering van de in 5.3.1 a t/m c genoemde activiteiten;
- b. worden deze persoonsgegevens uitsluitend verstrekt voor zover hiervoor de uitdrukkelijke toestemming is verkregen van de betrokkene of diens wettelijke vertegenwoordiger;
- c. legt de partij die de toestemming heeft verkregen deze schriftelijk vast en informeert Betrokkene dat hij zijn toestemming altijd weer kan intrekken;
- d. draagt de partij die toestemming heeft verkregen bij intrekking van die toestemming er zorg voor dat er geen verdere verstrekkingen meer plaats vinden;
- e. maakt de betrokken zorg- of hulpverlener een eigen afweging conform de voor hem geldende professionele standaarden, indien toestemming niet verkregen wordt en hij ervan overtuigd is dat zich hier een conflict van plichten voordoet, of goed hulpverlenerschap het verstrekken van persoonsgegevens verlangd.

Artikel 8. Documentatie individuele verstrekkingen

- 8.1. Indien Partijen daartoe verplicht zijn door voor hen geldende materiewetgeving, dan leggen zij de afzonderlijke verstrekkingen van Persoonsgegevens, inclusief onderbouwing van de noodzakelijkheid daarvan met het oog op de in artikel 5 en 6 vastgelegde grondslagen, vast. Dit geldt ten minste voor politie en OM. De politie documenteert iedere verstrekking conform de documentatieplicht van art 32 Wpg, het Openbaar Ministerie conform artikel 39j Wjsg.

Toelichting:

Sommige partijen zijn verplicht naast het verwerkingsregister ook afzonderlijke verstrekkingen vast te leggen. Dit geldt ten minste voor de Politie en het OM. Voor het Openbaar Ministerie geldt dat ten minste vastgelegd moet worden welke informatie verstrekt is, en wie de ontvangers (welke partijen) zijn van deze informatie. Deze informatie dient in ieder geval voor de duur van 4 jaar vastgelegd te zijn. Binnen het parket dienen goede afspraken gemaakt te worden met de privacy functionaris van het parket, zodat deze de informatie goed en makkelijk kan raadplegen. Dit is noodzakelijk om op een accurate wijze de rechten van betrokkenen te kunnen waarborgen.

De Documentatieplicht uit artikel 8 is iets anders dan het verstrekkingenregister uit de AVG zoals vermeld in artikel 24 van dit protocol.

Artikel 9. Dataminimalisatie

- 9.1 Partijen Verwerken niet meer Persoonsgegevens dan strikt noodzakelijk in relatie tot de in artikel 3.1 en 3.2 van dit Protocol geformuleerde doeleinden.
- 9.2 Ten behoeve van de Aanmelding van een Casus verstrekt de Partij die de Casus bij de Procesregisseur aanmeldt enkel die Persoonsgegevens die noodzakelijk zijn voor de Procesregisseur om de Casus te toetsen aan de criteria van complexe casuïstiek zoals geformuleerd in Bijlage 2 van het Convenant. De Procesregisseur registreert enkel die Persoonsgegevens in het informatiesysteem van het zorg- en veiligheidshuis die noodzakelijk zijn voor Triage.

- 9.3 In de Regionale Casustafel Verwerken Partijen alleen die Persoonsgegevens die noodzakelijk zijn voor het opstellen en uitvoeren van een integraal plan van aanpak en het afschalen van een Casus.
- 9.4 In het MDO Verwerken Partijen alleen die Persoonsgegevens die noodzakelijk zijn voor het opstellen en uitvoeren van een integraal plan van aanpak.
- 9.5 In het kader van Afschaling Verwerken Partijen alleen die Persoonsgegevens die noodzakelijk zijn om te bepalen of het plan van aanpak in het Regionale Casustafel tot de gewenste resultaten heeft geleid. Indien wordt besloten dat behandeling van de Casus in het zorg- en veiligheidshuis niet of niet langer noodzakelijk is, worden de betreffende Persoonsgegevens niet langer in het zorg- en veiligheidshuis Verwerkt. De Procesregisseur ziet erop toe dat Persoonsgegevens conform artikel 11 worden geanonimiseerd of onomkeerbaar vernietigd.
- 9.6 Wanneer de Partij die Persoonsgegevens in het zorg- en veiligheidshuis heeft verstrekt, kennis verkrijgt over de onjuistheid van die Persoonsgegevens, informeert die Partij de Casusregisseur en Procesregisseur hierover. De Procesregisseur coördineert de eventuele correctie van Persoonsgegevens in het zorg- en veiligheidshuis.
- 9.7 Enkel de Procesregisseur, de Informatiecoördinator, de Ondersteuner Casustafels en de voor het Regionale Casustafel uitgenodigde partners hebben toegang tot de Persoonsgegevens die worden Verwerkt op locatie of in het informatiesysteem van het zorg- en veiligheidshuis en enkel voor zover noodzakelijk voor hun rol in een specifieke Casus.

Artikel 10. Kwaliteit

- 10.1 Partijen dragen er zorg voor dat de Persoonsgegevens die zij in het kader van de onder artikel 3.2 geformuleerde doeleinden verstrekken toereikend, ter zake dienend, niet bovenmatig, juist en nauwkeurig zijn. De Partij die Persoonsgegevens in het zorg- en veiligheidshuis verstrekt blijft verantwoordelijk voor de juistheid, actualiteit en nauwkeurigheid van die Persoonsgegevens.

Artikel 11. Bewaren en Vernietigen

- 11.1 Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor het doel of de doeleinden waarvoor ze worden Verwerkt zoals geformuleerd onder artikel 3 en met inachtneming van artikel 9.
- 11.2 Na het besluit tot Afschalen worden Persoonsgegevens gefaseerd verwijderd;
 - a. Gegevens die noodzakelijk zijn voor de uitvoering van de werkzaamheden in het vervolg van de Casus overgedragen aan de betreffende Partner – eventueel met toestemming van de Partij die de gegevens heeft ingebracht;
 - b. Afschalingsfase 1 treedt in werking: het dossier blijft actief in GCOS voor het geval terugval optreedt (maximaal 6 maanden), met alleen toegang voor de bij de casus betrokken partners;
 - c. Afschalingsfase 2 treedt in werking 6 maanden na besluit tot Afschaling, waarbij alleen de aanmelder en procesregisseur achterblijven in GCOS, met alleen toegang voor de Informatiecoördinator;

- d. Afschalingsfase 3 treedt in werking na één jaar na besluit tot Afschaling. Het volledige dossier, inclusief administratieve gegevens, wordt door de Informatiecoördinator vernietigd.¹
- 11.3 Na één jaar kunnen gegevens, niet zijnde Persoonsgegevens, enkel worden bewaard voor managementdoeleinden.
- 11.4 De manager van het zorg- en veiligheidshuis is eindverantwoordelijk voor het bewaken van de vastgestelde termijnen en afspraken met betrekking tot gegevensvernietiging en – opslag.

Artikel 12. Beveiliging

- 12.1 Partijen dragen zorg voor passende technische en organisatorische beveiligingsmaatregelen om Persoonsgegevens te beschermen tegen verlies of enige vorm van onrechtmatige Verwerking zoals omschreven in Bijlage 3. Die maatregelen betreffen onder meer, maar niet uitsluitend, maatregelen met betrekking tot de toegang tot Persoonsgegevens, alsook het gebruik van beveiligde verbindingen voor de verstrekking van Persoonsgegevens.
- 12.2 Wanneer Persoonsgegevens aan andere Partijen worden verstrekt, gebeurt dit uitsluitend op een adequaat beveiligde manier, conform de geldende beveiligingsnormen voor de betreffende gegevens.
- 12.3 De gemeente Zwolle draagt zorg voor de adequate beveiliging van Persoonsgegevens die worden Verwerkt op locatie en in de informatiesystemen van het zorg- en veiligheidshuis en rapporteren hierover indien nodig aan de Stuurgroep.
- 12.4 De Manager van het zorg- en veiligheidshuis is verantwoordelijk voor het toezien op de naleving van de beschermingsmaatregelen zoals geformuleerd in Bijlage 3 voor de Verwerking van Persoonsgegevens op locatie en in de informatiesystemen van het zorg- en veiligheidshuis en rapporteert hierover aan de Gemeente Zwolle en is bevoegd aanwijzingen te geven aan Partijen omtrent de juiste omgang met Persoonsgegevens in dat verband.

Artikel 13. Geheimhouding

- 13.1. Een ieder die op grond van dit Protocol kennis neemt van Persoonsgegevens is verplicht tot geheimhouding daarvan, tenzij de wet tot bekendmaking verplicht. De Manager, Procesregisseur en eventueel ander ondersteunend personeel van het zorg- en veiligheidshuis worden door middel van een geheimhoudingsverklaring tot geheimhouding gebonden.
- 13.2. Partijen dragen er zorg voor dat iedere medewerker die in de uitvoering van het Convenant of dit Protocol in aanraking komt met Persoonsgegevens geheimhouding van die gegevens waarborgt.
- 13.3. Alle medewerkers van het zorg- en veiligheidshuis, inclusief medewerkers op basis van een dienstverleningsovereenkomst, deelnemers aan Regionale Casustafelgen en MDO's en overige afgevaardigden van Partijen die toegang hebben tot Persoonsgegevens die onder dit Protocol worden Verwerkt, beschikken over een Verklaring Omtrent Gedrag (verder VOG), dan wel hebben een veiligheidsonderzoek op grond van de voor de eigen organisatie geldende wet- en regelgeving doorlopen.
- 13.4. Wettelijke geheimhoudingsplichten zijn onverminderd van toepassing op eenieder die Strafrechtelijke persoonsgegevens of andere Bijzondere Persoonsgegevens in het kader van de samenwerking in het zorg- en veiligheidshuis ontvangt.

¹ Het systeem van (gefaseerde) afschaling wordt momenteel door GCOS verder uitgebouwd.

- 13.5. De Partijen in het samenwerkingsverband mogen de Persoonsgegevens afkomstig van de politie en Openbaar Ministerie slechts verwerken voor het specifieke doel waarvoor deze zijn verstrekt ten behoeve van de Casus. Deze Persoonsgegevens mogen alleen verder worden Verwerkt door de ontvangende Partijen indien het doel van de verdere verwerking verenigbaar is met dit doel waarvoor de Persoonsgegevens zijn verstrekt. Onverenigbaar gebruik van de gegevens, ook intern binnen de organisaties van de ontvangende Partijen, is niet toegestaan.
- 13.6. De Partijen in het samenwerkingsverband mogen de Persoonsgegevens afkomstig van andere Partijen die aan een geheimhoudingsplicht als onder meer bedoeld in de Wet Geneeskundige behandelovereenkomst (artikel 7:457 BW), Reclasseringsregeling 1995, Jeugdwet of Wet Maatschappelijke Ondersteuning zijn gebonden, slechts Verwerken voor het specifieke doel van de casus waarvoor deze zijn verstrekt. De Persoonsgegevens mogen alleen verder worden Verwerkt door de ontvangende Partijen met toestemming van de verstreckende Partij en indien het doel van de verdere verwerking verenigbaar is met dit doel waarvoor de Persoonsgegevens zijn verstrekt. Onverenigbaar gebruik van de Persoonsgegevens, ook intern binnen de organisaties van de ontvangende Partijen, is niet toegestaan.
- 13.7. Wanneer de grond voor het verstrekken van de Persoonsgegevens als bedoeld in dit lid gebaseerd is op toestemming van Betrokkene als bedoeld artikel 6 lid 1 onder a AVG en/of artikel 9 lid 2 onder a AVG en Betrokkene trekt deze toestemming in, laat de verstreckende Partij dit aan de ontvangende Partij weten, waarbij ook de toestemming voor Verwerking en verder Verwerking voor de ontvangende Partij vervalt.

Toelichting:
Het opzettelijk schenden van de geheimhoudingsplicht is strafbaar gesteld in artikel 272 Wetboek van strafrecht (verder WvSr)

Artikel 14. Datalekken

- 14.1. Partijen houden procedures in stand die er op gericht zijn om inbreuken in de beveiligingsmaatregelen zoals geformuleerd in Bijlage 3 met betrekking tot de bescherming van Persoonsgegevens redelijkerwijs op te sporen en daarop actie te ondernemen, daaronder begrepen maatregelen tot herstel.
- 14.2. De gemeente Zwolle is verantwoordelijk voor het in stand houden van procedures zoals bedoeld in artikel 14.1 voor de Verwerking van Persoonsgegevens op locatie of in de informatiesystemen van het zorg- en veiligheidshuis. De Manager ziet toe op de naleving van deze procedures in het zorg- en veiligheidshuis.
- 14.3. Partijen stellen de Manager onverwijld maar uiterlijk binnen 24 uur na kennisneming schriftelijk op de hoogte van een inbreuk op persoonsgegevens in de zin van artikel 4, onder 12, AVG dan wel artikel 26g Wet justitiële en strafvorderlijke gegevens die een risico inhoudt voor de rechten en vrijheden van betrokkenen zoals bedoeld in artikel 34 AVG. Deze kennisgeving omvat in ieder geval:
- a. De aard en omvang van de inbreuk;
 - b. De contactgegevens van de persoon bij wie meer informatie over de inbreuk kan worden verkregen;

- c. De maatregelen die kunnen worden genomen om de gevolgen van de inbreuk te voorkomen of beperken;
 - d. De mogelijke gevolgen en risico's van de inbreuk op de bescherming van Persoonsgegevens voor de Betrokkene;
 - e. De maatregelen die Partij zelf reeds heeft genomen of zal nemen om de bescherming van Persoonsgegevens te herstellen.
- 14.4. De Manager informeert Partijen middels het Kerngroepoverleg schriftelijk over een inbreuk zoals bedoeld in artikel 14.3.
- 14.5. Verantwoordelijke Partijen melden, indien wettelijk verplicht, een inbreuk zoals bedoeld in Artikel 14.3 bij de Autoriteit Persoonsgegevens. De Manager stuurt een afschrift van de melding aan de Autoriteit Persoonsgegevens aan de Stuurgroep.
- 14.6. Wanneer een inbreuk als bedoeld in Artikel 14.3 waarschijnlijk een hoog risico voor de rechten en vrijheden van Betrokkene(n) zal inhouden als bedoeld in artikel 34 AVG, wordt de betrokkene door de verantwoordelijke partijen over de inbreuk schriftelijk geïnformeerd. De beslissing tot melding aan de Betrokkene wordt met de betrokken Partners genomen. De inhoud van die melding wordt in het Kerngroepoverleg afgestemd, dan wel door het Kerngroepoverleg aan één Partij gemandateerd.
- 14.7. Partijen verlenen elkaar de medewerking die redelijkerwijs van elkaar mag worden verwacht om aan de op Partijen rustende kennisgevingsverplichtingen te voldoen, mede met het oog op een eventueel onderzoek door de Autoriteit Persoonsgegevens naar aanleiding van de schriftelijke inbreukmelding.
- 14.8. Kennisgeving van de inbreuk aan de Autoriteit Persoonsgegevens door de Partijen gebeurt zonder onredelijke vertraging maar in ieder geval binnen 72 uur na ontdekking en geschiedt volgens de daartoe door de Autoriteit Persoonsgegevens ter beschikking gestelde procedure. De kennisgeving aan de Autoriteit Persoonsgegevens omvat minimaal:
- a. de aard van de inbreuk;
 - b. een omschrijving van de categorieën Betrokkenen van wie Persoonsgegevens zijn betrokken bij de inbreuk;
 - c. de categorieën Persoonsgegevens;
 - d. of de Persoonsgegevens zijn versleuteld, geanonimiseerd, of anderszins onbegrijpelijk zijn gemaakt;
 - e. de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
 - f. de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van de Persoonsgegevens en de maatregelen die Partij heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.
- 14.9. Kennisgeving van de inbreuk aan Betrokkene zoals bedoeld in artikel 14.6 is niet vereist indien:
- a. passende technische en organisatorische maatregelen zijn genomen die de bescherming van Persoonsgegevens ook na de inbreuk garanderen;
 - b. achteraf genomen maatregelen de waarschijnlijkheid op een hoog privacy risico hebben weggenomen, of;
 - c. de mededeling aan Betrokkene een onevenredig grote inspanning zou vragen.
- 14.10. Voorts kan de mededeling aan betrokkene worden uitgesteld, beperkt of achterwege gelaten worden, indien de inbreuk enkel ziet op gegevens afkomstig van het Openbaar Ministerie, en indien dit noodzakelijk en evenredig is:
- a. ter vermijding van belemmering van gerechtelijke onderzoeken of procedures;

- b. ter vermindering van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
 - c. ter bescherming van de openbare veiligheid;
 - d. ter bescherming van de rechten en vrijheden van derden;
 - e. ter bescherming van de nationale veiligheid.
- 14.11. Partijen houden afzonderlijk een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van de Persoonsgegevens. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen, alsmede de tekst van de kennisgeving aan de Betrokkene. De Manager van het zorg- en veiligheidshuis houdt een overzicht bij van gelijksoortige inbreuken die plaatsvinden op locatie of in de informatiesystemen van het zorg- en veiligheidshuis.

Artikel 15. Data Protection Impact Analyse (verder DPIA)

- 15.1. Er wordt aangaande Verwerkingen onder dit Protocol, of bij wijzigingen van de Verwerkingen, gedurende het eerste jaar van dit Protocol, door Partijen middels het Kerngroepoverleg een Gegevensbeschermingseffectbeoordeling uitgevoerd conform artikel 35 AVG. De Manager coördineert dit proces. Waar mogelijk wordt aangesloten bij de landelijke DPIA.
- 15.2. Bij de uitvoering van de Gegevensbeschermingseffectbeoordeling wordt aangesloten bij een landelijk model danwel het model Gegevensbeschermingseffectbeoordeling van de gemeente Zwolle gevolgd.
- 15.3. Bij een voornemen omtrent de inzet van nieuwe technologieën kan dit voornemen ter advies worden voorgelegd aan het Landelijk Overleg Managers Veiligheidshuizen. Het Landelijk Overleg Managers Veiligheidshuizen kan advies uitbrengen over de beoogde inzet van nieuwe technologieën.
- 15.4. De uitkomsten van de Gegevensbeschermingseffectbeoordeling worden ter besluitvorming voorgelegd aan de Stuurgroep. De Stuurgroep kan hiervoor advies vragen aan het Kerngroepoverleg over de voorgenomen nieuwe Verwerking zoals bedoeld in artikel 15.1. De Stuurgroep legt waar nodig op grond van artikel 36 AVG namens alle gezamenlijke Verwerkingsverantwoordelijken de beoogde Verwerking voor aan de Autoriteit Persoonsgegevens.

Artikel 16. Informatieverstrekking aan Betrokkenen

- 16.1. Vóór het verstrekken van Persoonsgegevens in het kader van de samenwerking wordt Betrokkene door de gemeente waar Betrokkene ingezetene is, geïnformeerd over het voornemen diens Persoonsgegevens verder te Verwerken in het kader van samenwerking in het zorg- en veiligheidshuis onder dit Protocol.
- 16.2. Deze informerende Partij maakt het tijdstip waarop en de wijze van informeren kenbaar aan de overige bij een Casus betrokken Partijen.
- 16.3. De Manager draagt zorg voor het publiceren van een privacy statement op de website van het zorg- en veiligheidshuis.
- 16.4. Alle deelnemende partijen zorgen via hun eigen website voor vermelding van deelname aan het zorg- en veiligheidshuis en voor een verwijzing naar de website van het betreffende zorg- en veiligheidshuis/ de Veiligheidshuizen waaraan zij deelnemen, alsook voor verwijzing naar het zorg- en veiligheidshuis convenant en het privacyprotocol.

- 16.5. De onder artikel 16.1 bedoelde informatieverstrekking, alsook het onder artikel 16.3 genoemde privacy statement, bevatten ten minste de volgende informatie:
- a. De doeleinden voor de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis zoals beschreven in artikel 3.2.
 - b. De Partijen die deelnemen aan de samenwerking in het zorg- en veiligheidshuis;
 - c. De termijn waarvoor de Persoonsgegevens worden opgeslagen en bewaard zoals omschreven onder artikel 11, dan wel de criteria voor het bepalen van die termijn;
 - d. Dat Betrokkene verscheidene rechten heeft met betrekking tot de Verwerking van diens Persoonsgegevens zoals geformuleerd onder artikel 17 tot en met 21;
 - e. Indien de Verwerking van Persoonsgegevens is gebaseerd op toestemming, dat Betrokkene het recht heeft deze te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de Verwerking van de Persoonsgegevens die heeft plaatsgevonden vóór intrekking van de toestemming;
 - f. Dat Betrokkene het recht heeft een klacht in te dienen over de Verwerking van zijn of haar Persoonsgegevens onder dit Protocol bij het zorg- en veiligheidshuis en bij de Autoriteit Persoonsgegevens;
 - g. Nadere uitleg indien de Persoonsgegevens moeten worden verstrekt of verder Verwerkt op grond van een wettelijke of contractuele verplichting;
 - h. Nadere uitleg indien Betrokkene verplicht is de Persoonsgegevens te verstrekken;
 - i. Indien sprake is van geautomatiseerde besluitvorming, met inbegrip van profilering, uitleg over de achterliggende logica, het belang van de verwerkingsactiviteiten en de verwachte gevolgen voor de Betrokkene.
 - j. De contactgegevens van de locatie van het Veiligheidshuis bij wie de Betrokkene terecht kan voor meer informatie over de Verwerking van zijn Persoonsgegevens, dan wel waar hij zijn rechten geldend kan maken.
- 16.6. De informatieverplichting zoals bedoeld in artikel 16.1 is niet van toepassing indien het achterwege laten van informeren van Betrokkene noodzakelijk is in het belang van:
- a. De veiligheid van de staat;
 - b. De voorkoming, opsporing en vervolging van strafbare feiten;
 - c. Gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
 - d. Het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder b en c, of;
 - e. De bescherming van de betrokkene of van de rechten en vrijheden van anderen.
- 16.7. Partijen leggen de motivatie voor het niet voldoen aan de informatieplicht op grond van Artikel 16.6 schriftelijk vast en leggen vast wanneer zij verwachten dat betrokkene wel geïnformeerd kan worden, alsook van welke omstandigheden dit afhankelijk is, hoe periodiek wordt getoetst of deze omstandigheden nog aanwezig zijn en hoe dan wel wanneer Betrokkene geïnformeerd zal worden.

Artikel 17. Rechten van de Betrokkene

- 17.1. Betrokkene kan bij Partijen een verzoek indienen om:
- a. Inzage te krijgen in de Persoonsgegevens die door Partijen over hem of haar worden Verwerkt;

- b. Correctie of verwijdering van de hem betreffende Persoonsgegevens dan wel beperking van de Verwerking;
 - c. Bezwaar te maken tegen de Verwerking;
 - d. Zijn of haar Persoonsgegevens over te dragen.
- 17.2. Verzoeken lopen vervolgens via de werkprocessen van de betreffende partij bij wie het verzoek is ingediend;
- 17.3. Verzoeken door Betrokkene ten aanzien van Persoonsgegevens die worden Verwerkt op locatie of in het informatiesysteem van het zorg- en veiligheidshuis worden gecoördineerd door de Procesregisseur. De Procesregisseur wordt hierbij ondersteund door de administratief medewerker. De Manager legt het verzoek voor aan het Kerngroepoverleg en stemt daarin met Partijen de beantwoording van het verzoek af.
- 17.4. Indien het verzoek als bedoeld in Artikel 17.1 direct is gericht aan een der Partijen wordt de Manager hierover zo spoedig mogelijk door die Partij in kennis gesteld, opdat deze de beantwoording van het verzoek conform artikel 17.2 kan coördineren. Beantwoording van het verzoek door de Partij wordt in het Kerngroepoverleg afgestemd.
- 17.5. Het bepaalde in artikel 17.2 en artikel 17.3 ontslaat Partijen niet van diens eigen verantwoordelijkheid als Verwerkingsverantwoordelijke ten aanzien van een verzoek van Betrokkene.
- 17.6. Artikel 17.1 t/m 17.4, alsmede de artikelen 18, 19 en 20 zijn niet van toepassing op gegevens die verstrekt zijn door het College van procureurs-generaal. Op deze gegevens is de WjSg van toepassing. Verstrekkingen van gegevens door het College van procureurs-generaal worden ingevolge artikel 8 van dit Protocol en artikel 39j Wjsg schriftelijk vastgelegd en bewaard voor de duur van 4 jaar. Inzage- en rectificatieverzoeken worden beoordeeld door de privacyfunctionaris van het verstreckende parket van het Openbaar Ministerie. Verzetschriften tegen verwerking van gegevens worden beoordeeld door de afdeling Bestuurlijke en juridische zaken van het Parket-Generaal.
- 17.7. Op gegevens die eerder verstrekt zijn door de politie is de geheimhoudingsplicht van de Wpg van toepassing en zijn derhalve artikel 18, 19 en 20 van dit Protocol niet van toepassing. Inzage- en correctieverzoeken worden beoordeeld door het Wpg loket van de verstreckende eenheid van de politie. Verzet- en bezwaarschriften tegen verwerking van gegevens worden beoordeeld door de privacyfunctionaris en/ of jurist van de verstreckende eenheid van de politie, conform artikel 29 Wpg.

Artikel 18. Recht op inzage

- 18.1. In het geval dat het verzoek ziet op inzage in de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis door Partijen zoals bedoeld in artikel 17.1 onder a, dient de beantwoording van dat verzoek in een volledig overzicht in begrijpelijke vorm met ten minste de volgende informatie te bevatten:
 - a. de verwerkingsdoeleinden;
 - b. de betrokken categorieën van Persoonsgegevens;
 - c. de ontvangers of categorieën van ontvangers aan wie de Persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
 - d. indien mogelijk, de periode gedurende welke de Persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;

- e. dat de Betrokkene het recht heeft de Verwerkingsverantwoordelijke(n) te verzoeken dat Persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
 - f. dat de Betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
 - g. wanneer de Persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
 - h. het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4 AVG bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de Betrokkene.
- 18.2. Het schriftelijke verzoek wordt binnen vier weken door de Manager beantwoord. Een verzoek tot inzage wordt enkel geweigerd, indien en voor zover dit noodzakelijk is met het oog op in de wet gespecificeerde weigeringsgronden.
- 18.3. Een eventuele (gedeeltelijke) afwijzing is schriftelijk en gemotiveerd.
- 18.4. Alvorens aan een verzoek als bedoeld in artikel 17.1 wordt voldaan, verifiëren Partijen de identiteit van de Betrokkene die het verzoek indient. Betrokkene dient hiervoor persoonlijk langs te komen bij het zorg- en veiligheidshuis met een ID-bewijs om de identiteit van betrokkene te kunnen vaststellen.
- 18.5. Bij voldoen aan een verzoek als bedoeld in artikel 17.1, verstrekt de Manager namens de Verwerkingsverantwoordelijke aan de Betrokkene een kopie van de Persoonsgegevens die worden verwerkt.

Artikel 19. Recht op rectificatie en verwijdering

- 19.1. Indien de Betrokkene op grond van zijn verzoek om inzage een verzoek tot rectificatie of verwijdering van bepaalde hem of haar betreffende onjuiste Persoonsgegevens zoals bedoeld in artikel 17.1 onder b doet bij het zorg- en veiligheidshuis, legt de Manager dit verzoek voor aan het Kerngroepoverleg met het oog op de beoordeling van het verzoek.
- 19.2. Onjuiste Persoonsgegevens betreffende de Betrokkene worden op diens verzoek onverwijld gecorrigeerd.
- 19.3. Persoonsgegevens betreffende de Betrokkene worden zonder onredelijke vertraging op diens verzoek verwijderd wanneer deze:
- a. voor het doel van de Verwerking onvolledig of niet ter zake dienend zijn; of
 - b. anderszins in strijd met een wettelijk voorschrift worden Verwerkt.
- 19.4. De Manager informeert de Betrokkene over de beslissing omtrent zijn verzoek tot correctie of verwijdering van hem of haar betreffende Persoonsgegevens schriftelijk en gemotiveerd zo spoedig mogelijk, maar uiterlijk binnen 4 weken na ontvangst van het verzoek.

Artikel 20. Recht op bezwaar

- 20.1. Betrokkene kan bezwaar maken tegen de verwerking van hem betreffende persoonsgegevens, zoals verwoord in artikel 20 AVG.
- 20.2. Indien een verzoek tot verzet door Betrokkene bij één der Partijen wordt ingediend, informeert die Partij onverwijld de Manager over het ingediende verzoek.

- 20.3. De Manager legt het door Betrokkene ingeroepen recht van bezwaar voor aan het Kerngroepoverleg om te beoordelen of het verzoek gerechtvaardigd is en coördineert de afhandeling daarvan.
- 20.4. De Manager informeert de Betrokkene over de beslissing zoals bedoeld in artikel 17.3 binnen 4 weken en draagt er zorg voor dat de beslissing binnen deze 4 weken wordt uitgevoerd. Een beslissing om niet, of niet geheel, te voldoen wordt altijd gemotiveerd en kan met het oog op artikel 21 AVG enkel worden gebaseerd op dwingende gerechtvaardigde gronden.

Artikel 21. Recht op overdraagbaarheid van Persoonsgegevens

- 21.1. Het recht op overdraagbaarheid van Persoonsgegevens is niet van toepassing op Partijen in het zorg- en veiligheidshuis.

Artikel 22. Verwerkers

- 22.1. Partijen besteden de Verwerking van Persoonsgegevens onder dit Protocol niet uit zonder dat de Stuurgroep tevoren schriftelijk toestemming heeft gegeven over de beoogde verandering inzake de inzet van Verwerkers die ten behoeve van het zorg- en veiligheidshuis Persoonsgegevens Verwerken.
- 22.2. Een overeenkomst van opdracht tussen Partijen en een door Stuurgroep goedgekeurde Verwerker inzake Verwerking van Persoonsgegevens dient ten minste hetzelfde beschermingsniveau te bieden aan de belangen van Betrokkene als het onderhavige Protocol. Meer in het bijzonder moet de Verwerker voor de Verwerkingen van Persoonsgegevens in het kader van dit Protocol een vergelijkbaar niveau van beveiliging garanderen als in Bijlage 3 van dit Protocol.
- 22.3. Partijen leggen de afspraken tussen hen en Verwerker(s) omtrent de omgang met Persoonsgegevens die Verwerker ten behoeve van Partijen Verwerkt, in een schriftelijke overeenkomst vast. De voorzitter van de Stuurgroep is bevoegd deze overeenkomst namens Partijen aan te gaan.
- 22.4. De Manager houdt een lijst bij van de overeenkomsten die met schriftelijke toestemming van de Stuurgroep zijn overeengekomen, welke minimaal eenmaal per jaar wordt bijgewerkt. Deze lijst zal beschikbaar worden gehouden ten behoeve van Partijen en de toezichthouder.

Artikel 23. Verstrekking aan derden

- 23.1. Persoonsgegevens die in het kader van dit Protocol worden Verwerkt, worden niet verstrekt aan anderen dan deelnemers aan het Regionale Casustafel of MDO, behoudens het bepaalde in Artikel 19 en tenzij Partijen hiertoe wettelijk verplicht zijn. Deze verstrekking wordt schriftelijk vastgelegd door de Procesregisseur.
- 23.2. Indien een verstrekking van Persoonsgegevens aan derden plaatsvindt, is dat een individuele afweging van elke Partij op grond van zijn eigen wet- en regelgeving en komt voor de eigen verantwoordelijkheid van elke partij.

Artikel 24. Verwerkingsregister en Functionaris Gegevensbescherming

- 24.1. Partijen registreren hun Verwerkingen van Persoonsgegevens onder dit Protocol in een eigen register van verwerkingsactiviteiten.

- 24.2. Aanvullend neemt Procesregisseur de Verwerkingen van Persoonsgegevens op locatie en in de informatiesystemen van het zorg- en veiligheidshuis op in een gezamenlijk register van verwerkingsactiviteiten onder dit Protocol ten behoeve van Partijen.
- 24.3. Het register van verwerkingsactiviteiten bevat minimaal de volgende informatie:
- a. De naam en contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken (of diens vertegenwoordiger);
 - b. De verwerkingsdoeleinden;
 - c. Een beschrijving van de categorieën Persoonsgegevens die worden Verwerkt;
 - d. Een beschrijven van de categorieën Betrokkenen;
 - e. De categorieën van ontvangers aan wie de Persoonsgegevens worden (of zullen worden) verstrekt;
 - f. Indien van toepassing, doorgifte van Persoonsgegevens aan derde landen of internationale organisaties.
- 24.4. De Functionarissen Gegevensbescherming van de afzonderlijke Partijen hebben, zonder aankondiging van bezoek vooraf, recht op toegang tot de gebouwen en overleg ruimtes van het zorg- en veiligheidshuis en tot de Verwerkingen en register van Verwerkingen, alsook toegang tot enige andere informatie, voor zover dit noodzakelijk is voor diens toezichthoudende werkzaamheden.
- 24.5. De Privacy Adviseur van het zorg- en veiligheidshuis dient als eerste aanspreekpunt voor de betrokken Functionarissen Gegevensbescherming.
- 24.6. De Functionarissen Gegevensbescherming van de Verwerkingsverantwoordelijken houden toezicht op de naleving van de verplichtingen in dit Protocol en zijn bevoegd aanwijzingen te geven aan de Manager en Procesregisseur.

Artikel 25. Aansprakelijkheid

- 25.1. Partijen zetten zich in voor een goede uitvoering van het bepaalde in dit Protocol en zullen zich houden aan de in dit Protocol gemaakte afspraken.
- 25.2. Partijen zijn ieder voor zich aansprakelijk voor aanspraken van Betrokkenen, of Derden op schadevergoeding op grond van directe of indirecte schade, administratieve boetes of andere aanspraken van derden in geval van toerekenbare tekortkoming door de aangesproken Partij in de nakoming van het bepaalde in dit Protocol en de bijbehorende Bijlagen.
- 25.3. Wanneer meerdere Verwerkingsverantwoordelijken of Verwerkers bij dezelfde Verwerking betrokken zijn, en verantwoordelijk zijn voor schade die door die Verwerking is veroorzaakt, wordt elke Verwerkingsverantwoordelijke of Verwerker voor de gehele schade aansprakelijk gehouden teneinde te garanderen dat de schade van betrokkene daadwerkelijk wordt vergoed.
- 25.4. Een Verwerker is slechts aansprakelijk voor de schade die door Verwerking is veroorzaakt wanneer bij de Verwerking niet is voldaan aan de specifiek tot Verwerkers gerichte verplichtingen van de Algemene Verordening Gegevensbescherming of buiten dan wel in strijd met de rechtmatige instructies van de Verwerkingsverantwoordelijke is gehandeld.
- 25.5. Onverminderd het gestelde in lid 4 kan iedere Verwerkingsverantwoordelijke of Verwerker die de volledige vergoeding heeft betaald vervolgens bij de andere Verwerkingsverantwoordelijken of Verwerkers die bij dezelfde Verwerking betrokken zijn, kunnen het deel van de schadevergoeding verhalen dat overeenkomt met hun deel van de aansprakelijkheid voor de schade. Een Verwerkingsverantwoordelijke of Verwerker kan door

andere Verwerkingsverantwoordelijken of Verwerkers worden vrijgesteld van onderlinge betaling van schadevergoeding indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.

Artikel 26. Toezicht en handhaving

- 26.1. Onverminderd de verantwoordelijkheden van de Functionarissen Gegevensbescherming van de verwerkingsverantwoordelijken houden de Manager en de Procesregisseur toezicht op de naleving van de verplichtingen in dit Protocol en zijn bevoegd aanwijzingen te geven aan medewerkers in het zorg- en veiligheidshuis omtrent de uitvoering van het bepaalde in dit Protocol.

Artikel 27. Wijzigingen

- 27.1. De bepalingen in dit Protocol kunnen door de Partijen in gezamenlijk overleg worden gewijzigd. Wijzigingen in dit Protocol worden door het Managersoverleg besloten. Mondelinge mededelingen, toezeggingen of afspraken welke betrekking hebben op de inhoud van dit Protocol, hebben geen rechtskracht, tenzij deze uitdrukkelijk schriftelijk zijn bevestigd door de Manager.
- 27.2. Wijziging van het Protocol vergt het opnieuw ondertekenen door Partijen van het gewijzigde Protocol, indien de wijziging de kern van het Protocol raakt.
- 27.3. In geval van wijzigingen, waaronder inbegrepen toetreding van een nieuwe organisatie tot dit Protocol, die door een Partij onaanvaardbaar worden ervaren, kan deze Partij deelname aan het zorg- en veiligheidshuis schriftelijk opzeggen met ingang van het tijdstip waarop het gewijzigde Protocol van kracht wordt. Na opzegging van deelname aan het Convenant en dit Protocol verkrijgt die Partij niet langer toegang tot de Persoonsgegevens die op locatie of in de informatiesystemen van het zorg- en veiligheidshuis worden verwerkt onder dit Protocol.

Artikel 28. Toetreding

- 28.1. Toetreding door andere organisaties tot dit Protocol kan enkel wanneer die Partij is toegetreden conform Artikel 21 van dat Convenant.
- 28.2. Partijen worden vooraf door de secretaris van de Stuurgroep op de hoogte gebracht van de voorgenomen toetreding. Indien de toetredende partij niet staat benoemd in het Handvat dient voorafgaand aan de uitwisseling van Persoonsgegevens met de toetredende partij een juridische analyse te worden opgesteld conform hoofdstuk 5 van het Handvat. De toetredende Partij voert waar nodig de aanbeveling uit die analyse uit, alvorens uitwisseling van Persoonsgegevens in het zorg- en veiligheidshuis met die partij plaatsvindt.
- 28.3. In geval van toetreding tot het Convenant, vindt toetreding tot het Protocol plaats door middel van ondertekening van Bijlage 1 bij dit Protocol door die andere organisatie en de voorzitter van de Stuurgroep.

Artikel 29. Duur, opzegging, beëindiging

- 29.1. Dit Protocol treedt in werking op de dag van ondertekening door Partijen en wordt voor dezelfde duur als het Convenant. In geval van verlenging van het Convenant wordt dit Protocol met een gelijklopende termijn verlengd.

- 29.2. De Stuurgroep kan, zonder rechterlijke tussenkomst en met meerderheid van stemmen, na ingebrekestelling, een Partij met onmiddellijke ingang uitsluiten van de samenwerking in het zorg- en veiligheidshuis, indien de afspraken zoals neergelegd in dit Protocol niet door de desbetreffende Partij worden nagekomen.
- 29.3. Verplichtingen die naar hun aard zijn bestemd om ook na beëindiging of uitsluiting van het project voort te duren, blijven na beëindigingen van dit Protocol bestaan. Tot deze verplichtingen behoren onder meer die ter zake van geheimhouding en de beveiliging van Persoonsgegevens.

Artikel 30. Opvolging

- 30.1. Dit Protocol vervangt alle eerdere door Partijen gesloten Protocollen met betrekking tot de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis voor de doelen zoals beschreven in Artikel 3.1 van dit Protocol.

Artikel 31. Monitoring, toezicht, audit, wetenschappelijk onderzoek en evaluatie

- 31.1 In het kader van een opdracht tot uitvoering van een wetenschappelijk onderzoek zijn Partijen gezamenlijk opdrachtgever en worden de specifieke bepalingen uit wet- en regelgeving alsmede de interne voor Partijen geldende voorschriften voor wetenschappelijk onderzoek van Partijen in acht genomen.
- 31.2 Partijen zullen dit Protocol twee jaar na inwerking treden landelijk en regionaal evalueren, waarbij bij voorkeur een audit zal plaatsvinden door een externe onafhankelijke partij.

Artikel 32. Toepasselijk recht

- 32.1. Op dit Protocol is Nederlands recht van toepassing.

Aldus overeengekomen:

Partijen hebben kennis genomen van artikel 1 tot en met 32 en de bijlagen 1 tot en met 4 van dit Privacyprotocol en tekenen voor akkoord

Gemeente
in dezen rechtsgeldig vertegenwoordigd door:
Datum en plaats:

Bijlage 1: Toetredingsformulier nieuwe partner tot Protocol

[naam organisatie], statutair gevestigd te [...] en kantoorhoudend aan [...], hierbij rechtsgeldig vertegenwoordigd door [naam, functie],

overwegende dat:

- Deelname aan het Protocol gelet op de publieke en/of maatschappelijke taak die zichzelf in het kader van integrale veiligheid en complexe casuïstiek toedicht en gelet op de verantwoordelijkheid en/of bevoegdheid van ondergetekende een bijdrage levert aan de doelstelling zoals geformuleerd in artikel 2 van het Convenant en artikel 3.2 van het Protocol;
- De Stuurgroep positief heeft besloten op toetreding van ondergetekende aan het Convenant en dit Protocol;

verklaart daartoe het volgende:

- Ondergetekende onderschrijft de in het Protocol geformuleerde doelstellingen, verplicht zich de bepalingen in het Protocol te zullen naleven en verklaart zich in dit kader gerechtigd tot het uitwisselen van Persoonsgegevens met Partijen.

Aldus ondertekend te [...], op datum [...]

Naam organisatie:

Naam bevoegde functionaris:

.....

Namens Stuurgroep:

Naam:

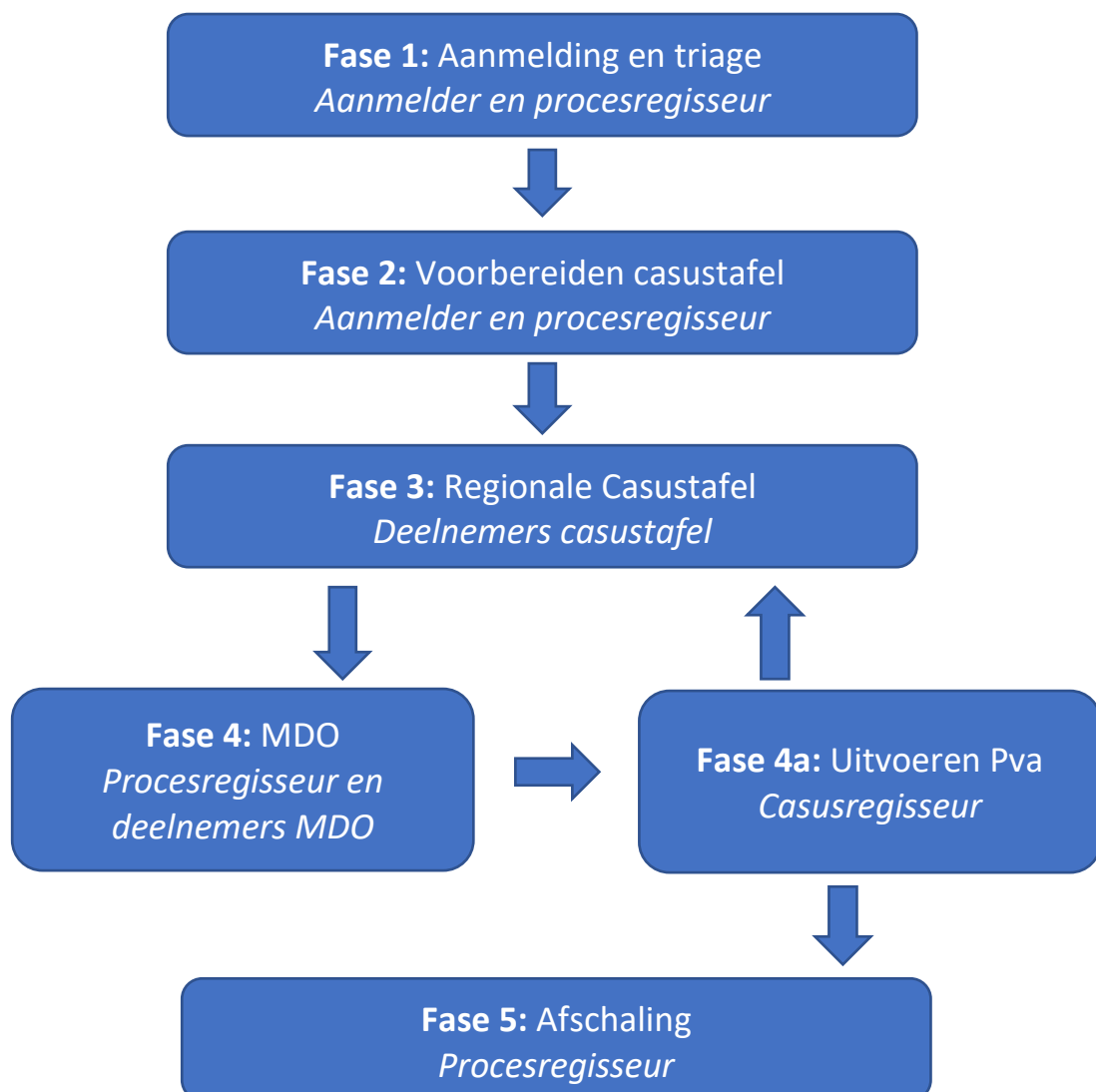
.....

Bijlage 2: Werkproces zorg- en veiligheidshuis

Partijen Verwerken in het kader van het zorg- en veiligheidshuis voor ieder van onderstaande fasen enkel de Persoonsgegevens die voor die afzonderlijke fase noodzakelijk zijn voor de uitvoering van ieder van de daarbij geformuleerde processtappen. Deze zijn hieronder weergegeven.

Dit werkproces geldt voor casuïstiek op in ieder geval de gebieden:

- a. Veelplegers
- b. Top x (zwaar overlastgevende casuïstiek met veiligheidsrisico)
- c. Risicjongeren
- d. Complexe GGZ met veiligheidsrisico



	Toelichting werkproces Veiligheidshuis	Belangrijkste betrokkenen
Het algemene werkproces op gebied van complexe domeinoverstijgende casuïstiek is gericht op het voorkomen en verminderen van recidive, (ernstige) overlast, criminaliteit, maatschappelijke onrust, en maatschappelijke uitval bij complexe problemen, door een combinatie van repressie, bestuurlijke interventie én zorg, hetgeen gezien moet worden als een zwaarwegende taak van algemeen belang.		
Fase 1: Aanmelding en triage	De aanmelding komt vanuit de partners bij de procesregisseurs van het Veiligheidshuis. Procesregisseur stemt deze aanmelding af met in ieder geval de betrokken gemeente en vult samen met andere partners het beeld aan. Gezamenlijk wordt bepaald waar de casus thuishoort en op welke casustafel de casus wordt besproken. Procesregisseur legt de casus vast in GCOS. Doel: Registreren en verrijken bekende informatie	<i>Aanmeldende partij en procesregisseur</i>
Fase 2: Voorbereiden Casustafel	De administratief medewerker ondersteuning Casustafels stelt, in overleg met de procesregisseurs, de agenda voor de casustafels op en nodigt de benodigde partners uit voor casustafels. Wordt vastgelegd in GCOS. Doel: voorbereiden casustafel, uitnodigen partners	<i>Administratief medewerker Ondersteuning Casustafels en procesregisseurs</i>
Fase 3: Regionale Casustafel	Tijdens de casustafel wordt kort besproken welke stappen ondernomen moeten worden in de casus en wordt de richting van het plan van aanpak bepaald. Ook wordt bepaald wie procesregie voert. Casuïstiek die al eerder besproken is, kan hier gemonitord worden. Per casus kunnen de volgende besluiten genomen worden: - Afschalen - Procesregie elders dan VHH - Procesregie VHH - ISD - ZSM advies Doel: gedragen richting casus bepalen, procesregisseur aanwijzen en monitoren	<i>Procesregisseur (voorzitter), deelnemers casustafel, administratief medewerker Ondersteuning Casustafels</i>
Fase 4: MDO	Tijdens het MDO wordt gezamenlijk het plan van aanpak opgesteld. Ook wordt bepaald wie de Casusregisseur wordt en wie de cliënt informeert. Afspraken worden vastgelegd. Doel: formuleren plan van aanpak, afstemmen casusregie	<i>Procesregisseur (voorzitter), deelnemers MDO</i>

Fase 4a: Uitvoeren plan van aanpak	Voortgang plan van aanpak wordt besproken op de Regionale casustafel en/of MDO's en zo nodig wordt het plan van aanpak bijgesteld. Uiteraard kan ook besloten worden tot afschaling van betrokkenheid van het Veiligheidshuis (Fase 5). Doel: uitvoering, monitoring en besluit tot bijstellen of afschalen casuïstiek	<i>Casusregisseur in overleg met procesregisseur Veiligheidshuis en bij plan van aanpak betrokken partners</i>
Fase 5: Afschalen	De laatste fase is de afschaling. Dit geschiedt gefaseerd. Na het besluit tot Afschalen worden Persoonsgegevens gefaseerd verwijderd, conform artikel 11 van het Privacy Protocol. Doel: monitoring en tot slot vernietigen (persoons-) gegevens.	<i>Procesregisseur en betrokken partners (vooral bij overdracht)</i>

Bijlage 3: Beveiligingsbeleid Persoonsgegevens

Partijen dienen een beleid op te stellen dat ziet op de bescherming van Persoonsgegevens. Hiervoor kan aansluiting worden gezocht bij het informatiebeveiligingsbeleid, doch daar dient dan expliciet aandacht te worden besteed aan de technische en organisatorische maatregelen ten behoeve van de bescherming van Persoonsgegevens. Deze maatregelen dienen passend te zijn met het oog op het risico voor Betrokkenen en conform de “Cbp Richtsnoeren – Beveiliging van persoonsgegevens” ten minste het volgende te bevatten:

- **Beleidsdocument voor informatiebeveiliging**
Het beleidsdocument gaat expliciet in op de maatregelen die de verantwoordelijke treft om de verwerkte persoonsgegevens te beveiligen. Het document is goedgekeurd op bestuurlijk c.q. leidinggevend niveau en kenbaar gemaakt aan alle werknemers en relevante externe partijen.
- **Toewijzen van verantwoordelijkheden voor informatiebeveiliging**
Alle verantwoordelijkheden, zowel op sturend als op uitvoerend niveau, zijn duidelijk gedefinieerd en belegd.
- **Beveiligingsbewustzijn**
Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers krijgen geschikte training en regelmatige bijscholing over het informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures van de organisatie, voor zover relevant voor hun functie. Binnen de training en bijscholing wordt expliciet aandacht besteed aan de omgang met persoonsgegevens.
- **Fysieke beveiliging en beveiliging van apparatuur**
IT voorzieningen en apparatuur zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. De geboden bescherming is in overeenstemming met de vastgestelde risico's.
- **Toegangsbeveiliging**
Er zijn procedures om bevoegde gebruikers toegang te geven tot de informatiesystemen en -diensten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen. De procedures omvatten alle fasen in de levenscyclus van de gebruikerstoegang, van de eerste registratie van nieuwe gebruikers tot de uiteindelijke afmelding van gebruikers die niet langer toegang tot informatiesystemen en -diensten nodig hebben. Waar van toepassing wordt bijzondere aandacht besteed aan het beheren van toegangsrechten van gebruikers met extra ruime bevoegdheden, zoals systeembeheerders.
- **Logging en controle**
Activiteiten die gebruikers uitvoeren met persoonsgegevens worden vastgelegd in logbestanden. Hetzelfde geldt voor andere relevante gebeurtenissen, zoals pogingen om ongeautoriseerd toegang te krijgen tot persoonsgegevens en verstoringen die kunnen leiden tot verminking of verlies van persoonsgegevens. De logbestanden worden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de persoonsgegevens en waar nodig wordt actie ondernomen.
De verantwoordelijke moet er rekening mee houden dat er, als de gegevens in de logbestanden tot personen herleidbaar zijn, sprake is van een verwerking van

persoonsgegevens in de zin van de [AVG] waarop de verplichtingen uit deze wet van toepassing zijn. In dat geval kan er ook sprake zijn van een personeelsvolgsysteem in de zin van artikel 27 lid 1 van de Wet op de ondernemingsraden (WOR), waarvoor instemming van de ondernemingsraad is vereist.

- **Beheer van technische kwetsbaarheden**

Software, zoals browsers, virusscanners en operating systems, wordt up-to-date gehouden. Ook installeert de verantwoordelijke tijdig oplossingen die de leverancier uitbrengt voor beveiligingslekken in deze software. Meer in het algemeen verkrijgt de verantwoordelijke tijdig informatie over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden wordt geëvalueerd en de verantwoordelijke treft geschikte maatregelen getroffen voor de behandeling van de risico's die daarmee samenhangen.

- **Incidentenbeheer**

Er zijn procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging, zodra ze zijn gerapporteerd. Het beoordelen van de risico's voor de betrokkenen en het effectief informeren van de betrokkenen en, waar van toepassing, de toezichthouder is in deze procedures opgenomen. De lessen getrokken uit de afgehandelde incidenten worden gebruikt om de beveiliging waar mogelijk structureel te verbeteren. Als een vervolgprocedure na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), wordt het bewijsmateriaal verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

- **Afhandeling van datalekken en beveiligingsincidenten**

De verantwoordelijke meldt datalekken die onder een wettelijke meldplicht vallen bij de betreffende toezichthouder.⁷³ Als hij daartoe wettelijk verplicht is, of als er anderszins aanleiding voor is, informeert hij ook de betrokkenen over het beveiligingsincident of het datalek.

- **Continuïteitsbeheer**

Door natuurrampen, ongevallen, uitval van apparatuur of opzettelijk handelen kunnen persoons gegevens verloren gaan. Door in de organisatie continuïteitsbeheer in te richten worden de gevolgen tot een aanvaardbaar niveau beperkt, waarbij gebruik wordt gemaakt van een combinatie van preventieve maatregelen en herstelmaatregelen.

Er is pas sprake van een passend beveiligingsniveau als de gekozen maatregelen onderdeel zijn van de dagelijkse praktijk van de organisatie. De eerste stap is documentatie: de relevante beveiligings maatregelen zijn gespecificeerd en geïntegreerd in functionele en technische beschrijvingen van ict systemen, in gebruikershandleidingen, werkinstructies, contracten, dienstenniveauovereenkomsten en andere relevante documenten. De tweede stap is daadwerkelijke implementatie van de gekozen maatregelen.

Een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker, alsmede de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, verwerkt deze slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen.”

De hierboven genoemde maatregelen ‘beveiligingsbewustzijn’, ‘toegangsbeveiliging’ en ‘logging en controle’ zijn er mede op gericht om ongeoorloofde omgang met persoonsgegevens binnen de organisatie tegen te gaan. “

De Autoriteit Persoonsgegevens sluit hierbij grotendeels aan op de EN-ISO/IEC 27002:2017. Voor de Verwerking van bijzondere Persoonsgegevens, meer in het bijzonder gegevens betreffende iemands gezondheid, verwijst de Autoriteit Persoonsgegevens ook naar de NEN7510.

De fysieke documenten betreffende het beveiligingsbeleid Persoonsgegevens van de Beheergemeente Zwolle die zijn op te vragen bij de gemeente Zwolle.

Bijlage 4: Categorieën Persoonsgegevens en Betrokkenen

Partijen Verwerken ten behoeve van de doelstellingen en onder voorwaarden zoals beschreven in dit Protocol enkel de volgende categorieën Persoonsgegevens van de volgende categorieën Betrokkenen:

Categorie 1:

Categorie Betrokkenen:

Van Personen, op wie het onder dit Protocol beschreven plan van aanpak en bijbehorende interventies zijn gericht, worden geen andere dan de volgende categorieën Persoonsgegevens verwerkt:.

Persoonsgegevens:

- volledige personalia (naam, geboorteplaats, geboortedatum);
- adresgegevens (straat, huisnummer, postcode, woonplaats);
- gegevens omtrent woonsituatie;
- financiële gegevens;
- gegevens betreffende relaties met overige gezinsleden/ directe sociale contacten;
- toezicht- en handavingsgegevens, gegevens omtrent bestuursrechtelijke maatregelen of voornemens daartoe

Strafrechtelijke Persoonsgegeven, te weten:

- Politiegegevens (artikel 8 en 13 Politiegegevens);
- Strafvorderlijke gegevens en relevante justitiële gegevens;
- Tenuitvoerleggingsgegevens

Bijzondere Persoonsgegevens, te weten:

- Burgerservicenummer (BSN)
- Gegevens over gezondheid;
- Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.

Categorie 2:

Categorie Betrokkenen:

Van directe relaties van Categorie1 Betrokkenen, waaronder gezinsleden en directe sociale contacten, worden geen andere dan de volgende categorieën Persoonsgegevens verwerkt:

Persoonsgegevens:

- volledige personalia (naam, geboortedatum, geboorteplaats);
- adresgegevens (straat, huisnummer, postcode, woonplaats);
- contactgegevens (telefoonnummer, e-mailadres);
- toezicht- en handavingsgegevens of omtrent bestuurlijke maatregelen of voornemens daartoe voor zo ver in directe relatie met Betrokkene van Categorie 1;

- Gegevens omtrent inzage verzoeken, verzoeken om rectificatie, verzet en klachten.

Strafrechtelijke Persoonsgegevens (indien van toepassing), te weten:

- Politiegegevens (artikel 8 en 13 Politiegegevens);
- Strafvorderlijke gegevens;

Bijzondere Persoonsgegevens en gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten zoals bedoeld in artikel 9 en 10 AVG, te weten:

- Gegevens over gezondheid;
- Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.

Categorie 3:

Categorie Betrokkenen:

Van medewerkers van instanties of instellingen die betrokken zijn bij de begeleiding, zorg- en hulpverlening van betrokkene (ook interventies voorafgaande aan de Aanmelding), worden geen andere dan de volgende categorieën Persoonsgegevens verwerkt:

Persoonsgegevens:

- naam;
- naam organisatie organisatieaanduiding (typering bijv. instelling voor GGZ);
- Contactgegevens (zakelijk telefoonnummer, e-mailadres);
- Datum start betrokkenheid en einde betrokkenheid

Categorie 4:

Categorie Betrokkenen:

Van Medewerkers van derden die betrokken zijn bij de uitvoering van interventies (ook interventies voorafgaande aan de Aanmelding), worden geen andere dan de volgende categorieën

Persoonsgegevens verwerkt:

Persoonsgegevens:

- naam;
- naam organisatie organisatieaanduiding (typering bijv. instelling voor GGZ);
- functie binnen het zorg- en veiligheidshuis;
- contactgegevens (zakelijk telefoonnummer, e-mailadres);

Toelichting:

Bovenstaande categorieën zijn voor de gemeenten en zorg en welzijnspartijen niet uitputtend en dienen door Partijen nader te worden ingevuld in overleg met de privacy adviseurs van de gemeenten en zorginstellingen.