

Privacy Protocol

Integrale Veiligheid en Complexe Multi-Problematiek Veiligheidshuis Midden-Limburg

Context:

Met dit Privacy Protocol worden afspraken rondom de uitwisseling en het verder gebruik van persoonsgegevens door en tussen verschillende partijen in het Veiligheidshuis Midden-Limburg geformaliseerd en vastgelegd. Uit dit Privacy Protocol blijkt met welk doel persoonsgegevens worden verwerkt, wie voor welke acties met betrekking tot persoonsgegevens verantwoordelijk is, wanneer 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.

Formuleringen, begrippen en andere specifieke Veiligheidshuis-gerelateerde termen zijn afgeleid uit het Handvat “Gegevensuitwisseling in het zorg- en veiligheidsdomein – een juridisch handvat voor zorg- en veiligheidshuizen”, versie 1.1. van juli 2017 en het Landelijk Kader Veiligheidshuizen. Ook wordt aangesloten bij de werkwijze zoals in het Handvat beschreven.

Dit Privacy Protocol en de daarin gehanteerde terminologie is gebaseerd op de Algemene Verordening Gegevensbescherming, alsook de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens.

Privacy Protocol tussen ketenpartners Veiligheidshuis Midden-Limburg

De ondergetekenden:

De colleges van burgemeester en wethouders en de burgemeesters, ieder voor zover het zijn bevoegdheid betreft, van de gemeenten:

Gemeente Echt-Susteren;
Gemeente Leudal;
Gemeente Maasgouw;
Gemeente Nederweert;
Gemeente Roerdalen;
Gemeente Roermond;
Gemeente Weert,

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

en

de Politie Eenheid Limburg, hierbij rechtsgeldig vertegenwoordigd door Sectorhoofd District Noord en Midden Limburg, Compagniescommandant Bewakingseenheid NL;

het Openbaar Ministerie arrondissementsparket Limburg, hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

Raad voor de Kinderbescherming, gevestigd te [plaats] en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

3RO (3 Reclasseringsorganisaties), gevestigd te [plaats] en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

Bureau Jeugdzorg Limburg, gevestigd te [plaats] en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

Algemeen Maatschappelijk Werk Midden-Limburg, gevestigd te [plaats] en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

Veilig Thuis, gevestigd te [plaats] en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

Centrum voor Jeugd en Gezin Midden-Limburg, gevestigd te [plaats] en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

MEE Noord- en Midden Limburg, gevestigd te [plaats] en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

Penitentiare Inrichting Zuid Oost, gevestigd te [plaats] en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

Penitentiare Inrichting Sittard, gevestigd te [plaats] en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

GGZ-instelling Vincent van Gogh, gevestigd te [plaats] en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

Met GGZ, gevestigd te [plaats] en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

De Rooyse Wissel, gevestigd te Oostrum en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

Pedagogisch Sociaal Werk, gevestigd te [plaats] en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

Moveoo, gevestigd te Roermond en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

William Schrikker Groep, gevestigd te Amsterdam en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

Zelfregiecentrum, gevestigd te Weert en kantoorhoudend te [adres], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

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

de volgende overwegingen in aanmerking nemende:

- Partijen in het kader van samenwerking op het gebied van integrale veiligheid en complexe casuïstiek het Veiligheidshuis Midden-Limburg (hierna: 'het Veiligheidshuis') hebben opgezet;
- Partijen voor deze samenwerking afspraken hebben vastgelegd in het Convenant 'Samenwerking tussen ketenpartners in het Veiligheidshuis Midden-Limburg, gesloten op 30 april 2020' (verder: het Convenant), waar dit Privacy Protocol deel van uitmaakt;
- voor de samenwerking in het Veiligheidshuis de uitwisseling van gegevens, waaronder Persoonsgegevens, tussen de Partijen noodzakelijk is;
- in het door Partijen opgezette Veiligheidshuis Persoonsgegevens worden verwerkt ten dienste en onder verantwoordelijkheid van Partijen;
- Partijen slechts die Persoonsgegevens binnen het Veiligheidshuis delen die noodzakelijk zijn voor het doel van de samenwerking;
- op de samenwerking wet- en regelgeving met betrekking tot de bescherming van Persoonsgegevens van toepassing is waarbij Partijen conform deze wet- en regelgeving willen samenwerken;
- dit Privacy Protocol de gedragsregels omschrijft bij het verstrekken en verder Verwerken van Persoonsgegevens door Partijen in het kader van de samenwerking op het gebied van integrale veiligheid en complexe multi-problematiek, alsook de verschillende verantwoordelijkheden met het oog op de rechten en plichten uit toepasselijke privacy wet- en regelgeving, belegend;
- met dit Privacy Protocol reeds invulling wordt gegeven aan de in artikel 26 Algemene Verordening Gegevensbescherming neergelegde verplichting voor Partijen om op een transparante wijze hun samenwerkingsafspraken en hun verantwoordelijkheden jegens elkaar en jegens Betrokkene vast te leggen;
- dit Privacy Protocol aansluit bij het bepaalde in het 'Landelijk Kader Veiligheidshuizen' van het Ministerie van Veiligheid en Justitie, vastgesteld in januari 2013 (verder aangeduid als: 'het Landelijk Kader') en het 'Handvat Gegevensuitwisseling in het zorg en veiligheidsdomein – een juridisch handvat voor zorg- en veiligheidshuizen', versie 1.1. van juli 2017, (verder aangeduid als: 'het Handvat'), alsmede bij de in het Handvat en het Landelijk Kader gebezigde terminologie;
- dit Privacy Protocol verder wordt aangehaald als 'het Protocol'.

verklaren te zijn overeengekomen:

Artikel 1. Definities

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

- 1.1. 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 identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator 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 lid 1 AVG);
- 1.2. Politiegegevens: elk Persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt (artikel 1, sub a, Wpg);
- 1.3. Strafvorderlijke gegevens: Persoonsgegevens of gegevens over een rechtspersoon die zijn verkregen in het kader van een strafforderlijk onderzoek en die het openbaar ministerie in een strafdossier of langs geautomatiseerde weg verwerkt in een gegevensbestand (artikel 1 sub b Wjsg);
- 1.4. Justitiële gegevens: bij algemene maatregel van bestuur omschreven Persoonsgegevens of gegevens over een rechtspersoon inzake de toepassing van het strafrecht of de straffordering, die in een bestand worden Verwerkt (artikel 1 sub a Wjsg, respectievelijk Bjsjg);
- 1.5. Tenuitvoerleggingsgegevens: persoonsgegevens of gegevens over een rechtspersoon inzake de tenuitvoerlegging van strafrechtelijke beslissingen, die in een dossier of een ander gegevensbestand zijn of worden verwerkt;
- 1.6. Bijzondere Persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 AVG);
- 1.7. Strafrechtelijke persoonsgegevens: Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (zoals bedoeld in artikel 10 AVG);
- 1.8. Verwerken: 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, lid 2, AVG);
- 1.9. Betrokkene: de natuurlijke persoon op wie informatie, waaronder Persoonsgegevens, betrekking heeft (artikel 4, lid, 1 AVG);
- 1.10. Derde: een natuurlijk persoon of rechtspersoon, niet zijnde de betrokkene, noch één der Partijen;

- 1.11. Verwerkingsverantwoordelijke(n): een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze Verwerking in het Unierecht of het lidstatelijke recht is vastgesteld, kan daarin reeds zijn bepaald wie de Verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen (artikel 4 lid 7 AVG);
- 1.12. Afzonderlijke Verwerkingsverantwoordelijken: Partijen zijn Afzonderlijke Verwerkingsverantwoordelijke voor zelfstandige Verwerkingen en wanneer verschillende Verwerkingen min of meer geïntegreerd zijn, maar geen sprake is van Gezamenlijke Verwerkingsverantwoordelijken;
- 1.13. Gezamenlijke Verwerkingsverantwoordelijken: Van Gezamenlijke Verwerkingsverantwoordelijkheid is sprake wanneer Verwerkingen zijn geïntegreerd, en niet één Partij als Verwerkingsverantwoordelijke kan worden aangemerkt voor de geïntegreerde Verwerkingen. In dat geval zijn de Partijen Verwerkingsverantwoordelijken voor het geheel van de Verwerking;
- 1.14. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt (artikel 4, lid 8, AVG);
- 1.15. Casusregie: het uitvoeren van werkzaamheden gericht op het bewaren van de onderlinge samenhang bij het uitvoeren van het plan van aanpak bij het behandelen van één specifieke Casus;
- 1.16. Procesregie: het uitvoeren van werkzaamheden gericht op de totstandkoming van samenwerking tussen Partijen bij het behandelen van één specifieke Casus en de ondersteuning van de Casusregisseur bij de uitvoering van het plan van aanpak;
- 1.17. Casus: een geval of situatie dat of die voldoet aan de criteria voor complexe casuïstiek zoals geformuleerd in Bijlage 2 van het Convenant, en die is Aangemeld bij het Veiligheidshuis ter beoordeling en eventuele bespreking in het Ronde Tafel Overleg;
- 1.18. Aanmelding en screening: het voordragen van een Casus door één der Partijen en het uitwisselen van informatie, waaronder Persoonsgegevens, tussen de Procesregisseur van het Veiligheidshuis en de aanmeldende Partij ter toetsing of de Casus in aanmerking komt voor behandeling in het Veiligheidshuis;
- 1.19. Triage: het proces waarbij relevante Partijen worden bevestigd 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 eventueel Ronde Tafel Overleg, en tot een afweging welke Partijen relevant zijn om te betrekken bij een Ronde Tafel Overleg;
- 1.20. Ronde Tafel Overleg (RTO): fase waarin overleg plaatsvindt door Partijen gericht op de totstandkoming van een plan van aanpak, afstemming tijdens de uitvoering daarvan, en het beoordelen of Casus kan worden afgeschaald;
- 1.21. Afschaling: fase die volgt op het besluit in het Ronde Tafel Overleg dat de betrokkenheid van het Veiligheidshuis niet langer nodig is, waarin het dossier dat in het systeem van het Veiligheidshuis is aangelegd ten behoeve van procesregie, geschoond wordt van alle niet langer noodzakelijke informatie, en uiteindelijk verdwijnt uit het systeem van het Veiligheidshuis;
- 1.22. Procesregisseur: de medewerker van het zorg- veiligheidshuis die namens een van de Partijen is belast met de werkzaamheden in Artikel 9 van het Convenant;
- 1.23. Casusregisseur: de medewerker van een van de Partijen die is belast met de taken in Artikel 10 van het Convenant;

- 1.24. Manager: de persoon die is belast met de taken zoals geformuleerd in Artikel 8 van het Convenant;
- 1.25. Stuurgroep: het verband van afgevaardigden van Partijen zoals geformuleerd in Artikel 4 van het Convenant;
- 1.26. Voorbereidingsgroep stuurgroep vhhml (hierna: Voorbereidingsgroep stuurgroep): het verband van afgevaardigden van Partijen zoals geformuleerd in Artikel 5 van het Convenant;
- 1.27. Privacyadviseur: het Veiligheidshuis heeft een medewerker die belast is met privacyadvisering of kan gebruik maken van een privacyadviseur van de gemeente Roermond. Deze persoon is ook belast met beleidsontwikkeling over gegevensverwerking en helpt mee met de voorbereiding van audits;
- 1.28. Jaarplan: het door de Stuurgroep op grond van Artikel 4.1 van het Convenant vastgestelde plan betreffende de inhoudelijke koers van het Veiligheidshuis;
- 1.29. Werkproces: het door de Voorbereidingsgroep stuurgroep op grond van Artikel 5.6 van het Convenant vastgestelde proces(sen) voor samenwerking in het Veiligheidshuis, waaronder het proces omtrent en het delen van informatie en het Afschalen van een Casus;
- 1.30. AVG: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);
- 1.31. Wjsg: Wet justitiële en strafvorderlijke gegevens;
- 1.32. Bjsg: Besluit justitiële en strafvorderlijke gegevens;
- 1.33. Wpg: Wet politiegegevens;
- 1.34. Bpg: Besluit politiegegevens.

Artikel 2. Afzonderlijke en Gezamenlijke Verwerkingsverantwoordelijken

- 2.1. Partijen in het Veiligheidshuis zijn Afzonderlijke Verwerkingsverantwoordelijke voor de Persoonsgegevens die zij verstrekken aan de Procesregisseur ten behoeve van de Aanmelding en screening en aan Partijen in het kader van Triage, Ronde Tafel Overleg, en Afschaling.
- 2.2. Partijen in het Veiligheidshuis zijn conform artikel 26 Algemene Verordening Gegevensbescherming 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 Veiligheidshuis in het kader van de samenwerking voor de doeleinden zoals omschreven in artikel 3.
- 2.3. Verwerking van Persoonsgegevens in het Veiligheidshuis door personeel van het Veiligheidshuis geschiedt onder gezag van de Partij die de betreffende Persoonsgegevens heeft verstrekt. Deze Partij wordt voor die Verwerking aangeduid als Verwerkingsverantwoordelijke.

Artikel 3. Doel Verwerking Persoonsgegevens

- 3.1. Dit Protocol ziet op alle Verwerkingen van Persoonsgegevens door Partijen in het kader van de uitvoering van artikel 2 van het Convenant.
- 3.2. Het verwerken van Persoonsgegevens in het Veiligheidshuis vindt plaats met als doel het gezamenlijk door Partijen bijdragen aan de veiligheid als onderdeel van het integrale zorg- en veiligheidsbeleid van de Gemeenten. De samenwerking is meer specifiek gericht op het voorkomen en verminderen van recidive, (ernstige) overlast, criminaliteit en maatschappelijke uitval bij complexe problemen, door een combinatie van repressie, bestuurlijke interventie én zorg, hetgeen gezien moet worden als een zwaarwegend algemeen belang. Meer specifiek draagt de Verwerking van Persoonsgegevens in het Veiligheidshuis bij aan:
 - a. het oplossen van complexe multi-problematiek, problematiek waarbij personen die het subject zijn in de casuïstiek te maken hebben met meerdere problemen die op meer dan één leefgebied spelen;
 - b. het voorkomen van (verder) crimineel en/of overlast-gevend gedrag of verder afglijden van die personen;
 - c. het oplossen van ernstige lokale of gebiedsgebonden veiligheidsproblematiek; en
 - d. het mogelijk maken van samenwerking met het oog op de hierboven geformuleerde doeleinden.
- 3.3. Om het onder artikel 3.2 geformuleerde doel te bereiken Verwerken Partijen gezamenlijk de nodige Persoonsgegevens in het kader van Aanmelding en screening, Triage, Ronde Tafel Overleg, en Afschaling. Voor elk van deze fasen in het werkproces zijn specifieke doelen voor de Verwerking van Persoonsgegevens in het Veiligheidshuis van toepassing. Deze doelen zijn gespecificeerd in Bijlage 2.
- 3.4. Partijen Verwerken de Persoonsgegevens die zij in het kader van de samenwerking onder dit Protocol hebben verkregen niet voor andere doeleinden dan de doelen omschreven in artikel 3.2.
- 3.5. Bij het Verwerken van Persoonsgegevens in het Veiligheidshuis worden de volgende uitgangspunten in acht genomen:
 - a. Er is sprake van een strikte doelbinding per fase van de voor de te Verwerken Persoonsgegevens en alleen de voor het doel van die fase noodzakelijke persoonsgegevens worden verwerkt;
 - b. Als het doel van de Verwerking van Persoonsgegevens wijzigt, of, de casus gaat door naar een volgende fase, wordt als eerste opnieuw beoordeeld of de eerder verwerkte gegevens ook daarvoor noodzakelijk zijn en vervolgens of de gegevens daarvoor ook (verder) gebruikt mogen worden;
 - c. Een partner die in een bepaalde fase Persoonsgegevens verstrekt behoudt de zeggenschap over het verdere gebruik van die gegevens en of die voor een andere fase en/of andere doelen gebruikt mogen worden;
 - d. Partners die bij de behandeling van een casus kennisnemen van Persoonsgegevens afkomstig van een andere partner mogen deze gegevens enkel verder gebruiken voor hun eigen taken in het kader van de casusbehandeling, als de partner die de gegevens heeft ingebracht, dit afzonderlijk accordeert.

Artikel 4. Categorieën Persoonsgegevens

- 4.1. In het kader van de samenwerking worden door Partijen van de in Bijlage 4 categorieën Betrokkenen de daarin genoemde categorieën Persoonsgegevens Verwerkt.
- 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 Veiligheidshuis, of in de door de Stuurgroep aangewezen informatiesystemen en conform het beveiligingsbeleid zoals opgenomen in Bijlage 3 bij dit Protocol.

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 10 van het Convenant valt.
- 5.1.3 Voor de verwerking van persoonsgegevens als bedoeld in artikel 5.1.1 zijn van toepassing de grondslag conform de AVG en/of andere wettelijke grondslag, en de wettelijke bepalingen op grond waarvan de aanmeldende partij, dan wel de partij onder wiens verantwoordelijkheid de casusregisseur valt, de casus heeft aangemeld respectievelijk de casusregie voert.
- 5.1.4 De verantwoordelijke voor de verwerking van persoonsgegevens zoals bedoeld in artikel 5.1.1 betreft de verantwoordelijke zoals bedoeld in artikel 2.2 van dit protocol.

5.2 Verstrekken van persoonsgegevens ten behoeve van aanmelding en screening, triage en Ronde Tafel 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 screening, triage of Ronde Tafel Overleg worden uitgevoerd.
- 5.2.3 De grondslag conform de AVG voor het inbrengen van persoonsgegevens als bedoeld in artikel 5.2.1 wordt ontleend aan de eigen taak, en/of de taak van de partij ten behoeve waarvan de werkzaamheden in het kader van aanmelding en screening, triage of Ronde Tafel Overleg worden uitgevoerd.
- 5.2.4 De verantwoordelijke voor de verstrekking van persoonsgegevens als bedoeld in artikel 5.2.1 betreft de verantwoordelijke zoals bedoeld in artikel 2.1 van dit protocol.

5.3 Verstrekken van gegevens bij het uitvoering geven aan afspraken uit het Ronde Tafel 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:
- het uitvoering geven aan interventies en acties die in het Ronde Tafel Overleg zijn afgesproken;
 - het voeren van de casusregie op het plan van aanpak als dat in het Ronde Tafel Overleg is afgesproken;
 - het toebedelen van de casus aan een specifieke partij ten behoeve van verdere afhandeling, zoals het adviseren van de aanmelder of het aanbrengen van de casus bij een andere overlegtafel.
- 5.3.2. De grondslag conform de AVG voor het verstrekken van persoonsgegevens als verwoord in artikel 5.3.1 wordt ontleend aan de eigen taak en/of de taak van de partij die de activiteiten onder artikel 5.3.1 a t/m c uitvoert.
- 5.3.3. De verantwoordelijke voor de verstrekking van persoonsgegevens als bedoeld in artikel 5.3.1 betreft de verantwoordelijke zoals bedoeld in artikel 2.3.

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, lid 1, sub e, AVG voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de aanmeldende partner, dan wel de partner onder wiens verantwoordelijkheid de casusregisseur valt. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens. Voor gegevens afkomstig van het Openbaar Ministerie, is de grondslag gelegen in de artikel 8a, 39f en 51c Wet justitiële en strafvorderlijke gegevens.
- 6.2. De grondslag voor het inbrengen van persoonsgegevens als bedoeld in artikel 5.2.1, is artikel 6, lid 1, sub e, AVG voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de aanmeldende partner, dan wel de partner onder wiens verantwoordelijkheid de casusregisseur valt, en/of de verstreckende partij. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens. De grondslag voor het verstrekken van justitiële, strafvorderlijke en/of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.
- 6.3. De grondslag voor de verstrekking van persoonsgegevens als bedoeld in artikel 5.3.1, is artikel 6, lid 1, sub e, AVG 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 Wet politiegegevens. De grondslag voor het verstrekken van justitiële, strafvorderlijke en/of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.
- 6.4. De onder 6.1, 6.2 en 6.3 bedoelde grondslag kan bij casussen slechts van toepassing zijn indien dit voortvloeit uit de goede uitvoering van de taken en werkzaamheden van partijen, en de verwerking plaatsvindt namens of de verstrekking plaatsvindt aan een van de onder a t/m m genoemde partijen en voorwaarden:
- het bestuursorgaan de burgemeester: de goede uitvoering van taken en de uitoefening van bevoegdheden van de burgemeester, waaronder in het bijzonder taken en bevoegdheden op het gebied van Openbare Orde en Veiligheid zoals neergelegd in artikel 172 van de Gemeentewet.

- b. het bestuursorgaan het College van B&W: de goede uitvoering van taken van het college van burgemeester en wethouders, waaronder in het bijzonder taken in het sociaal domein zoals bedoeld in de Wmo artikel 2.3.1 t/m 2.3.5, de Jeugdwet artikel 2,3 en 2.4, de Participatiewet artikel 7.1, en artikel 3 van de Wet gemeentelijke schuldhulpverlening.
- c. het Openbaar Ministerie: voor de strafrechtelijke handhaving van de rechtsorde alsmede andere bij de wet vastgestelde taken (artikel 124 Wet op de Rechterlijke organisatie). De grondslag voor het verstrekken van justitiële, strafvorderlijke of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.
- d. de politie: vervulling van taken zoals bedoeld in de Politiewet artikel 3, te weten taken op het gebied van opsporing, handhaving van de rechtsorde en hulp aan hen die dat behoeven. De grondslag voor het verstrekken van persoonsgegevens inclusief politiegegevens is gelegen in artikel 20 Wpg. Deze verstrekkingen dienen nader te zijn vastgelegd in de onlosmakelijk bij dit Privacy Protocol behorende en ondertekende Artikel 20 Wpg Beslissing, waarin staat vermeld dat er alleen artikel 8 en 13 Politiegegevens worden verstrekt. De Artikel 20 Beslissing wordt ondertekend door de gemandateerde politiechef van de Eenheid, en het gezag te weten de Burgemeesters en de Officier van Justitie. In artikel 7 zijn nadere voorwaarden benoemd die van toepassing zijn op gegevens die in het kader van deze taken worden verstrekt.
- e. de Raad voor de Kinderbescherming: de goede uitvoering van de taken van de Raad voor de Kinderbescherming, waaronder in het bijzonder taken zoals bedoeld in boek 1 afdeling 3 van het Burgerlijk Wetboek, waaronder de artt. 1:240 BW en de artt. 1:255 juncto 1:257 BW, de artt. 77o en 77hh van het Wetboek van Strafrecht, de artt. 126 nd en 491 van het Wetboek van Strafvordering alsmede art. 28 van het Besluit Tenuitvoerlegging Jeugdstrafrecht 1994, de Algemene Wet Bestuursrecht, de artt. 2.4, 3.1 en 3.2 van de Jeugdwet alsmede art. 7.3.11 lid 4 van de Jeugdwet en art. 4 onder c, lid 1 van de Wet Opneming Buitenlandse Kinderen ter Adoptie (Wobka). Met inachtneming van het Kwaliteitskader 2020 van de Raad voor de Kinderbescherming.
- f. Veilig Thuis: de goede uitvoering van de taken van het AMHK, waaronder in het bijzonder taken zoals bedoeld in artikel 4.1.1 van de Wmo, met inachtneming van het Handelingsprotocol Veilig Thuis 2019.
- g. een Reclasseringsinstelling: de goede uitvoering van taken van de reclasseringsinstelling, waaronder in het bijzonder taken zoals bedoeld in de Reclasseringsregeling 1995 artikel 8, lid 1.
- h. een Gecertificeerde Instelling zoals bedoeld in de Jeugdwet artikel 1.1: de goede uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering zoals bedoeld in de Jeugdwet artikel 1.1.
- i. een instelling voor Geestelijke Gezondheidszorg: de uitvoering van de taken bij behandeling , verpleging, verzorging en bejegening van personen met een psychische stoornis, inclusief verslaving met of zonder verblijf in het kader van de Wgbo of de Wet verplichte ggz.

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

Artikel 7. Doorwerking 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 (Bpg), voor een ander doel politiegegevens zijn verstrekt aan een van de convenantpartijen, dan worden deze gegevens door de desbetreffende ontvanger in principe niet als persoonsgegevens door verstrekt aan de procesregisseur van het Veiligheidshuis. Bij voorkeur worden door de politie op grond van artikel 20 Wpg opnieuw actuele politiegegevens verstrekt aan de procesregisseur van het Veiligheidshuis voor de doelen zoals genoemd in artikel 3.2, 3.3 en Bijlage 2. De politie kan in uitzonderingsgevallen ook toestemming geven aan de ontvanger voor doorverstrekking aan de procesregisseur van het Veiligheidshuis maar legt deze toestemming vast in haar systemen.

- 7.2. Indien voor het inbrengen en/of verstrekken van persoonsgegevens zoals bedoeld in de artikelen 5.2 en 5.3 toestemming noodzakelijk is voor doorbreken geheimhoudingsbepalingen zoals bijvoorbeeld verwoord in de Wgbo (artikel 7:457 BW) en artikel 88 wet big, de beroepscode van de Jeugdzorgwerker artikel J, beroepscode NIP artikel 71 t/m 87 (psycholoog), of beroepscode NVO artikel 8 (pedagoog), de Reclasseringsregeling 1995 artikel 37, dan:
- a. wordt deze gevraagd op het moment dat duidelijk is dat het inbrengen of verstrekken noodzakelijk is t.b.v. van de in de betreffende fase aan de orde zijnde doelen, of de uitvoering van de in 5.3.1 a t/m c genoemde activiteiten;
 - b. worden deze persoonsgegevens uitsluitend verstrekt voor zover hiervoor de uitdrukkelijke toestemming is verkregen van de betrokkene of diens wettelijke vertegenwoordiger;
 - c. legt de partij die de toestemming heeft verkregen deze schriftelijk vast en informeert Betrokkene dat hij zijn toestemming altijd weer kan intrekken;
 - d. draagt de partij die toestemming heeft verkregen bij intrekking van die toestemming er zorg voor dat er geen verdere verstrekkingen meer plaatsvinden;
 - e. maakt de betrokken zorg- of hulpverlener een eigen afweging conform de voor hem geldende professionele standaarden, indien toestemming niet verkregen wordt en hij ervan overtuigd is dat zich hier een conflict van plichten voordoet, of goed hulpverlenerschap het verstrekken van persoonsgegevens verlangt.

Artikel 8. Documentatie individuele verstrekkingen

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

Artikel 9. Dataminimalisatie

- 9.1. Partijen Verwerken niet meer Persoonsgegevens dan noodzakelijk met het oog op de in artikel 3.2 van dit Protocol geformuleerde doeleinden.
- 9.2. Ten behoeve van de Screening 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 Veiligheidshuis die noodzakelijk zijn voor Triage.
- 9.3. In het Ronde Tafel Overleg Verwerken Partijen alleen die Persoonsgegevens die noodzakelijk zijn voor het opstellen en uitvoeren van een integraal plan van aanpak.
- 9.4. In het kader van Afschaling Verwerken Partijen alleen die Persoonsgegevens die noodzakelijk zijn om te bepalen of het plan van aanpak in het Ronde Tafel Overleg tot de gewenste resultaten heeft geleid. Indien wordt besloten dat behandeling van de Casus in het Veiligheidshuis niet of niet langer noodzakelijk is, worden de betreffende Persoonsgegevens niet langer in het Veiligheidshuis Verwerkt. De procesregisseur ziet erop toe dat Persoonsgegevens conform artikel 11 worden geanonimiseerd of vernietigd.
- 9.5. Wanneer de Partij die Persoonsgegevens in het Veiligheidshuis heeft verstrekt, kennis verkrijgt over de onjuistheid van die Persoonsgegevens, informeert die Partij de Casusregisseur en Procesregisseur hierover. De Procesregisseur coördineert de eventuele correctie van Persoonsgegevens in het Veiligheidshuis.

- 9.6. Enkel de Procesregisseur, Casusregisseur, Manager, administratief medewerker en afgevaardigden van Partijen in het Ronde Tafel Overleg hebben toegang tot de Persoonsgegevens die worden Verwerkt op locatie of in het informatiesysteem van het Veiligheidshuis en enkel voor zover noodzakelijk voor hun rol in een specifieke Casus.

Artikel 10. Kwaliteit

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

Artikel 11. Bewaren en Vernietigen

- 11.1. Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor het doel of de doeleinden waarvoor ze worden Verwerkt zoals geformuleerd onder artikel 3 en met inachtneming van artikel 9.
- 11.2. Persoonsgegevens worden vernietigd zodra de Verwerking daarvan niet langer nodig is voor het doel waarvoor zij zijn Verwerkt, maar uiterlijk binnen 1 jaar na het besluit tot afschaling.
- a. Persoonsgegevens kunnen tot zes maanden na besluit tot Afschaling worden bewaard in een vorm waarmee enkel de Procesregisseur en administratief medewerker toegang hebben tot de gegevens.
 - b. Na zes maanden na besluit tot Afschaling worden persoonsgegevens gearchiveerd en heeft enkel de Manager toegang tot die Persoonsgegevens.
 - c. Na één jaar na besluit tot Afschaling worden de Persoonsgegevens vernietigd.
- 11.3. Na één jaar kunnen gegevens, niet zijnde Persoonsgegevens, enkel worden bewaard voor managementdoeleinden.

Artikel 12. Beveiliging

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

Artikel 13. Geheimhouding

- 13.1. Een ieder die op grond van dit Protocol kennis neemt van Persoonsgegevens is verplicht tot geheimhouding daarvan, tenzij de wet tot bekendmaking verplicht. De Manager, Procesregisseur en eventueel ander ondersteunend personeel van het Veiligheidshuis worden door middel van een geheimhoudingsverklaring tot geheimhouding gebonden.
- 13.2. Partijen dragen er zorg voor dat iedere medewerker die in de uitvoering van het Convenant of dit Protocol in aanraking komt met Persoonsgegevens geheimhouding van die gegevens waarborgt.
- 13.3. Alle medewerkers van het Veiligheidshuis, inclusief medewerkers op basis van een dienstverleningsovereenkomst, deelnemers aan Ronde Tafel Overleggen en overige afgevaardigden van Partijen die toegang hebben tot Persoonsgegevens die onder dit Protocol worden Verwerkt, beschikken over een positieve Verklaring Omtrent Gedrag, dan wel hebben een veiligheidsonderzoek op grond van de voor de eigen organisatie geldende wet- en regelgeving doorlopen.
- 13.4. Wettelijke geheimhoudingsplichten zijn onverminderd van toepassing op eenieder die Strafrechtelijke persoonsgegevens of andere Bijzondere Persoonsgegevens in het kader van de samenwerking in het Veiligheidshuis ontvangt.
- 13.5. De Partijen in het samenwerkingsverband mogen de Persoonsgegevens afkomstig van de politie en Openbaar Ministerie slechts verwerken voor het specifieke doel waarvoor deze zijn verstrekt ten behoeve van de Casus. Deze Persoonsgegevens mogen alleen verder worden Verwerkt door de ontvangende Partijen indien het doel van de verdere verwerking verenigbaar is met dit doel waarvoor de Persoonsgegevens zijn verstrekt. Onverenigbaar gebruik van de gegevens, ook intern binnen de organisaties van de ontvangende Partijen, is niet toegestaan.
- 13.6. De Partijen in het samenwerkingsverband mogen de Persoonsgegevens afkomstig van andere Partijen die aan een geheimhoudingsplicht als onder meer bedoeld in de Wet Geneeskundige behandelovereenkomst (artikel 7:457 BW), Reclasseringsregeling 1995, Jeugdwet of Wet Maatschappelijke Ondersteuning zijn gebonden, slechts Verwerken voor het specifieke doel van de casus waarvoor deze zijn verstrekt. De Persoonsgegevens mogen alleen verder worden Verwerkt door de ontvangende Partijen met toestemming van de verstreckende Partij en indien het doel van de verdere verwerking verenigbaar is met dit doel waarvoor de Persoonsgegevens zijn verstrekt. Onverenigbaar gebruik van de Persoonsgegevens, ook intern binnen de organisaties van de ontvangende Partijen, is niet toegestaan.
- 13.7. Wanneer de grond voor het verstrekken van de Persoonsgegevens als bedoeld in artikel 7 gebaseerd is op toestemming van Betrokkene als bedoeld artikel 6, lid 1, onder a, AVG en/of artikel 9, lid 2, onder a, AVG en Betrokkene trekt deze toestemming in, laat de verstreckende Partij dit aan de ontvangende Partij weten, waarbij ook de toestemming voor Verwerking en verdere Verwerking voor de ontvangende Partij vervalt.

Artikel 14. Datalekken

- 14.1. Partijen houden procedures in stand die er op gericht zijn om inbreuken in de beveiligingsmaatregelen zoals geformuleerd in Bijlage 3 met betrekking tot de bescherming van Persoonsgegevens redelijkerwijs te detecteren en daarop actie te ondernemen, daaronder begrepen maatregelen tot herstel.
- 14.2. De gemeente Roermond 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 Veiligheidshuis. De manager ziet toe op de naleving van deze procedures in het Veiligheidshuis.
- 14.3. Partijen stellen de Manager onverwijld maar uiterlijk binnen 36 uur na kennisneming op de hoogte van een inbreuk op persoonsgegevens in de zin van artikel 4, onder 12, AVG dan wel artikel 26g Wet justitiële en strafvorderlijke gegevens die een risico inhoudt voor de rechten en vrijheden van betrokkenen zoals bedoeld in artikel 33 AVG. Deze kennisgeving omvat in ieder geval:
 - a. De aard en omvang van de inbreuk;
 - b. De contactgegevens van de persoon bij wie meer informatie over de inbreuk kan worden verkregen;
 - c. De maatregelen die kunnen worden genomen om de gevolgen van de inbreuk te voorkomen of beperken;
 - d. De mogelijke gevolgen en risico's van de inbreuk op de bescherming van Persoonsgegevens voor de Betrokkene;
 - e. De maatregelen die Partij zelf reeds heeft genomen of zal nemen om de bescherming van Persoonsgegevens te herstellen.
- 14.4. De Manager informeert Partijen middels de Voorbereidingsgroep stuurgroep schriftelijk over een inbreuk zoals bedoeld in artikel 14.3.
- 14.5. Partijen melden, indien wettelijk verplicht, een inbreuk zoals bedoeld in Artikel 14.3 bij de Autoriteit Persoonsgegevens. De Manager stuurt een afschrift van de melding aan de Autoriteit Persoonsgegevens aan de Voorbereidingsgroep Stuurgroep en de Stuurgroep.
- 14.6. Wanneer een inbreuk als bedoeld in Artikel 14.3 waarschijnlijk een hoog risico voor de rechten en vrijheden van Betrokkene(n) zal inhouden als bedoeld in artikel 34 AVG, wordt deze over de inbreuk geïnformeerd. Partijen informeren de Betrokkene over de inbreuk. De beslissing tot melding aan de Betrokkene wordt in de Voorbereidingsgroep stuurgroep genomen. De inhoud van die melding wordt in de Voorbereidingsgroep stuurgroep afgestemd, dan wel door de Voorbereidingsgroep stuurgroep aan één Partij gemandateerd.
- 14.7. Partijen verlenen elkaar de medewerking die redelijkerwijs van elkaar mag worden verwacht om aan de op Partijen rustende kennisgevingsverplichtingen te voldoen, mede met het oog op een eventueel onderzoek door de Autoriteit Persoonsgegevens.
- 14.8. Kennisgeving van de inbreuk aan de Autoriteit Persoonsgegevens door de Partijen gebeurt zonder onredelijke vertraging maar in ieder geval binnen 72 uur na ontdekking en geschiedt volgens de daartoe door de Autoriteit Persoonsgegevens ter beschikking gestelde procedure. De kennisgeving aan de Autoriteit Persoonsgegevens omvat minimaal:
 - a. de aard van de inbreuk;
 - b. een omschrijving van de categorieën Betrokkenen van wie Persoonsgegevens zijn betrokken bij de inbreuk;
 - c. de categorieën Persoonsgegevens;
 - d. of de Persoonsgegevens zijn versleuteld, geanonimiseerd, of anderszins onbegrijpelijk zijn gemaakt;
 - e. de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
 - f. de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van de Persoonsgegevens en de maatregelen die Partij heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

- 14.9. Kennisgeving van de inbreuk aan Betrokkene zoals bedoeld in Artikel 14.5 is niet vereist indien:
- a. passende technische en organisatorische maatregelen zijn genomen die de bescherming van Persoonsgegevens ook na de inbreuk garanderen;
 - b. achteraf genomen maatregelen de waarschijnlijkheid op een hoog privacy risico hebben weggenomen, of;
 - c. wanneer mededeling aan Betrokkene een onevenredig inspanning zou vragen.
- 14.10. Voorts kan de mededeling aan betrokkene worden uitgesteld, beperkt of achterwege gelaten worden, indien de inbreuk enkel ziet op gegevens afkomstig van het Openbaar Ministerie, en indien dit noodzakelijk en evenredig is:
- a. ter vermijding van belemmering van gerechtelijke onderzoeken of procedures;
 - b. ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
 - c. ter bescherming van de openbare veiligheid;
 - d. ter bescherming van de rechten en vrijheden van derden;
 - e. ter bescherming van de nationale veiligheid.
- 14.11. Partijen houden een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van de Persoonsgegevens. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen, alsmede de tekst van de kennisgeving aan de Betrokkene. De Manager houdt een overzicht bij van gelijksoortige inbreuken die plaatsvinden op locatie of in de informatiesystemen van het Veiligheidshuis.

Artikel 15. Privacy by Design

- 15.1. Voorafgaand aan een (nieuwe) Verwerking(en) onder dit Protocol, of de inzet van nieuwe technologieën voor de Verwerkingen onder dit Protocol, voeren Partijen middels de Voorbereidingsgroep stuurgroep een Gegevensbeschermingseffectbeoordeling uit conform artikel 35 AVG. De Manager coördineert dit proces.
- 15.2. Bij de uitvoering van de Gegevensbeschermingseffectbeoordeling wordt het model Gegevensbeschermingseffectbeoordeling Rijksdienst gevolgd.
- 15.3. Bij een voornemen omtrent de inzet van nieuwe technologieën kan dit voornemen ter advies worden voorgelegd aan het Landelijk Overleg Managers Veiligheidshuizen. Het Landelijk Overleg Managers Veiligheidshuizen kan advies uitbrengen over de beoogde inzet van nieuwe technologieën.
- 15.4. De uitkomsten van de Gegevensbeschermingseffectbeoordeling worden ter besluitvorming voorgelegd aan de Stuurgroep. De Stuurgroep kan hiervoor advies vragen aan de Voorbereidingsgroep stuurgroep over de voorgenomen nieuwe Verwerking zoals bedoeld in artikel 15.1. De Stuurgroep legt waar nodig op grond van artikel 36 AVG namens alle gezamenlijke Verwerkingsverantwoordelijken de beoogde Verwerking voor aan de Autoriteit Persoonsgegevens.

Artikel 16. Informatieverstrekking aan Betrokkenen

- 16.1. Vóór het verstrekken van Persoonsgegevens in het kader van de samenwerking wordt Betrokkene door de verstrekken Partij, dan wel de Partij die de Casusregie voert, geïnformeerd over het voornemen diens Persoonsgegevens verder te Verwerken in het kader van samenwerking in het Veiligheidshuis onder dit Protocol.
- 16.2. Deze informerende Partij maakt het tijdstip waarop en de wijze van informeren kenbaar aan de overige bij een Casus betrokken Partijen.
- 16.3. De Manager draagt zorg voor het publiceren van een privacy statement op de website van het Veiligheidshuis.
- 16.4. Alle deelnemende partijen zorgen op hun eigen website voor vermelding van deelname aan het Veiligheidshuis en voor een verwijzing naar de website van het Veiligheidshuis, alsook voor verwijzing naar het Veiligheidshuis 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 Veiligheidshuis zoals beschreven in artikel 3.2.
 - b. De Partijen die deelnemen aan de samenwerking in het Veiligheidshuis;
 - c. De termijn waarvoor de Persoonsgegevens worden opgeslagen en bewaard zoals omschreven onder artikel 11, dan wel de criteria voor het bepalen van die termijn;
 - d. Dat Betrokkene verscheidene rechten heeft met betrekking tot de Verwerking van diens Persoonsgegevens zoals geformuleerd onder artikel 17 tot en met 21;
 - e. Indien de Verwerking van Persoonsgegevens is gebaseerd op toestemming, dat Betrokkene het recht heeft deze te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de Verwerking van de Persoonsgegevens die heeft plaatsgevonden vóór intrekking van de toestemming;
 - f. Dat Betrokkene het recht heeft een klacht in te dienen over de Verwerking van zijn of haar Persoonsgegevens onder dit Protocol bij het Veiligheidshuis en bij de Autoriteit Persoonsgegevens;
 - g. Nadere uitleg indien de Persoonsgegevens moeten worden verstrekt of verder Verwerkt op grond van een wettelijke of contractuele verplichting;
 - h. Nadere uitleg indien Betrokkene verplicht is de Persoonsgegevens te verstrekken;
 - i. Indien sprake is van geautomatiseerde besluitvorming, met inbegrip van profilering, uitleg over de achterliggende logica, het belang van de verwerkingsactiviteiten en de verwachte gevolgen voor de Betrokkene.
 - j. De contactgegevens van de Manager bij wie de Betrokkene terecht kan voor meer informatie over de Verwerking van zijn Persoonsgegevens, dan wel waar hij zijn rechten geldend kan maken.
- 16.6. De informatieverplichting zoals bedoeld in artikel 16.1 is niet van toepassing indien het achterwege laten van informeren van Betrokkene noodzakelijk en evenredig is ter waarborging van:
 - a. de nationale veiligheid;
 - b. landsverdediging;
 - c. de openbare veiligheid;
 - d. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
 - e. andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van Nederland, met name een belangrijk economisch of financieel belang van de Europese Unie of van Nederland, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;

- f. de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
 - g. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscode voor gereguleerde beroepen;
 - h. een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d, e en g;
 - i. de bescherming van de betrokkene of van de rechten en vrijheden van anderen; of
 - j. de inning van civielrechtelijke vorderingen.
- 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 Betrokkenen

- 17.1. Betrokkenen kunnen bij Partijen een verzoek indienen om:
- a. Inzage te krijgen in de Persoonsgegevens die door Partijen over hem of haar worden Verwerkt;
 - b. Rectificatie of wissing 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 door Betrokkene ten aanzien van Persoonsgegevens die worden Verwerkt op locatie of in het informatiesysteem van het Veiligheidshuis worden gecoördineerd door de Manager. De Manager wordt hierbij ondersteund door de Procesregisseur. De Manager legt het verzoek via de Procesregisseur voor aan het Ronde Tafel Overleg en stemt daarin met Partijen de beantwoording van het verzoek af.
- 17.3. Indien het verzoek als bedoeld in Artikel 17.1 direct is gericht aan een der Partijen wordt de Manager hierover zo spoedig mogelijk door die Partij in kennis gesteld, opdat deze de beantwoording van het verzoek conform artikel 17.2 kan coördineren. Beantwoording van het verzoek door de Partij wordt in de Voorbereidingsgroep stuurgroep afgestemd.
- 17.4. Het bepaalde in artikel 17.2 en artikel 17.3 ontslaat Partijen niet van diens verantwoordelijkheid als Verwerkingsverantwoordelijke ten aanzien van een verzoek van Betrokkene.
- 17.5. Artikel 17.1 t/m 17.4, alsmede de artikelen 18, 19 en 20 zijn niet van toepassing op gegevens die verstrekt zijn door het College van procureurs-generaal. Op deze gegevens is de Wet justitiële en strafvorderlijke gegevens van toepassing. Verstrekkingen van gegevens door het College van procureurs-generaal worden ingevolge artikel 8 van dit Protocol en artikel 39j Wjsg schriftelijk vastgelegd en bewaard voor de duur van 4 jaar. Inzage- en rectificatieverzoeken worden beoordeeld door de privacyfunctionaris van het verstreckende parket van het Openbaar Ministerie. Verzetschriften tegen verwerking van gegevens worden beoordeeld door de afdeling Bestuurlijke en juridische zaken van het Parket-Generaal.
- 17.6. Op gegevens die eerder verstrekt zijn door de politie is de geheimhoudingsplicht van de Wet politiegegevens van toepassing. Derhalve zijn artikel 18, 19 en 20 van dit Protocol niet van toepassing. Inzage- en correctieverzoeken worden beoordeeld door de verstreckende eenheid van de politie. Verzet- en bezwaarschriften tegen verwerking van gegevens worden beoordeeld door de verstreckende eenheid van de politie, conform art. 29 Wpg.

Artikel 18. Recht op inzage

- 18.1. In het geval het verzoek ziet op inzage in de Verwerking van Persoonsgegevens in het Veiligheidshuis door Partijen zoals bedoeld in artikel 17.1 onder a, dient de beantwoording van dat verzoek 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 een klacht in te dienen bij een toezichthoudende autoriteit;
 - g) wanneer de Persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
 - h) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4 AVG bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de Betrokkene.
- 18.2. Het verzoek wordt binnen vier weken door de Manager beantwoord; de Manager doet dit namens de betrokken partijen die elk zelf verantwoordelijke zijn. Een verzoek tot inzage wordt enkel geweigerd, indien en voor zover dit noodzakelijk is met het oog op in de wet gespecificeerde weigeringsgronden.
- 18.3. Een eventuele (gedeeltelijke) afwijzing is schriftelijk en gemotiveerd.
- 18.4. Alvorens aan een verzoek als bedoeld in artikel 17.1 wordt voldaan, verifiëren Partijen de identiteit van de Betrokkene die het verzoek indient. Betrokkene dient hiervoor persoonlijk langs te komen bij het Veiligheidshuis.
- 18.5. Bij voldoen aan een verzoek als bedoeld in artikel 17.1, verstrekt de Manager namens de Verwerkingsverantwoordelijke(n) aan de Betrokkene een kopie van de Persoonsgegevens die worden verwerkt.

Artikel 19. Recht op rectificatie en gegevenswissing

- 19.1. Indien de Betrokkene op grond van zijn verzoek om inzage een verzoek tot rectificatie of wissing van bepaalde hem of haar betreffende Persoonsgegevens zoals bedoeld in artikel 17.1 onder b doet bij het Veiligheidshuis, legt de Manager dit verzoek voor aan de Voorbereidingsgroep Stuurgroep (de Partijen binnen het Veiligheidshuis die de betreffende persoonsgegevens voor die verwerking hebben verstrekt of ontvangen) met het oog op de beoordeling van het verzoek.
- 19.2. Onjuiste Persoonsgegevens betreffende de Betrokkene worden op diens verzoek onverwijld gerectificeerd.
- 19.3. Persoonsgegevens betreffende de Betrokkene worden zonder onredelijke vertraging op diens verzoek gewist wanneer deze:
- a. voor het doel van de Verwerking onvolledig of niet ter zake dienend zijn; of
 - b. anderszins in strijd met een wettelijk voorschrift worden Verwerkt.

- 19.4. De Manager informeert de Betrokkene over de beslissing omtrent zijn verzoek tot rectificatie of wissing van hem of haar betreffende Persoonsgegevens schriftelijk en gemotiveerd zo spoedig mogelijk, maar uiterlijk binnen 4 weken na ontvangst van het verzoek.

Artikel 20. Recht van bezwaar

- 20.1. Indien de Verwerking van Persoonsgegevens door Partijen is gebaseerd op de grondslagen van artikel 6, lid 1, onder e of f, Algemene Verordening Gegevensbescherming, kan de Betrokkene daartegen te allen tijde bezwaar aantekenen in verband met zijn bijzondere persoonlijke omstandigheden.
- 20.2. Indien een recht van bezwaar 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 de Voorbereidingsgroep stuurgroep (de Partijen binnen het Veiligheidshuis die de betreffende persoonsgegevens voor die verwerking hebben verstrekt of ontvangen) om te beoordelen of het verzoek gerechtvaardigd is en coördineert de afhandeling daarvan.
- 20.4. De Manager informeert de Betrokkene over de beslissing zoals bedoeld in artikel 17.3 binnen 4 weken en draagt er zorg voor dat de beslissing binnen deze 4 weken wordt uitgevoerd. Een beslissing om niet, of niet geheel, te voldoen wordt altijd gemotiveerd en kan met het oog op artikel 21 AVG enkel worden gebaseerd op dwingende gerechtvaardigde gronden.

Artikel 21. Recht op overdraagbaarheid van Persoonsgegevens

- 21.1. Het recht op overdraagbaarheid van Persoonsgegevens is niet van toepassing op Partijen in het Veiligheidshuis.

Artikel 22. Verwerkers

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

Artikel 23. Verstrekking aan derden

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

Artikel 24. Verwerkingsregister en Functionaris Gegevensbescherming

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

Artikel 25. Aansprakelijkheid

- 25.1. Partijen zetten zich in voor een goede uitvoering van het bepaalde in dit Protocol en zullen zich houden aan de dienaangaande in dit Protocol gemaakte afspraken.
- 25.2. Partijen zijn ieder voor zich aansprakelijk voor aanspraken van Betrokkenen, of Derden op schadevergoeding op grond van directe of indirecte schade, administratieve boetes of andere aanspraken van derden in geval van toerekenbare tekortkoming door de aangesproken Partij in de nakoming van het bepaalde in dit Protocol en de bijbehorende Bijlagen.

- 25.3. Wanneer meerdere Verwerkingsverantwoordelijken of Verwerkers bij dezelfde Verwerking betrokken zijn, en verantwoordelijk zijn voor schade die door die Verwerking is veroorzaakt, wordt elke Verwerkingsverantwoordelijke of Verwerker voor de gehele schade aansprakelijk gehouden teneinde te garanderen dat de betrokkene daadwerkelijk wordt vergoed.
- 25.4. Een Verwerker is slechts aansprakelijk voor de schade die door Verwerking is veroorzaakt wanneer bij de Verwerking niet is voldaan aan de specifiek tot Verwerkers gerichte verplichtingen van de Algemene Verordening Gegevensbescherming of buiten dan wel in strijd met de rechtmatige instructies van de Verwerkingsverantwoordelijke is gehandeld.
- 25.5. Onverminderd het gestelde in lid 4 kan iedere Verwerkingsverantwoordelijke of Verwerker die de volledige vergoeding heeft betaald vervolgens bij de andere Verwerkingsverantwoordelijken of Verwerkers die bij dezelfde Verwerking betrokken zijn, het deel van de schadevergoeding verhalen dat overeenkomt met hun deel van de aansprakelijkheid voor de schade. Een Verwerkingsverantwoordelijke of Verwerker kan door andere Verwerkingsverantwoordelijken of Verwerkers worden vrijgesteld van onderlinge betaling van schadevergoeding indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.

Artikel 26. Toezicht en handhaving

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

Artikel 27. Wijzigingen

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

Artikel 28. Toetreding

- 28.1. Toetreding door andere organisaties tot dit Protocol kan enkel wanneer die Partij is toegetreden tot het Convenant conform Artikel 17 van het Convenant.
- 28.2. Partijen worden vooraf door de secretaris van de Stuurgroep op de hoogte gebracht van de voorgenomen toetreding. Indien de toetredende partij niet staat benoemd in het Handvat dient voorafgaand aan de uitwisseling van Persoonsgegevens met de toetredende partij een juridische analyse te worden opgesteld conform hoofdstuk 5 van het Handvat. De toetredende Partij voert waar nodig de aanbeveling uit die analyse uit, alvorens uitwisseling van Persoonsgegevens in het Veiligheidshuis met die partij plaatsvindt.

- 28.3. In geval van toetreding tot het Convenant, vindt toetreding tot het Protocol plaats door middel van ondertekening van Bijlage 1 bij dit Protocol door die andere organisatie en de voorzitter van de Stuurgroep.

Artikel 29. Duur, opzegging, beëindiging

- 29.1. Dit Protocol treedt in werking op de dag van ondertekening door Partijen en geldt voor dezelfde duur als het Convenant. In geval van verlenging van het Convenant wordt dit Protocol met een gelijklopende termijn verlengd.
- 29.2. De Stuurgroep kan, zonder rechterlijke tussenkomst en met meerderheid van stemmen, na ingebrekestelling, een Partij met onmiddellijke ingang uitsluiten van de samenwerking in het Veiligheidshuis, indien de afspraken zoals neergelegd in dit Protocol niet door de desbetreffende Partij worden nagekomen.
- 29.3. Verplichtingen die naar hun aard zijn bestemd om ook na beëindiging of uitsluiting van het project voort te duren, blijven na beëindigingen van dit Protocol bestaan. Tot deze verplichtingen behoren onder meer die ter zake van geheimhouding en de beveiliging van Persoonsgegevens.

Artikel 30. Opvolging

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

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

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

Artikel 32. Toepasselijk recht

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

Gemeente Leudal

in dezen rechtsgeldig vertegenwoordigd door: de burgemeester

Datum en plaats:

Gemeente Maasgouw

in dezen rechtsgeldig vertegenwoordigd door: de burgemeester

Datum en plaats:

<i>Gemeente Nederweert</i>
in dezen rechtsgeldig vertegenwoordigd door: de burgemeester
Datum en plaats:

<i>Gemeente Roerdalen</i>
in dezen rechtsgeldig vertegenwoordigd door: de wethouder
Datum en plaats:

<i>Gemeente Roermond</i>
in dezen rechtsgeldig vertegenwoordigd door: de burgemeester
Datum en plaats:

<i>Gemeente Weert</i>
in dezen rechtsgeldig vertegenwoordigd door: de burgemeester
Datum en plaats:

Politie Eenheid Limburg

in dezen rechtsgeldig vertegenwoordig door:
Sectorhoofd District Noord en Midden Limburg
Compagniescommandant Bewakingseenheid NL

dr. B.R. van Gelderen

Datum en plaats:

Openbaar Ministerie arrondissementsparket Limburg

in dezen rechtsgeldig vertegenwoordigd door: *[naam en functie]*

Datum en plaats:

<i>Raad voor de Kinderbescherming</i>
in dezen rechtsgeldig vertegenwoordigd door: <i>[naam en functie]</i>
Datum en plaats:

3 RO

in dezen rechtsgeldig vertegenwoordigd door: *[naam en functie]*

Datum en plaats:

Bureau Jeugdzorg Limburg

in dezen rechtsgeldig vertegenwoordigd door: *[naam en functie]*

Datum en plaats:

Algemeen Maatschappelijk Werk Midden-Limburg

in dezen rechtsgeldig vertegenwoordigd door: *[naam en functie]*

Datum en plaats:

<i>Veilig Thuis</i>
in dezen rechtsgeldig vertegenwoordigd door: <i>[naam en functie]</i>
Datum en plaats:

Centrum voor Jeugd en Gezin

in dezen rechtsgeldig vertegenwoordigd door: *[naam en functie]*

Datum en plaats:

MEE Noord- en Midden Limburg

in dezen rechtsgeldig vertegenwoordigd door: *[naam en functie]*

Datum en plaats:

Penitentiare Inrichting Sittard

in dezen rechtsgeldig vertegenwoordigd door: *[naam en functie]*

Datum en plaats:

Penitentiare Inrichting Zuid Oost

in dezen rechtsgeldig vertegenwoordigd door: *[naam en functie]*

Datum en plaats:

GGZ-instelling Vincent van Gogh

in dezen rechtsgeldig vertegenwoordigd door: *[naam en functie]*

Datum en plaats:

Met GGZ

in dezen rechtsgeldig vertegenwoordigd door: *[naam en functie]*

Datum en plaats:

De Rooyse Wissel

in dezen rechtsgeldig vertegenwoordigd door: *[naam en functie]*

Datum en plaats:

Pedagogisch Sociaal Werk

in dezen rechtsgeldig vertegenwoordigd door: *[naam en functie]*

Datum en plaats:

Moveoo

in dezen rechtsgeldig vertegenwoordigd door: *[naam en functie]*

Datum en plaats:

<i>William Schrikker groep</i>
in dezen rechtsgeldig vertegenwoordigd door: <i>[naam en functie]</i>
Datum en plaats:

<i>Zelfregiecentrum</i>
in dezen rechtsgeldig vertegenwoordigd door: <i>[naam en functie]</i>
Datum en plaats:

Bijlage 1: Toetredingsformulier nieuwe partner tot Protocol

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

overwegende dat:

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

verklaart daartoe het volgende:

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

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

Naam organisatie:

Naam bevoegde functionaris:

.....

Namens Stuurgroep:

Naam:

.....

Bijlage 2: Doeleinden Verwerking van Persoonsgegevens per processtap

Partijen Verwerken in het kader van het Veiligheidshuis voor ieder van onderstaande fasen enkel de Persoonsgegevens die voor die afzonderlijke fase noodzakelijk zijn voor de uitvoering van ieder van de daarbij geformuleerde toepasselijke processtappen: Zie hiervoor de Werkprocesbeschrijving Veiligheidshuis Midden-Limburg Integrale Veiligheid en Complexe Multi-problematiek, waarin alle processtappen zijn beschreven.

Aanmelding en screening

- Beoordelen of een Casus die door een Partij wordt aangedragen voldoet aan de criteria voor behandeling in het Veiligheidshuis. Deze criteria volgen uit het Landelijk Kader.

Triage

- Bepalen eerste beeld en verrijken van informatie uit Screening;
- Op basis van informatie van partners komen tot een nadere afweging ten aanzien van de routing van de casus, tot een bepaling van doel en thema's van een eventueel Ronde Tafel Overleg, en tot een afweging welke partners relevant zijn om te betrekken bij een Ronde Tafel Overleg;
- Voorbereiding Ronde Tafel Overleg.

Ronde Tafel Overleg

- Opstellen gezamenlijk toestandsbeeld door bij het Ronde Tafel Overleg betrokken Partijen;
- Opstellen integraal plan van aanpak;
- Monitoren van de uitvoering en resultaten van het plan van aanpak;
- Bepalen of verdere verstrekking van Persoonsgegevens aan andere samenwerkingsverbanden noodzakelijk en mogelijk is;
- Besluiten tot afbouwen betrokkenheid Veiligheidshuis;
- Besluiten tot Opschaling van de Casus;

Afschaling

- Bepalen van noodzakelijke te verstrekken Persoonsgegevens in het kader van Afschaling en de verstrekking daarvan aan bijvoorbeeld de Casusregisseur;

Bijlage 3: Beveiligingsbeleid Persoonsgegevens

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

- **Beleidsdocument voor informatiebeveiliging**
Het beleidsdocument gaat expliciet in op de maatregelen die de verantwoordelijke treft om de verwerkte persoonsgegevens te beveiligen. Het document is goedgekeurd op bestuurlijk c.q. leidinggevend niveau en kenbaar gemaakt aan alle werknemers en relevante externe partijen.
- **Toewijzen van verantwoordelijkheden voor informatiebeveiliging**
Alle verantwoordelijkheden, zowel op sturend als op uitvoerend niveau, zijn duidelijk gedefinieerd en belegd.
- **Beveiligingsbewustzijn**
Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers krijgen geschikte training en regelmatige bijscholing over het informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures van de organisatie, voor zover relevant voor hun functie. Binnen de training en bijscholing wordt expliciet aandacht besteed aan de omgang met persoonsgegevens.
- **Fysieke beveiliging en beveiliging van apparatuur**
IT voorzieningen en apparatuur zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. De geboden bescherming is in overeenstemming met de vastgestelde risico's.
- **Toegangsbeveiliging**
Er zijn procedures om bevoegde gebruikers toegang te geven tot de informatiesystemen en diensten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen. De procedures omvatten alle fasen in de levenscyclus van de gebruikerstoegang, van de eerste registratie van nieuwe gebruikers tot de uiteindelijke afmelding van gebruikers die niet langer toegang tot informatiesystemen en -diensten nodig hebben. Waar van toepassing wordt bijzondere aandacht besteed aan het beheren van toegangsrechten van gebruikers met extra ruime bevoegdheden, zoals systeembeheerders.
- **Logging en controle**
*Activiteiten die gebruikers uitvoeren met persoonsgegevens worden vastgelegd in logbestanden. Hetzelfde geldt voor andere relevante gebeurtenissen, zoals pogingen om ongeautoriseerd toegang te krijgen tot persoonsgegevens en verstoringen die kunnen leiden tot verminking of verlies van persoonsgegevens. De logbestanden worden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de persoonsgegevens en waar nodig wordt actie ondernomen.
De verantwoordelijke moet er rekening mee houden dat er, als de gegevens in de logbestanden tot personen herleidbaar zijn, sprake is van een verwerking van persoonsgegevens in de zin van de [AVG] waarop de verplichtingen uit deze wet van toepassing zijn. In dat geval kan er ook sprake zijn van een personeelsvolgsysteem in de zin van artikel 27 lid 1 van de Wet op de ondernemingsraden (WOR), waarvoor instemming van de ondernemingsraad is vereist.*

- **Correcte verwerking in toepassingssystemen**
In alle toepassingssystemen, inclusief toepassingen die door gebruikers zelf zijn ontwikkeld, zijn beveiligingsmaatregelen ingebouwd. Tot deze beveiligingsmaatregelen behoort de controle dat de invoer, de interne verwerking en de uitvoer aan vooraf gestelde eisen voldoen (validatie). Voor systemen waarin bijzondere of strafrechtelijke persoonsgegevens worden verwerkt of die invloed hebben op de verwerking van bijzondere of strafrechtelijke persoonsgegevens, kunnen aanvullende beveiligingsmaatregelen nodig zijn.
- **Beheer van technische kwetsbaarheden**
Software, zoals browsers, virusscanners en operating systems, wordt up-to-date gehouden. Ook installeert de verantwoordelijke tijdig oplossingen die de leverancier uitbrengt voor beveiligingslekken in deze software. Meer in het algemeen verkrijgt de verantwoordelijke tijdig informatie over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden wordt geëvalueerd en de verantwoordelijke treft geschikte maatregelen getroffen voor de behandeling van de risico's die daarmee samenhangen.
- **Incidentenbeheer**
Er zijn procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging, zodra ze zijn gerapporteerd. Het beoordelen van de risico's voor de betrokkenen en het effectief informeren van de betrokkenen en, waar van toepassing, de toezichthouder is in deze procedures opgenomen. De lessen getrokken uit de afgehandelde incidenten worden gebruikt om de beveiliging waar mogelijk structureel te verbeteren. Als een vervolgprocedure na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), wordt het bewijsmateriaal verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.
- **Afhandeling van datalekken en beveiligingsincidenten**
De verantwoordelijke meldt datalekken die onder een wettelijke meldplicht vallen bij de betreffende toezichthouder. 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 verwerkingsverantwoordelijke of van de verwerker, alsmede de verwerker zelf, voor zover deze toegang hebben tot persoonsgegevens, verwerkt deze slechts in opdracht van de verwerkingsverantwoordelijke, behoudens afwijkende wettelijke verplichtingen."

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

De Autoriteit Persoonsgegevens sluit hierbij grotendeels aan op de EN-ISO/IEC 27002:2007. Voor de Verwerking van bijzondere Persoonsgegevens, meer in het bijzonder gegevens betreffende iemands gezondheid, verwijst de Autoriteit Persoonsgegevens ook naar de NEN7510.

Als er een datalek bij het Veiligheidshuis optreedt, loopt de melding via de partijen waarvan de gegevens gelekt zijn, i.c. de betrokkenen bij een casus, of indien het een inbraak in de systemen betreft alle convenantpartners.

Bijlage 4: Categorieën Persoonsgegevens en Betrokkenen

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

Categorie 1:

Categorie Betrokkenen:

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

Persoonsgegevens:

- volledige personalia (naam, geboorteplaats, geboortedatum);
- adresgegevens (straat, huisnummer, postcode, woonplaats);
- contactgegevens (telefoonnummer, e-mailadres);
- gegevens omtrent woonsituatie;
- financiële gegevens;
- gegevens betreffende relaties met overige gezinsleden/ directe sociale contacten;
- toezicht- en handavingsgegevens, gegevens omtrent bestuursrechtelijke maatregelen of voornemens daartoe;
- Politiegegevens ten behoeve van de hulpverleningstaak (niet zijnde persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten zoals bedoeld in artikel 10 AVG).

Bijzondere Persoonsgegevens zoals bedoeld in artikel 9 AVG, te weten:

- Gegevens over gezondheid;
- Persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken;
- Persoonsgegevens waaruit ras of etnische afkomst blijken;
- Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

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

- Politiegegevens;
- Strafvorderlijke gegevens en relevante justitiële gegevens;
- Tenuitvoerleggingsgegevens.

Voor de Verwerking van Bijzondere Persoonsgegevens kent de AVG in beginsel een verwerkingsverbod. De verwerking van deze gegevens is niet toegestaan, behoudens voor zover het verwerkingsverbod is opgeheven in artikel 9 en 10 AVG, alsook artikel 23 t/m 33 Uitvoeringswet AVG.

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 en gegevenswissing, en gegevens omtrent bezwaar en klachten;
- Politiegegevens ten behoeve van de hulpverleningstaak (niet zijnde persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten zoals bedoeld in artikel 10 AVG).

Bijzondere Persoonsgegevens zoals bedoeld in artikel 9 AVG, te weten:

- Gegevens over gezondheid.

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

- Politiegegevens;
- Strafvorderlijke gegevens.

Voor de Verwerking van Bijzondere Persoonsgegevens kent de AVG in beginsel een verwerkingsverbod. De verwerking van deze gegevens is niet toegestaan, behoudens voor zover het verwerkingsverbod is opgeheven in artikel 9 en 10 AVG, alsook artikel 23 t/m 33 Uitvoeringswet AVG.

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;
- 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;
- functie binnen het Veiligheidshuis;
- contactgegevens (zakelijk telefoonnummer, e-mailadres).