

# Privacy Protocol

Integrale veiligheid en complexe multi-problematiek  
Zorg en Veiligheidshuis Twente

## Context

De samenwerking bij het behandelen van complexe casuïstiek kan in het algemeen niet zonder het uitwisselen van persoonsgegevens. Het omgaan met persoonsgegevens van burgers is aan wetgeving gebonden. Het Europees Verdrag van de Rechten van de Mens, het Handvest van de grondrechten van de Europese Unie, de Grondwet en Europese en nationale wetgeving schrijven voor dat overheden c.q. bestuursorganen, instellingen en bedrijven alleen om bepaalde redenen een inbreuk mogen maken op het persoonlijk leven van burgers en uitsluitend op basis van een wettelijke regeling.

Voor samenwerkingsverbanden in het zorg- en veiligheidsdomein rondom complexe casuïstiek betekent dit dat er slechts persoonsgegevens van burgers kunnen worden uitgewisseld als daarvoor een specifieke wettelijke grondslag is aan te wijzen. Die wettelijke grondslag voor de uitwisseling van persoonsgegevens is niet in één wet te vinden. De privacywet Algemene Verordening Gegevensverwerking (hierna 'AVG') vormt de basis, maar de diverse organisaties en professionals in de samenwerkingsverbanden hebben ook te maken met andere wet- en regelgeving zoals de Wet geneeskundige behandelovereenkomst (hierna 'WGBO'), de Jeugdwet, de Wet politiegegevens (hierna 'Wpg'), de Wet Justitiële en strafvorderlijke gegevens (hierna 'Wjsg') en de Reclasseringsregeling 1995.

Het is hierbij goed om voor ogen te houden dat het uitwisselen van gegevens, maar ook het correct toepassen van de privacyregels een belangrijk doel dient. De samenwerking tussen het zorg- en veiligheidsdomein is gericht op hulp aan burgers die kampen met (complexe) multi-problematiek ten behoeve van een veilige samenleving. Om die hulp effectief te laten zijn, is het belangrijk dat deze personen vertrouwen hebben en houden in zorgprofessionals en zorginstellingen, in de Raad voor de Kinderbescherming, reclasseringsinstellingen, het Openbaar Ministerie, politie, gemeenten en andere overheden. Dat houdt onder andere in dat men weet dat er bij het omgaan met zijn/haar persoonsgegevens zorgvuldigheid wordt betracht. Even belangrijk is dat partners in de samenwerking erop kunnen vertrouwen dat alle partners zorgvuldig met persoonsgegevens omgaan.

Het toepassen van de verschillende wettelijke regels kan soms lastig zijn, bijvoorbeeld omdat de wetgeving niet altijd een pasklaar antwoord biedt op de vraag of gegevens uitgewisseld mogen worden. Soms ervaren de betrokken organisaties en professionals de privacyregels als een probleem. Inzicht in de mogelijkheden die andere partijen hebben om persoonsgegevens uit te wisselen, kan dan helpen bij het maken van afwegingen over het uitwisselen van persoonsgegevens. Met dit Privacy Protocol integrale veiligheid en complexe multi-problematiek Zorg en Veiligheidshuis Twente (hierna 'Privacy Protocol') proberen we daarin te voorzien en zijn afspraken rondom de uitwisseling en het verdere gebruik van persoonsgegevens door en tussen verschillende partijen in het Zorg en Veiligheidshuis Twente (hierna 'ZVH') 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 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, met uitzondering van hetgeen al is geregeld in het bijbehorende Convenant.

De in dit Privacy Protocol gehanteerde terminologie is gebaseerd op de AVG, de Wpg en de Wjsg. Het is tot stand gekomen in samenwerking tussen (privacy)adviseurs van verschillende landelijke partijen, Considerati en het Ministerie van Justitie en Veiligheid.

Verder is aangesloten bij de werkwijze zoals beschreven in de tweede herziene uitgave van het Handvat “Gegevensuitwisseling bij samenwerking rond casuïstiek in het zorg- en veiligheidsdomein, een juridisch kader”, versie 2.2., juli 2020 (hierna ‘Handvat’). Hierin zijn belangrijke samenwerkingsafspraken, zoals over gegevensuitwisseling tussen partijen en de verwerkingscapaciteiten binnen het samenwerkingsverband, nader uitgewerkt. Ook formuleringen, begrippen en andere specifieke ZVH-gerelateerde termen zijn afgeleid uit dit Handvat en het Landelijk Kader Veiligheidshuizen. Daarnaast is geput uit het eerdere samenwerkingsconvenant.

Goed om in deze context nog te benoemen is dat het Handvat in opdracht van de landelijke stuurgroep zorg- en veiligheid geactualiseerd is op basis van de AVG, de Uitvoeringswet AVG en de – als gevolg van de Richtlijn gegevensbescherming opsporing en vervolging – gewijzigde Wpg en de Wjsg.

Dit Handvat kan gemakkelijk (online) bekeken worden via onderstaande link voor het raadplegen van het algemeen juridisch kader gegevensverwerking, de grondslagen per organisatie (vanaf pagina 23) en voor toepassing van het Handvat in de praktijk. Dit zorgt voor helderheid en neemt onduidelijkheden zo veel mogelijk weg.

<https://vng.nl/sites/default/files/2020-08/handvat-gegevensuitwisseling-zvh-versie-2.2.pdf>

## Privacy Protocol integrale veiligheid en complexe multi-problematiek ZVH Twente

De ondergetekenden, zijnde:

De gemeenten:

- Almelo;
- Borne;
- Dinkelland;
- Enschede;
- Haaksbergen;
- Hellendoorn;
- Hengelo;
- Hof van Twente;
- Losser;
- Oldenzaal;
- Rijssen-Holten;
- Tubbergen;
- Twenterand;
- Wierden;

ieder rechtsgeldig vertegenwoordigd door de burgemeester of het college van burgemeester en wethouders, ieder voor zover het zijn bevoegdheid betreft. Verder afzonderlijk aangeduid als 'Partij' of 'Gemeente' en gezamenlijk als 'Gemeenten',

en de ketenpartners:

- Dienst Justitiële Inrichtingen;
- Humanitas onder dak Twente;
- GGD Twente;
- Jeugdbescherming Overijssel;
- Leger des Heils Jeugdbescherming en Reclassering;
- Mediant;
- OM Arrondissementsparket Oost-Nederland;
- Politie Regionale Eenheid Oost-Nederland;
- Raad voor de Kinderbescherming;
- Reclassering Nederland;
- Stichting Dimence;
- Stichting Maatschappelijke dienstverlening Enschede-Haaksbergen;
- Stichting Tactus Sociale Verslavingszorg;
- Stichting Tactus Verslavingsreclassering;
- Stichting Transfore;
- Veilig Thuis Twente;

ieder rechtsgeldig vertegenwoordigd door een bevoegde functionaris. Hierna afzonderlijk te noemen 'Partij' en gezamenlijk, inclusief gemeenten, te noemen 'Partijen'.

De volgende overwegingen in aanmerking nemende:

- Partijen in het kader van samenwerking op het gebied van integrale veiligheid en complexe casuïstiek, zoals beschreven in het 'Landelijke Kader Veiligheidshuizen van het Ministerie van Veiligheid en Justitie, vastgesteld in januari 2013' (hierna 'Landelijk Kader'), het ZVH hebben opgezet.
- Partijen voor deze samenwerking afspraken vastleggen in het Convenant 'Samenwerkingsconvenant tussen ketenpartners Zorg-en Veiligheidshuis Twente' (hierna 'het Convenant'), welke gelijktijdig met dit Privacy Protocol vastgesteld wordt en waar dit Privacy Protocol deel van uitmaakt.
- Voor de samenwerking in het ZVH de uitwisseling van (bijzondere) (persoons-) gegevens tussen de Partijen noodzakelijk is.
- In het door Partijen opgezette ZVH persoonsgegevens worden verwerkt ten dienste en onder verantwoordelijkheid van partijen.
- Partijen slechts die persoonsgegevens binnen het ZVH 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 samenwerken.
- Dit Privacy Protocol de gedragsregels omschrijft voor 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.
- Met dit Privacy Protocol invulling wordt gegeven aan de in artikel 26 van de AVG neergelegde verplichting voor partijen om op een transparante wijze hun samenwerkingsafspraken en hun verantwoordelijkheden jegens elkaar en jegens betrokkene(n) vast te leggen.

Verklaren te zijn overeengekomen als volgt:

## Artikel 1. Definities

De onderstaande definities zullen hierna met een hoofdletter in dit Privacy Protocol worden weergegeven. In dit Privacy Protocol en de daarbij behorende bijlage(n) wordt verstaan onder:

- 1.1. **Aanmelding:** het voordragen van een Casus door één der Partijen en het uitwisselen van informatie, waaronder Persoonsgegevens, tussen de Procesregisseur van het ZVH en de aanmeldende Partij ter toetsing of de Casus in aanmerking komt voor behandeling in het ZVH.
- 1.2. **Afschaling:** de fase die volgt op het besluit van de Regionale Casustafel dat de betrokkenheid van het ZVH niet langer nodig is, waarin het dossier dat in het systeem van het ZVH is aangelegd ten behoeve van procesregie, geschoond wordt van alle niet langer noodzakelijke informatie en uiteindelijk verdwijnt uit het systeem van het ZVH.
- 1.3. **Afzonderlijke Verwerkingsverantwoordelijken:** Partijen zijn Afzonderlijke Verwerkingsverantwoordelijke voor zelfstandige Verwerkingen wanneer verschillende Verwerkingen min of meer geïntegreerd zijn, maar er geen sprake is van Gezamenlijke Verwerkingsverantwoordelijken.
- 1.4. **AVG:** Algemene Verordening Gegevensbescherming (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 over de bescherming van natuurlijke personen in verband met de Verwerking van Persoonsgegevens en over het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.
- 1.5. **Betrokkene:** de natuurlijke persoon op wie informatie, waaronder Persoonsgegevens, betrekking heeft (artikel 4 onder 1 van de AVG).
- 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 AVG.
- 1.7. **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 ZVH ter beoordeling en eventuele bespreking in de Regionale Casustafel.
- 1.8. **Casusregie:** het uitvoeren van werkzaamheden gericht op het bewaren van de onderlinge samenhang bij het uitvoeren van het gezamenlijk opgestelde Plan van Aanpak bij het behandelen van één specifieke Casus.
- 1.9. **Casusregisseur:** medewerker van één van de Partijen die belast is met de taken in artikel 12 van het Convenant.
- 1.10. **Derde:** een natuurlijk persoon of rechtspersoon, niet zijnde de Betrokkene, noch één der Partijen van dit Privacy Protocol.
- 1.11. **DVO:** Districtelijk Veiligheidsoverleg.
- 1.12. **Expertgroepoverleg:** de Expertgroep Zorg, Veiligheid en Straf. Het verband van afgevaardigden van Partijen zoals geformuleerd in artikel 5 van het Convenant.
- 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. **GCOS:** Generiek Casusoverleg Ondersteunend Systeem van het ZVH.
- 1.15. **Informatiecoördinator:** persoon die is belast met de taken zoals geformuleerd in artikel 13 van het Convenant.

- 1.1. **Jaarplan:** het door de Stuurgroep voorgestelde, op grond van artikel 4.4 van het Convenant, door de Partijen vastgestelde plan over de operationele en inhoudelijke kaders en het financieel en inhoudelijk beleid van het ZVH.
- 1.16. **Justitiële gegevens:** bij algemene maatregel van bestuur omschreven Persoonsgegevens of gegevens over een rechtspersoon over de toepassing van het strafrecht of de strafvordering, die in een bestand worden verwerkt (artikel 1 sub a Wjsg, respectievelijk Besluit Justitiële strafvorderlijke gegevens (hierna 'Bjsg').
- 1.17. **Landelijk Kader:** het 'Landelijk Kader Veiligheidshuizen – vóór en dóór partners', opgesteld door het Ministerie van Veiligheid en Justitie, d.d. januari 2013.
- 1.18. **Manager:** de persoon die belast is met de taken zoals geformuleerd in artikel 10 van het Convenant.
- 1.19. **Multidisciplinair overleg:** fase waarin gezamenlijk het Plan van Aanpak wordt opgesteld.
- 1.20. **Ondersteuner Regionale Casustafels:** de persoon die belast is met de taken zoals geformuleerd in artikel 14 van het Convenant.
- 1.21. **Persoonsgegevens:** alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de Betrokkene) als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4 onder 1 van de AVG).
- 1.22. **Plan van Aanpak:** het samenstel van acties, interventies en afspraken over een persoon of (gezin)systeem wat als doel heeft het perspectief van hem/haar/hen te verbeteren en overlast en gevaar voor veiligheid voor de omgeving te stoppen of te verkleinen. Het Plan van Aanpak kan ook de vorm van een scenario krijgen en is altijd gebaseerd op een integraal informatiebeeld.
- 1.23. **Politiegegevens:** elk Persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt (artikel 1 sub a Wpg).
- 1.24. **Privacy adviseur:** een medewerker in het ZVH of vallend onder één van de Partijen die belast is met de advisering op privacyvraagstukken. Deze persoon is ook belast met beleidsontwikkeling over gegevensverwerking en helpt mee met de voorbereiding van audits.
- 1.25. **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.
- 1.26. **Procesregisseur:** de medewerker van het ZVH die namens een van de Partijen belast is met de werkzaamheden zoals opgenomen in artikel 11 van het Convenant.
- 1.27. **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 een Casus kan worden afgeschaald.
- 1.28. **Strafrechtelijke persoonsgegevens:** Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen zoals bedoeld in artikel 10 van de AVG.
- 1.29. **Strafvorderlijke gegevens:** Persoonsgegevens of gegevens over een rechtspersoon die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het Openbaar Ministerie (hierna 'OM') in een strafdossier of langs geautomatiseerde weg verwerkt in een gegevensbestand (artikel 1 sub b Wjsg).
- 1.30. **Stuurgroep:** de Stuurgroep Zorg, Veiligheid en Straf. Het verband van afgevaardigden van Partijen zoals geformuleerd in artikel 4 van het Convenant.

- 1.31. **Tenuitvoerleggingsgegevens:** Persoonsgegevens of gegevens van een rechtspersoon over de tenuitvoerlegging van strafrechtelijke beslissingen die in een dossier of een ander gegevensbestand zijn of worden verwerkt.
- 1.32. **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.
- 1.33. **Verwerker:** een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt (artikel 4 onder 8 van de AVG).
- 1.34. **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 van de AVG).
- 1.35. **Verwerkingsverantwoordelijke(n):** een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die, 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 al zijn bepaald wie de Verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen (artikel 4 onder 7 van de AVG).
- 1.36. **Vis2:** cliënt-volgsysteem van het ZVH.
- 1.37. **Werkproces:** het door het Expertgroepoverleg op grond van artikel 5.4 onder c van het Convenant, vastgestelde proces voor samenwerking in het ZVH, waaronder het proces over- en het delen van informatie en het op- en afschalen van een Casus.

## Artikel 2. Afzonderlijke en Gezamenlijke Verwerkingsverantwoordelijken

- 2.1. Partijen in het ZVH zijn Afzonderlijke Verwerkingsverantwoordelijken voor de Persoonsgegevens die zij verstrekken aan de Procesregisseur ten behoeve van de Aanmelding en aan Partijen in het kader van Triage, de Regionale Casustafel en Afschaling.
- 2.2. Partijen in het ZVH zijn in overeenstemming met artikel 26 van de AVG Gezamenlijke 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 ZVH in het kader van de samenwerking voor de doeleinden zoals omschreven in artikel 3.
- 2.3. Verwerking van Persoonsgegevens in het ZVH door personeel van het ZVH 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 van de AVG.

## Artikel 3. Doel Verwerking Persoonsgegevens

- 3.1. Dit Privacy 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 ZVH 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 ZVH:
- 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, en;
  - b. het voorkomen van (verder) crimineel en/of overlast gevend gedrag of verder afglijden van die personen, en;
  - 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, Multidisciplinair overleg en Afschaling. Voor elk van deze fasen in het Werkproces zijn specifieke doelen voor de Verwerking van Persoonsgegevens in het ZVH 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 Privacy Protocol hebben verkregen niet voor andere doeleinden dan de doelen omschreven in artikel 3.2 en ook niet in het kader van nevenactiviteiten.
- 3.5. Bij het verwerken van Persoonsgegevens in het ZVH 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 eerst opnieuw beoordeeld of de eerder verwerkte gegevens ook daarvoor noodzakelijk zijn en vervolgens of de gegevens daarvoor ook (verder) gebruikt mogen worden;
  - c. de Partij 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. partijen die bij de behandeling van een Casus kennisnemen van Persoonsgegevens afkomstig van een andere Partij, mogen deze gegevens enkel verder gebruiken voor hun eigen taken in het kader van de casusbehandeling, als de Partij die de gegevens heeft ingebracht, dit afzonderlijk schriftelijk accordeert.

#### **Artikel 4. Categorieën Persoonsgegevens**

- 4.1. Partijen verwerken de genoemde categorieën Persoonsgegevens van de in Bijlage 4 benoemde 'categorieën Betrokkenen' die nodig zijn voor de samenwerking.

*Toelichting: Persoonsgegevens betreft informatie die direct of indirect herleidbaar is tot een natuurlijk persoon, zoals geformuleerd in artikel 1: Definities van dit Privacy Protocol. 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 ZVH, of in de door de Stuurgroep aangewezen informatiesystemen en in overeenstemming met het beveiligingsbeleid zoals opgenomen in Bijlage 3 bij dit Privacy Protocol.

*Toelichting: Door het Ministerie van Justitie en Veiligheid is voor onder andere overleggen in het ZVH het systeem GCOS ontwikkeld (Generiek Casusoverleg Onderhoud Systeem). Als GCOS door Partijen ook voor andere werkprocessen/ samenwerkingsverbanden wordt gebruikt dan het ZVH beschreven, 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 ZVH in GCOS. Daarnaast maakt het ZVH Twente gebruik van het cliënt-volgsysteem Vis2 en geldt hiervoor hetzelfde.*

## **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 11 en 12 van het Convenant valt.
- 5.1.3 Voor de Verwerking van Persoonsgegevens als bedoeld in artikel 5.1.1 zijn van toepassing de grondslag in overeenstemming met 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 Privacy Protocol.

### **5.2 Verstrekken van Persoonsgegevens ten behoeve van Aanmelding, Triage en Regionale Casustafel en Multidisciplinair overleg**

- 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 in overeenstemming met 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 Privacy Protocol.

### **5.3 Verstrekken van gegevens bij het uitvoering geven aan afspraken uit de Regionale Casustafel en Multidisciplinair overleg**

- 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 aanbrenge van de Casus bij een andere overlegtafel.
- 5.3.2 De grondslag in overeenstemming met 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 van dit Privacy Protocol.

### **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 van de AVG lid 1 sub e, voor zover deze noodzakelijk zijn voor de uitvoering van taken van algemeen belang door de aanmeldende Partij, dan wel de Partij onder wiens verantwoordelijkheid de Casusregisseur valt. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wpg (verstrekking aan derden structureel voor samenwerkingsverbanden). Voor gegevens afkomstig van het OM, 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 Partij, dan wel de Partij onder wiens verantwoordelijkheid de Casusregisseur valt, en/of de verstreckende Partij. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wpg. 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 verstreckende partij. Voor de gegevens afkomstig

van de politie is de grondslag gelegen in artikel 20 Wpg. 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 een Casus slechts van toepassing zijn als dit voortvloeit uit de goede uitvoering van de taken en werkzaamheden van Partijen en de Verwerking plaatsvindt namens of de verstrekking plaatsvindt aan één van de hieronder genoemde Partijen en voorwaarden.
- a. **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 artikel 172 van de Gemeentewet.
  - b. **Bestuursorgaan het college van burgemeester en wethouders (hierna '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 Wet Maatschappelijke Ondersteuning (hierna 'Wmo') artikel 2.3.1 t/m 2.3.5, artikel 2.3 en 2.4 van de Jeugdwet, artikel 7.1 van de Participatiewet en artikel 3 van de Wet schuldhulpverlening.
  - c. **OM:** voor de strafrechtelijke handhaving van de rechtsorde alsmede andere bij de wet vastgestelde taken (artikel 124 Wet op de rechterlijke organisatie (hierna 'Wro'). De grondslag voor het verstrekken van Justitiële, Strafvorderlijke of Tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.
  - d. **Politie:** vervulling van taken zoals bedoeld in artikel 3 Politiewet, 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 in overeenstemming met artikel 8 en 13, Politiegegevens worden verstrekt. De artikel 20 Wpg-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 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 (hierna 'BW'), waaronder artikel 1:240 BW, artikel 1:255 juncto 1:257 BW, artikel 77o en 77hh van het Wetboek van Strafrecht, artikel 126 nd en 491 van het Wetboek van Strafvordering alsmede artikel 28 van het Besluit Tenuitvoerlegging Jeugdstrafrecht BES, de Algemene Wet Bestuursrecht (hierna 'Awb'), artikel 2.4, 3.1, 3.2 en 7.3.11 lid 4 van de Jeugdwet en artikel 4 onder c, lid 1 van de Wet opnemings buitenlandse kinderen ter adoptie (hierna 'Wobka'). Met inachtneming van het Kwaliteitskader 2021 van de Raad voor de Kinderbescherming.
  - f. **Veilig Thuis:** de goede uitvoering van de taken van het Advies- en meldpunt Huiselijk geweld en kindermishandeling (AMHK), waaronder in het bijzonder taken zoals bedoeld in artikel 4.1.1 van de Wmo, met inachtneming van het Privacy Protocol Veilig Thuis.
  - g. **Reclasseringsinstelling:** de goede uitvoering van taken van de reclasseringsinstelling, waaronder in het bijzonder taken zoals bedoeld in artikel 8 lid 1 van de Reclasseringsregeling 1995.
  - h. **Gecertificeerde instelling zoals bedoeld in artikel 1.1 van de Jeugdwet:** de goede uitvoering van kinderschermingsmaatregelen en jeugdreclassering zoals bedoeld in artikel 1.1. van de Jeugdwet.
  - i. **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, de Wet verplichte ggz of Wet zorg en dwang.
- j. **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. **GGD:** de uitvoering van de taken in het kader van de Openbare Geestelijke Gezondheidszorg (OGGZ-taken) op grond van artikel 1.2.1. sub a van de Wmo.
  - l. **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 de Wet Forensische zorg. De wettelijke grondslag voor de Verwerking en verstrekking van Persoonsgegevens is, na inwerkingtreding van de wijziging van de 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 van de Wet Justitie subsidies in samenhang met artikel I van de Regeling Aanwijzing rechtspersoon slachtofferhulp, en artikel 51aa Wetboek van Strafvordering in samenhang met artikel 1 onder e en artikel 3 van het Besluit slachtoffers van strafbare feiten. De wettelijke grondslag voor de Gegevensverwerking is mede gelegen in artikel 9 en/of artikel 10 AVG in samenhang met artikel 30 lid 3 onder a en lid 4 en artikel 33 lid 1 onder a Uitvoeringswet AVG. 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 artikel 1.1.1. van de Wmo, een zorgaanbieder zoals bedoeld in artikel 1.1.1. van de Wet langdurige zorg, dan wel een jeugdhulpaanbieder zoals bedoeld in artikel 1.1. van de Jeugdwet:** 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 hierboven in artikel 6.4 benoemde Partijen, hoofdstuk 3 van het Handvat.*

*Hieronder nogmaals de link naar het Handvat om (online) snel te raadplegen:*

<https://vng.nl/sites/default/files/2020-08/handvat-gegevensuitwisseling-zvh-versie-2.2.pdf>

*Partijen dienen ieder voor zich vast te stellen op grond van welke wettelijke grondslag zij Persoonsgegevens in het kader van de samenwerking van het ZVH 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 Privacy Protocol zijn voor een groot deel van de vaste Partijen in het ZVH, de taken benoemd die aan de orde zijn. Het Handvat voorziet in nadere invulling hiervan.*

*Publieke instellingen dienen de Verwerking van Persoonsgegevens in het ZVH voor de in artikel 3 genoemde doeleinden een grondslag in de wet te kunnen aanwijzen (artikel 6, lid 1 onder e, van de AVG). Private partijen dienen te onderzoeken of zij (uitdrukkelijke) toestemming kunnen krijgen voor de Verwerking (artikel 6, lid 1 onder a, van de 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, van de AVG).*

## **Artikel 7. Doorverwerking geheimhoudingsbepalingen en toepassing toestemmingsvereiste**

- 7.1 De geheimhoudingsbepaling van artikel 7 Wpg blijft 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 (hierna 'Bpg'), voor een ander doel Politiegegevens zijn verstrekt aan één van de Partijen, dan worden deze gegevens door de desbetreffende ontvanger in principe niet als Persoonsgegevens verstrekt aan de Procesregisseur van het ZVH. Bij voorkeur worden door de politie op grond van artikel 20 Wpg opnieuw actuele Politiegegevens verstrekt aan de Procesregisseur van het ZVH 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 doorversterking aan de Procesregisseur van het ZVH, 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 van de Wet op de beroepen in de individuele gezondheidszorg (hierna 'Wet BIG'), artikel J van de beroepscode van de Jeugdzorgwerker, artikel 71 t/m 87 van de beroepscode NIP (psycholoog), of artikel 8 van de beroepscode NVO (pedagoog) en artikel 37 van de Reclasseringsregeling 1995, dan:
- wordt deze gevraagd op het moment dat duidelijk is dat het inbrengen of verstrekken noodzakelijk is ten behoeve van de in de betreffende fase aan de orde zijnde doelen, of de uitvoering van de in artikel 5.3.1 a t/m c van dit Privacy Protocol genoemde activiteiten;
  - worden deze Persoonsgegevens uitsluitend verstrekt voor zover hiervoor de uitdrukkelijke toestemming is verkregen van de Betrokkene of diens wettelijke vertegenwoordiger;
  - legt de Partij die de toestemming heeft verkregen deze schriftelijk vast en informeert Betrokkene dat hij zijn toestemming altijd weer kan intrekken;
  - draagt de Partij die toestemming heeft verkregen bij intrekking van die toestemming er zorg voor dat er geen verdere verstrekkingen meer plaats vinden;
  - maakt de betrokken zorg- of hulpverlener een eigen afweging conform de voor hem geldende professionele standaarden als 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. Als Partijen daartoe verplicht zijn door voor hen geldende materiewetgeving, dan leggen zij de afzonderlijke Verstrekkingen van Persoonsgegevens vast, inclusief onderbouwing van de noodzakelijkheid daarvan met het oog op de in artikel 5 en 6 vastgelegde grondslagen. Dit geldt ten minste voor politie en OM. De politie documenteert iedere verstrekking in overeenstemming met de documentatieplicht van artikel 32 Wpg, het OM in overeenstemming met 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 OM 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 vier jaar vastgelegd te zijn. Binnen het parket dienen goede afspraken gemaakt te worden met de privacyfunctionaris 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 Privacy 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 Privacy 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 ZVH 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 Multidisciplinair overleg 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. Als wordt besloten dat behandeling van de Casus in het ZVH niet of niet langer noodzakelijk is, worden de betreffende Persoonsgegevens niet langer in het ZVH verwerkt. De Procesregisseur ziet erop toe dat Persoonsgegevens in overeenstemming met artikel 11 worden geanonimiseerd of onomkeerbaar vernietigd. Dit geldt eveneens voor de Partijen die de betreffende Persoonsgegevens hebben ontvangen.
- 9.6 Wanneer de Partij die Persoonsgegevens in het ZVH 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 ZVH en bij de betrokken Partijen.
- 9.7 Enkel de Procesregisseur, de Informatiecoördinator, de Casusregisseur, de Ondersteuner Casustafels en de voor het Regionale Casustafel uitgenodigde Partijen hebben toegang tot de

Persoonsgegevens die worden verwerkt op locatie of in het informatiesysteem van het ZVH en enkel voor zover noodzakelijk voor hun rol in een specifieke Casus.

### **Artikel 10. Kwaliteit**

10.1 Partijen zorgen ervoor 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 ZVH 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 als:
- a. gegevens die noodzakelijk zijn voor de uitvoering van de werkzaamheden in het vervolg van de Casus overgedragen zijn aan de betreffende Partij. Eventueel met toestemming van de Partij die de gegevens heeft ingebracht;
  - b. afschalingsfase 1 in werking treedt: het dossier blijft actief in GCOS en/of Vis2 voor het geval terugval optreedt (maximaal zes maanden), met alleen toegang voor de bij de Casus betrokken Partijen;
  - c. afschalingsfase 2 in werking treedt: zes maanden na besluit tot Afschaling, waarbij alleen de aanmelder en Procesregisseur achterblijven in GCOS en/of Vis2, met alleen toegang voor de Informatiecoördinator;
  - d. afschalingsfase 3 in werking treedt: na één jaar na besluit tot Afschaling. Het volledige dossier, inclusief administratieve gegevens, wordt door de Informatiecoördinator vernietigd.
- 11.3 Na één jaar kunnen gegevens, niet zijnde Persoonsgegevens, enkel worden bewaard voor managementdoeleinden.
- 11.4 De manager van het ZVH 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, in overeenstemming met de geldende beveiligingsnormen voor de betreffende gegevens.
- 12.3 De Regio Twente draagt zorg voor de adequate beveiliging van Persoonsgegevens die worden verwerkt op locatie en in de informatiesystemen van het ZVH en rapporteren hierover indien nodig aan de Stuurgroep.
- 12.4 De Manager van het ZVH 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 ZVH en rapporteert hierover aan de Regio Twente en is bevoegd aanwijzingen te geven aan Partijen over de juiste omgang met Persoonsgegevens in dat verband.



### Artikel 13. Geheimhouding

- 13.1. Een ieder die op grond van dit Privacy Protocol kennis neemt van Persoonsgegevens is verplicht tot geheimhouding daarvan, tenzij de wet tot bekendmaking verplicht. De Manager, Procesregisseurs en eventueel ander ondersteunend personeel van het ZVH, 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 Privacy Protocol in aanraking komt met Persoonsgegevens geheimhouding van die gegevens waarborgt.
- 13.3. Alle medewerkers van het ZVH, inclusief medewerkers op basis van een dienstverleningsovereenkomst, deelnemers aan Regionale Casustafels en Multidisciplinaire overleggen en overige afgevaardigden van Partijen die toegang hebben tot Persoonsgegevens die onder dit Privacy Protocol worden verwerkt, beschikken over een Verklaring Omtrent Gedrag (hierna 'VOG'), of hebben een veiligheidsonderzoek doorlopen op grond van de voor de eigen organisatie geldende wet- en regelgeving.
- 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 ZVH ontvangt.
- 13.5. De Partijen in het samenwerkingsverband mogen de Persoonsgegevens afkomstig van de politie en OM 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 als 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 WGBO (artikel 7:457 BW), Reclasseringsregeling 1995, Jeugdwet of Wmo 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 verstrekende Partij en als 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 verstrekende Partij dit aan de ontvangende Partij weten, waarbij ook de toestemming voor Verwerking en verder Verwerking voor de ontvangende Partij vervalst.

*Toelichting: Het opzettelijk schenden van de geheimhoudingsplicht is strafbaar gesteld in artikel 272 Wetboek van strafrecht.*

## Artikel 14. Datalekken

- 14.1. Partijen houden procedures in stand die erop 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 regio Twente 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 ZVH. De Manager ziet toe op de naleving van deze procedures in het ZVH.
- 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 I van de AVG dan wel artikel 26g Wvsg, die een risico inhoudt voor de rechten en vrijheden van Betrokkenen zoals bedoeld in artikel 34 van de 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 via het Expertgroepoverleg 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 (hierna 'AP'). De Manager stuurt een afschrift van de melding aan de AP 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 van de AVG, wordt de Betrokkene door de verantwoordelijke Partijen over de inbreuk schriftelijk geïnformeerd. De beslissing tot melding aan de Betrokkene, wordt samen met de betrokken Partijen genomen. De inhoud van die melding wordt in het Expertgroepoverleg afgestemd, dan wel door het Expertgroepoverleg 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 AP naar aanleiding van de schriftelijke inbreuk-melding.
- 14.8. Kennisgeving van de inbreuk aan de AP door de Partijen gebeurt zonder onredelijke vertraging, maar in ieder geval binnen 72 uur na ontdekking en geschiedt volgens de daartoe door de AP ter beschikking gestelde procedure. De kennisgeving aan de AP omvat ten minste:
  - 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 als:
- passende technische en organisatorische maatregelen zijn genomen die de bescherming van Persoonsgegevens ook na de inbreuk garanderen;
  - achteraf genomen maatregelen de waarschijnlijkheid op een hoog privacy risico hebben weggenomen, of;
  - 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, als de inbreuk enkel ziet op gegevens afkomstig van het OM, en indien dit noodzakelijk en evenredig is:
- ter vermijding van belemmering van gerechtelijke onderzoeken of procedures;
  - ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
  - ter bescherming van de openbare veiligheid;
  - ter bescherming van de rechten en vrijheden van derden;
  - 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 over de aard van de inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen, en ook de tekst van de kennisgeving aan de Betrokkene. De Manager van het ZVH houdt een overzicht bij van gelijksoortige inbreuken die plaatsvinden op locatie of in de informatiesystemen van het ZVH.

#### **Artikel 15. Data Protection Impact Analyse (hierna 'DPIA')**

- 15.1. Er wordt aangaande Verwerkingen onder dit Privacy Protocol, of bij wijzigingen van de Verwerkingen, gedurende het eerste jaar van dit Privacy Protocol, door Partijen middels het Expertgroepoverleg een gegevensbeschermingseffectbeoordeling uitgevoerd conform artikel 35 van de 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 of wordt het model gegevensbeschermingseffectbeoordeling van de regio Twente gevolgd.
- 15.3. Bij een voornemen over 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 Expertgroepoverleg over de voorgenomen nieuwe Verwerking zoals bedoeld in artikel 15.1. van dit Privacy Protocol. De Stuurgroep legt waar nodig op grond van artikel 36 van de AVG namens alle gezamenlijke Verwerkingsverantwoordelijken, de beoogde Verwerking voor aan de AP.

#### **Artikel 16. Informatieverstrekking aan Betrokkene**

- 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 ZVH onder dit Privacy 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 zorgt voor het publiceren van een privacy statement op de website van het ZVH.
- 16.4. Alle deelnemende Partijen zorgen via hun eigen website voor vermelding van deelname aan het ZVH en voor een verwijzing naar de website van het ZVH Twente alsook voor verwijzing naar het Convenant en het Privacy Protocol.
- 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 ZVH zoals beschreven in artikel 3.2;
  - b. de Partijen die deelnemen aan de samenwerking in het ZVH;
  - 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. als 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 Privacy Protocol bij het ZVH en bij de AP;
  - g. nadere uitleg als 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 ZVH 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 als 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 ZVH worden gecoördineerd door de Procesregisseur. De Procesregisseur wordt hierbij ondersteund door een administratief medewerker. De Manager legt het verzoek voor aan het Expertgroepoverleg 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 één der Partijen, wordt de Manager hierover zo spoedig mogelijk door die Partij in kennis gesteld, opdat deze de beantwoording van het verzoek in overeenstemming met artikel 17.2 kan coördineren. Beantwoording van het verzoek door de Partij wordt in het Expertgroepoverleg 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, en ook 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 op grond van artikel 8 van dit Privacy Protocol en artikel 39j Wjsg schriftelijk vastgelegd en bewaard voor de duur van vier jaar. Inzage- en rectificatieverzoeken worden beoordeeld door de privacyfunctionaris van het verstreckende parket van het OM. 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 daarom zijn artikel 18, 19 en 20 van dit Privacy 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, in overeenstemming met 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 ZVH 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 lid 1 en 4 van de 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, als 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 ZVH 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. Als 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 ZVH, legt de Manager dit verzoek voor aan het Expertgroepoverleg met het oog op de beoordeling van het verzoek.
- 19.2. Onjuiste Persoonsgegevens over de Betrokkene worden op diens verzoek onverwijld gecorrigeerd.
- 19.3. Persoonsgegevens over 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 over zijn/haar verzoek tot correctie of verwijdering van zijn of haar Persoonsgegevens schriftelijk en gemotiveerd zo spoedig mogelijk, maar uiterlijk binnen vier 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 21 van de AVG.
- 20.2. Als 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 Expertgroepoverleg 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 vier weken en draagt er zorg voor dat de beslissing binnen deze vier weken wordt uitgevoerd.

Een beslissing om niet, of niet geheel, te voldoen wordt altijd gemotiveerd en kan met het oog op artikel 21 van de 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 ZVH. Persoonsgegevens kunnen dus niet makkelijk worden overgedragen aan een andere Partij in het ZVH.

### **Artikel 22. Verwerkers**

- 22.1. Partijen besteden de Verwerking van Persoonsgegevens onder dit Privacy Protocol niet uit zonder dat de Stuurgroep tevoren schriftelijk toestemming heeft gegeven over een beoogde verandering inzake de inzet van verwerkers die ten behoeve van het ZVH Persoonsgegevens verwerken.
- 22.2. Een overeenkomst van opdracht tussen Partijen en een door Stuurgroep goedgekeurde verwerker over Verwerking van Persoonsgegevens dient ten minste hetzelfde beschermingsniveau te bieden aan de belangen van Betrokkene als het onderhavige Privacy Protocol. Meer in het bijzonder moet de verwerker voor de Verwerkingen van Persoonsgegevens in het kader van dit Privacy Protocol een vergelijkbaar niveau van beveiliging garanderen als in Bijlage 3 van dit Privacy Protocol.
- 22.3. Partijen leggen de afspraken tussen hen en verwerker(s) over 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 Privacy Protocol worden verwerkt, worden niet verstrekt aan anderen dan deelnemers aan het Regionale Casustafel of Multidisciplinaire overleg, behoudens het bepaalde in artikel 19 en tenzij Partijen hiertoe wettelijk verplicht zijn. Deze verstrekking wordt schriftelijk vastgelegd door de Procesregisseur.
- 23.2. Als 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 Privacy Protocol in een eigen register van Verwerkingsactiviteiten.
- 24.2. Aanvullend neemt Procesregisseur de Verwerkingen van Persoonsgegevens op locatie en in de informatiesystemen van het ZVH op in een gezamenlijk register van Verwerkingsactiviteiten onder dit Privacy 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 ZVH 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 ZVH 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 Privacy 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 Privacy Protocol en zullen zich houden aan de in dit Privacy Protocol gemaakte afspraken.
- 25.2. Partijen zijn ieder voor zich aansprakelijk voor aanspraken van Betrokkenen, of Derden voor 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 Privacy 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 een evenredig deel van de gehele schade aansprakelijk gehouden om 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 AVG of buiten, dan wel in strijd met, de rechtmatige instructies van de Verwerkingsverantwoordelijke is gehandeld.
- 25.5. Onverminderd het gestelde in lid 3 kan iedere Verwerkingsverantwoordelijke of verwerker die de volledige vergoeding heeft betaald vervolgens bij de andere Verwerkingsverantwoordelijken of verwerkers die bij dezelfde Verwerking betrokken zijn, 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 als 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 Privacy Protocol en zijn bevoegd aanwijzingen te geven aan medewerkers in het ZVH over de uitvoering van het bepaalde in dit Privacy Protocol.



## **Artikel 27. Wijzigingen**

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

## **Artikel 28. Toetreding**

- 28.1. Toetreding door andere organisaties tot dit Privacy Protocol kan enkel wanneer die Partij is toegetreden in overeenstemming met artikel 20 van het Convenant.
- 28.2. Partijen worden vooraf door de secretaris van de Stuurgroep op de hoogte gebracht van de voorgenomen toetreding. Als 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 volgens hoofdstuk 5 van het Handvat. De toetredende Partij voert waar nodig de aanbeveling uit die analyse uit, alvorens uitwisseling van Persoonsgegevens in het ZVH met die partij plaatsvindt.
- 28.3. In geval van toetreding tot het Convenant, vindt toetreding tot het Privacy Protocol plaats door middel van ondertekening van Bijlage 1 bij dit Privacy Protocol door die andere organisatie en de voorzitter van de Stuurgroep.

## **Artikel 29. Duur, opzegging, beëindiging**

- 29.1. Dit Privacy Protocol treedt in werking op de dag van ondertekening door Partijen en wordt voor dezelfde duur als het Convenant aangegaan. In geval van verlenging van het Convenant wordt dit Privacy 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 ZVH, als de afspraken zoals neergelegd in dit Privacy 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 Privacy Protocol bestaan. Tot deze verplichtingen behoren onder meer die ter zake van geheimhouding en de beveiliging van Persoonsgegevens.

## **Artikel 30. Opvolging**

- 30.1. Dit Privacy Protocol vervangt alle eerdere door Partijen gesloten Privacy Protocollen met betrekking tot de Verwerking van Persoonsgegevens in het ZVH voor de doelen zoals beschreven in artikel 3.2 van dit Privacy 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 Privacy 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 Privacy Protocol is Nederlands recht van toepassing.
- 32.2. Geschillen over dit Privacy Protocol zullen in eerste instantie zoveel mogelijk in gezamenlijk overleg worden opgelost.

## Aldus overeengekomen,

Partijen hebben kennisgenomen van artikel 1 tot en met 32 en de Bijlagen 1 tot en met 4 van dit Privacy Protocol en tekenen voor akkoord,

<b>Gemeente Almelo</b>
In dezen rechtsgeldig vertegenwoordig door burgemeester A.J. Gerritsen
Datum en plaats:

<b>Gemeente Borne</b>
In dezen rechtsgeldig vertegenwoordig door burgemeester J.H.R. Pierik
Datum en plaats:

<b>Gemeente Dinkelland</b>
In dezen rechtsgeldig vertegenwoordig door burgemeester J. Joosten
Datum en plaats:

<b>Gemeente Enschede</b>
In dezen rechtsgeldig vertegenwoordig door burgemeester R.W. Bleker
Datum en plaats:

<b>Gemeente Haaksbergen</b>
In dezen rechtsgeldig vertegenwoordig door burgemeester R.G. Welten
Datum en plaats:

<b>Gemeente Hellendoorn</b>
In dezen rechtsgeldig vertegenwoordig door burgemeester J.J. Eijbersen
Datum en plaats:

<b>Gemeente Hengelo</b>
In dezen rechtsgeldig vertegenwoordig door burgemeester S.W.J.G. Schelberg
Datum en plaats:

<b>Gemeente Hof van Twente</b>
In dezen rechtsgeldig vertegenwoordig door burgemeester H.A.M. Nauta- van Moorsel
Datum en plaats:

<b>Gemeente Losser</b>
In dezen rechtsgeldig vertegenwoordig door waarnemend burgemeester G.J. Kok
Datum en plaats:

<b>Gemeente Oldenzaal</b>
In dezen rechtsgeldig vertegenwoordig door burgemeester P.G. Welman
Datum en plaats:

<b>Gemeente Rijssen-Holten</b>
In dezen rechtsgeldig vertegenwoordig door burgemeester A.C. Hofland
Datum en plaats:

<b>Gemeente Tubbergen</b>
In dezen rechtsgeldig vertegenwoordig door burgemeester W. Haverkamp
Datum en plaats:

**Gemeente Twenterand**

In dezen rechtsgeldig vertegenwoordig door burgemeester J.C.F. Broekhuizen

Datum en plaats:

**Gemeente Wierden**

In dezen rechtsgeldig vertegenwoordig door D.J. Tichelaar- van Oene

Datum en plaats:

**Dienst Justitiële Inrichtingen, Oost Nederland**

In dezen rechtsgeldig vertegenwoordig door: Ton Golstein, Vestigingsdirecteur PI Almelo

Datum en plaats:

**GGD Twente**

In dezen rechtsgeldig vertegenwoordig door: Samantha Dinsbach, Directeur Publieke  
Gezondheid

Datum en plaats:

**Humanitas onderdak Twente**

In dezen rechtsgeldig vertegenwoordig door: Bert Deliën, Directeur/Bestuurder

Datum en plaats:

**Jeugdbescherming Overijssel**

In dezen rechtsgeldig vertegenwoordig door: Ruud Brinkman, Bestuurder

Datum en plaats:

**Leger des Heils Jeugdbescherming en Reclassering**

In dezen rechtsgeldig vertegenwoordig door: Kees van Harten, Regiomanager

Datum en plaats:

**Mediant**

In dezen rechtsgeldig vertegenwoordig door: Lia Verlinde, Geneesheer-Directeur

Datum en plaats:

**Openbaar Ministerie Arrondissementsparket Oost-Nederland**

In dezen rechtsgeldig vertegenwoordig door: Marthyne Kunst, Hoofdofficier Parket Oost Nederland

Datum en plaats:

**Politie Regionale Eenheid Oost-Nederland**

In dezen rechtsgeldig vertegenwoordig door: Karlijn Baalman, Districtchef

Datum en plaats:

**Raad voor de Kinderbescherming**

In dezen rechtsgeldig vertegenwoordig door: Helean Weurding, Gebiedsmanager

Datum en plaats:

**Reclassering Nederland**

In dezen rechtsgeldig vertegenwoordig door: Maarten Vuylsteke, Regiodirecteur Oost Nederland

Datum en plaats:



<b>Stichting Dimence</b>
In dezen rechtsgeldig vertegenwoordig door: Margriet Wiedemeyer, Directeur Bedrijfsvoering
Datum en plaats:

<b>Stichting Maatschappelijke dienstverlening Enschede-Haaksbergen</b>
In dezen rechtsgeldig vertegenwoordig door: Willem Loupatty, Directeur-Bestuurder
Datum en plaats:

<b>Stichting Tactus Sociale Verslavingszorg</b>
In dezen rechtsgeldig vertegenwoordig door: Michele Ruyten, Divisiemanager Oost
Datum en plaats:

<b>Stichting Tactus Verslavingsreclassering</b>
In dezen rechtsgeldig vertegenwoordig door: Ellen Schleedoorn, Regiomanager Reclassering
Datum en plaats:

**Stichting Transfore**

In dezen rechtsgeldig vertegenwoordig door: Directie, Tinie Hendriks en Inge Korfage

Datum en plaats:

**Veilig Thuis Twente**

In dezen rechtsgeldig vertegenwoordig door: Marjolein van Zon, Manager VTT

Datum en plaats:

## Bijlage 1: Toetredingsformulier nieuwe Partij tot Privacy Protocol

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

overwegende dat:

- Deelname aan het Privacy 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 Privacy Protocol;
- De Stuurgroep positief heeft besloten op toetreding van ondergetekende aan het Convenant en dit Privacy Protocol;

verklaart daartoe het volgende:

- Ondergetekende onderschrijft de in het Privacy Protocol geformuleerde doelstellingen, verplicht zich de bepalingen in het Privacy 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:

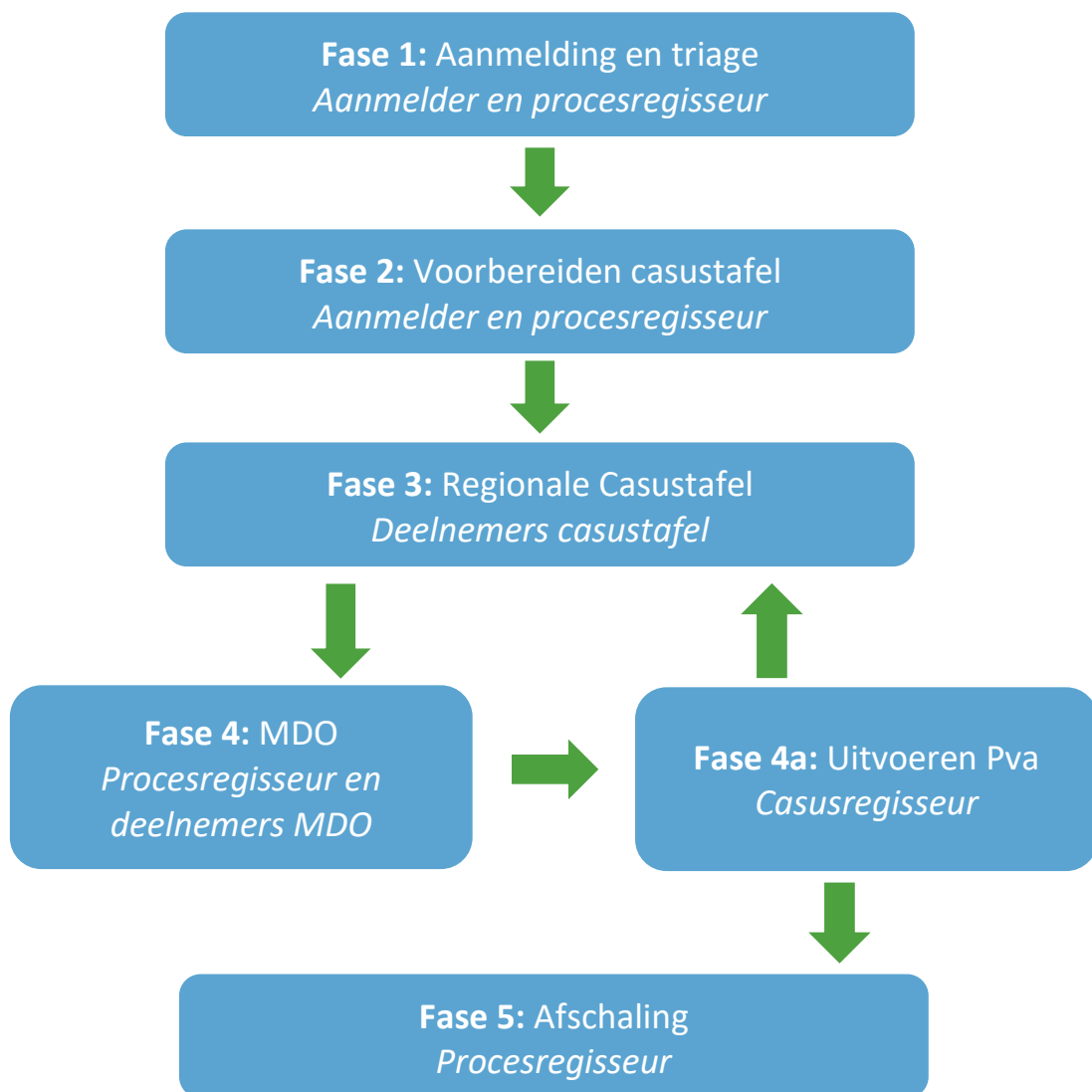
Naam:

## Bijlage 2: Werkproces ZVH

Partijen Verwerken in het kader van het ZVH 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 overlastgevend casuïstiek met veiligheidsrisico);
- c. risicojongeren;
- d. complexe GGZ met veiligheidsrisico;
- e. polarisatie en extremisme;
- f. mensenhandel.



## Toelichting werkproces ZVH Twente

Het algemene Werkproces op gebied van complexe domein-overstijgende 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:

In deze fase brengt één van de Partijen een cliënt aan bij de Procesregisseur van het ZVH. De Procesregisseur stemt deze aanmelding af met in ieder geval de betrokken Gemeente en vult samen met andere Partijen het beeld aan. Gezamenlijk wordt bepaald waar de Casus thuishoort en op welke casustafel de Casus wordt besproken. De Procesregisseur legt de Casus vast in GCOS en/of Vis2. Er vinden in deze fase nog geen verstrekkingen plaats aan andere Partijen in het ZVH. De gegevens blijven de verantwoordelijkheid van de aanbrengrer.

Doel: Registreren en verrijken bekende informatie  
Belangrijkste betrokkenen: Aanmeldende Partij en Procesregisseur

### Fase 2 Voorbereiden Casustafel:

De administratief medewerker of Ondersteuner Casustafels stelt, in overleg met de Procesregisseurs, de agenda voor de Regionale Casustafels op en nodigt de benodigde Partijen uit. Ook worden eventuele Betrokkene(n) geïnformeerd als dat nodig is. Dit wordt vastgelegd in GCOS en/of Vis2.

Doel: Voorbereiden casustafel, uitnodigen Partijen en eventueel informeren Betrokkene(n)  
Belangrijkste betrokkenen: Administratief medewerker, Ondersteuning Casustafels en Procesregisseurs

### Fase 3 Regionale Casustafel:

Tijdens de Regionale 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 ZVH
- Procesregie ZVH
- Inrichting Stelselmatige Daders (ISD)

Doel: Richting Casus bepalen, Procesregisseur aanwijzen en monitoren  
Belangrijkste betrokkenen: Procesregisseur (voorzitter), deelnemers casustafel, administratief medewerker Ondersteuning Casustafels

### Fase 4 Multi Disciplinair Overleg (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  
Belangrijkste betrokkenen: Procesregisseur (voorzitter), deelnemers MDO



## 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 in overeenstemming met 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.
- **Logbestanden 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 onrecht matige 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 vervolgpcedure 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. 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 Persoonsgegevens 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 beveiligingsmaatregelen 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, en ook 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 ‘logbestanden 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 over iemands gezondheid, verwijst de Autoriteit Persoonsgegevens ook naar de NEN7510.

De fysieke documenten over het beveiligingsbeleid Persoonsgegevens van de Beheerorganisatie Veiligheidsregio Twente en de regio Twente die zijn op te vragen bij de Veiligheidsregio Twente en de regio Twente.

## Bijlage 4: Categorieën Persoonsgegevens en Betrokkenen

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

### **Categorie 1: Categorie Betrokkenen:**

Van Personen, op wie het onder dit Privacy 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 Wpg);
- 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 van de 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 ZVH;
- contactgegevens (zakelijk telefoonnummer, e-mailadres);