SAMENWERKINGS CONVENANT

Convenant Samenwerking tussen ketenpartners in Zorg- en Veiligheidshuis Rotterdam-Rijnmond

Algemeen Bestuur vastgesteld d.d. 28-02-2024

Inhoud

Hoe dit Samenwerkingsconvenant te gebruiken

Met dit Samenwerkingsconvenant worden afspraken rondom de samenwerking tussen verschillende partijen in het Zorg- en Veiligheidshuis geformaliseerd en vastgelegd. Uit dit Samenwerkingsconvenant dient duidelijk te blijken wie, met welk doel en met welke inzet deelneemt aan het Zorg- en Veiligheidshuis, alsook wie waarover, op welk niveau, regie voert en hoe besluitvorming plaatsvindt.

In dit Samenwerkingsconvenant zijn de standaard onderdelen van een (meer-partijen) overeenkomst opgenomen. De verdeling van verantwoordelijkheden, rechten en plichten is uiteindelijk aan partijen om zelf in te vullen. Waar nodig is door middel van gearceerde teksten ruimte voor maatwerk of toelichting gegeven op de keuzemogelijkheden en de mogelijke gevolgen van die keuzes. Dit is echter niet uitputtend en dient door iedere partij die deelneemt aan dit Convenant zelf nader te worden onderzocht.

Formuleringen, begrippen en andere specifieke Zorg- en Veiligheidshuis-gerelateerde termen zijn afgeleid uit het Handvat "Gegevensuitwisseling in het zorg- en veiligheidsdomein – een juridisch handvat voor Zorg- en Veiligheidshuizen", versie 2.2. juli 2020 (hierna 'Handvat' genoemd) en het Landelijk Kader Veiligheidshuizen. Ook wordt aangesloten bij de werkwijze zoals in het Handvat beschreven.

Convenant Samenwerking tussen ketenpartners Zorg- en Veiligheidshuis Rotterdam Rijnmond

De ondergetekenden:

De Colleges van Burgemeester en Wethouders en de Burgemeesters, ieder voor zover het haar/zijn bevoegdheid betreft, van de gemeenten:

Burgemeester gemeente Albrandswaard;

Burgemeester gemeente Barendrecht;

Burgemeester gemeente Voorne aan Zee;

Burgemeester Capelle aan den IJssel

Wethouder Zorg gemeente Goeree Overflakkee;

Burgemeester gemeente Krimpen aan den IJssel;

Burgemeester gemeente Lansingerland;

Burgemeester gemeente Maassluis;

Burgemeester gemeente Nissewaard;

Burgemeester gemeente Ridderkerk;

Burgemeester gemeente Schiedam;

Wethouder Zorg gemeente Vlaardingen;

Burgemeester gemeente Rotterdam, voorzitterschap bestuur gedelegeerd aan wethouder Zorg Rotterdam;

Directeur Directie Veiligheid gemeente Rotterdam;

Directeur Maatschappelijke Ontwikkeling gemeente Rotterdam

Directeur GGZ Antes;

Algemeen directeur langdurige zorg en reclassering Fivoor;

Directeur GGZ Fivoor;

Dienst Justitiele Inrichtingen (DJI)

Directeur Middin;

Directeur Ipse de Brugge;

Directeur Mozaik/Pameijer;

Directeur Zuid Wester;

Directeur GGZ Delfland;

Directeur Veilig Thuis Rotterdam-Rijnmond;

Directeur Leger des Heils;

Hoofd Operatiën Eenheid Rotterdam Politie;

Hoofdofficier van Justitie Arrondissementsparket Rotterdam;

Regio directeur Reclassering Nederland, regio Zuid-West;

Directeur Slachtofferhulp Nederland regio Zuid-West;

Directeur Raad voor de Kinderbescherming Rotterdam;

Directeur Jeugdbescherming Rotterdam-Rijnmond;

Directeur William Schrikker Jeugdbescherming & Jeugdreclassering Zuid West Nederland;

Directeur HALT Nederland;

Directeur MEE Rotterdam;

N.I.F.P.;

Directeur Centrum voor Dienstverlening;

Directeur Arosa;

Directeur Fier;

Directeur Elkerlyc;

Directeur Enver;

Directeur Humanitas;

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

de volgende overwegingen in aanmerking nemende:

- Partijen in het kader van samenwerking op het gebied van integrale veiligheid en complexe casuïstiek het Zorg- en Veiligheidshuis Rotterdam-Rijnmond (hierna: 'Zorg- en Veiligheidshuis of ZVHRR') hebben opgezet;
- De Rijksoverheid per 1 januari 2013 de verantwoordelijkheid voor de veiligheidshuizen van het Openbaar Ministerie naar de zetelgemeente van de veiligheidsregio heeft overgedragen, waardoor de gemeentelijke strategische regierol verder versterkt is;
- Er bestuurlijke afspraken zijn gemaakt tussen het toenmalige Ministerie van Veiligheid en Justitie en de Vereniging Nederlandse Gemeenten, namens alle Nederlandse gemeenten, rondom de financiële bijdrage van de Rijksoverheid aan de Veiligheidshuizen, die zijn opgenomen als bijlage bij de brief van de Staatssecretaris van Veiligheid en Justitie d.d. 2 augustus 2012, kenmerk 287830;
- Van belang is dat partijen personele bijdragen blijven leveren in de vorm van partnerbijdragen aan triage- en/of casus-overleggen en/of structurele deelname aan het Zorg- en Veiligheidshuis;
- Partijen hun eigen bevoegdheden houden met betrekking tot de in het Zorg- en Veiligheidshuis besproken casuïstiek en het Zorg- en Veiligheidshuis de uitoefening van deze bevoegdheden niet overneemt, maar stuurt op een integrale en gezamenlijke inzet van partijen;
- Partijen nadrukkelijk het belang en de noodzaak onderschrijven dat alleen door domein-overstijgende en gezamenlijke inzet de complexe probleemsituaties die in het Zorg- en Veiligheidshuis worden voorgelegd, kunnen worden opgelost of verbeterd;
- Hiervoor enkele belangrijke voorwaarden zijn geformuleerd, waaronder de bestendiging van de goede aansluiting met en de herkenbaarheid voor alle partijen van het Zorg- en Veiligheidshuis en de bestuurlijke borging van de domein-overstijgende aanpak binnen het zorgdomein, justitieel domein en gemeentelijk domein;
- Partijen te kennen hebben gegeven de huidige samenwerking bestuurlijk-juridisch, beheersmatig, organisatorisch en financieel te willen versterken;
- Partijen hebben aangegeven alle onderlinge samenwerkingsafspraken rondom complexe multi-problematiek schriftelijk te willen vastleggen in een samenwerkingsconvenant;
- De afspraken rondom de verwerking van persoonsgegevens in het Privacy Protocol Integrale Veiligheid en Complexe Multi-Problematiek zijn vastgelegd, dat integraal onderdeel is van dit samenwerkingsconvenant;
- In de Landelijke Stuurgroep Zorg en Veiligheid vindt met landelijke vertegenwoordigers overleg plaats. In dit landelijke overleg worden de koers en landelijke prioriteiten van de Zorg- en Veiligheidshuizen

bepaald. Het landelijke overleg biedt hierbij kaders die op regionaal niveau nader worden ingevuld. Het landelijke niveau biedt een opschalingsmogelijkheid voor regionale ontwikkelpunten. Op landelijk niveau worden landelijke trends en ontwikkelpunten gesignaleerd en waar nodig oplossingen bedacht. Elke partner is verantwoordelijk voor afstemming en uitvoering van afspraken binnen de eigen organisatie op zowel landelijk als regionaal niveau.

- De managers van de Zorg- en Veiligheidshuizen zijn verenigd in de Vereniging van Managers Zorg- en Veiligheidshuizen;
- Dit samenwerkingsconvenant verder wordt aangehaald als 'het Convenant'.

verklaren te zijn overeengekomen:

Artikel1. Definities

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

1.1. Strategische Regie: de coördinatie van regionale samenwerking in het Zorg- en Veiligheidshuis, verbinding van verschillende ketens en afstemming met andere lokale en regionale samenwerkingsverbanden, organisaties en overlegtafels.

1.2. 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;

1.3. 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;

1.4. Casus: een geval of situatie dat of die voldoet aan de criteria voor complexe casuïstiek zoals geformuleerd in artikel 2, en die is aangemeld bij het Zorg- en Veiligheidshuis ter beoordeling en eventuele bespreking in het casusoverleg;

1.5. Betrokkene: de natuurlijke persoon op wie informatie, waaronder persoonsgegevens zoals beschreven in het privacy protocol, betrekking heeft;

1.6. Derde: de natuurlijk persoon of rechtspersoon, niet zijnde de betrokkene, noch één der partijen.

1.7. Aanmelding en Intake: het voordragen van een casus door één der partijen en het uitwisselen van informatie, waaronder persoonsgegevens, tussen de procesregisseur van het Zorg- en Veiligheidshuis en de aanmeldende partij ter toetsing of de casus in aanmerking komt voor behandeling in het Zorg- en Veiligheidshuis.

1.8. Triage: het proces waarbij relevante partijen worden bevraagd om te komen tot een nadere afweging ten aanzien van de routering van de casus, tot een bepaling van het doel en de thema's van een eventueel casusoverleg, en tot een afweging welke partijen relevant zijn om te betrekken bij een casusoverleg.

1.9. Casusoverleg: 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;

1.10. Afschaling: fase die volgt op het besluit in het casusoverleg dat de betrokkenheid van het Zorg- en Veiligheidshuis niet langer nodig is, waarin het dossier dat in het systeem van het Zorg- en Veiligheidshuis is aangelegd ten behoeve van procesregie, geschoond wordt van alle niet langer noodzakelijke informatie, en uiteindelijk verdwijnt uit het systeem van het Zorg- en Veiligheidshuis;

1.11. Procesregisseur: de medewerker van het Zorg- Veiligheidshuis die namens een van de partijen is belast met de werkzaamheden in artikel 13;

1.12. Casusregisseur: de medewerker van een van de partijen die is belast met de taken in artikel 14;

1.13. Hoofd: de persoon die is belast met de taken zoals geformuleerd in Artikel 12;

1.14. Algemeen Bestuur: het verband van afgevaardigden van partijen zoals geformuleerd in Artikel 5;

1.15. Dagelijks Bestuur: het verband van afgevaardigden van zoals geformuleerd in art 4:

1.16. Het Breed MT: het verband van afgevaardigden van partijen zoals geformuleerd in Artikel 7;

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. Jaarplan: het door de Algemeen Bestuur op grond van Artikel 5.4 vastgestelde plan betreffende de operationele en inhoudelijke kaders en het financieel en inhoudelijk beleid van het Zorg- en Veiligheidshuis.

1.19. Werkproces: het door het Breed MT op grond van Artikel 7.5, onder c, vastgestelde proces voor samenwerking in het Zorg- en Veiligheidshuis, waaronder het proces omtrent en het delen van informatie en het op- en afschalen van een casus.
1.20. Plan van aanpak: Een op de individuele behoeften van een cliënt toegesneden, samenhangend en, voor zover mogelijk en noodzakelijk, systeemgericht geheel van interventies, al dan niet (ten dele) aangeboden in het gedwongen kader van het strafrecht, het bestuursrecht en/of het civiele recht, daaronder ook begrepen nazorg na detentie.

Artikel 2. Visie, Doel en Werkwijze Zorg- en Veiligheidshuis

2.1 Het zorg- en veiligheidshuis is een samenwerkingsverband waarin zorg- en strafpartners en gemeenten, onder eenduidige regie, werken aan complexe zorg- en veiligheidsproblemen. De doelstelling van de samenwerking is bijdragen aan de algemene veiligheid, het verbeteren van de persoonlijke situatie, het voorkomen en verminderen van recidive, (ernstige) overlast, criminaliteit en/of maatschappelijke uitval. Dit gebeurt door een combinatie van repressie, bestuurlijke interventies en zorg, hetgeen moet worden gezien als een zwaarwegend algemeen belang.

2.2 Om het onder 2.1 geformuleerde doel te bereiken heeft het zorg- en veiligheidshuis drie functies:
   a) Het faciliteren en regisseren van Casusoverleggen waar complexe casuïstiek wordt besproken;
   b) Het functioneren als expertisecentrum voor multidisciplinaire zorg- en veiligheidsproblematiek en vraagbaak voor ketenpartners en professionals;
   c) Het signaleren van relevante trends en ontwikkelingen en (strategisch adviseren van sleutelpartners.

2.3 Daarnaast heeft het Zorg- en Veiligheidshuis een functie tot het behandelen van casuïstiek op de gebieden:
   a) Nazorg Jeugd
   b) Nazorg ex-gedetineerden
   c) Aanpak High Impact Crime
   d) Aanpak huiselijk geweld, stalking en kindermishandeling
   e) Aanpak radicalisering
   f) (Multi Disciplinaire Overleggen ten behoeve van) Wijkrechtspraak op Zuid

2.4 De onder 2.3 genoemde overleggen behoeven hun eigen privacy protocol waarin minimaal wordt beschreven wat de doelstelling is van deze overleggen en waar deze overleggen afwijken van het privacy protocol van het ZVHRR.

Artikel 3. Structuur Zorg- en Veiligheidshuis

3.1. Het Zorg- en Veiligheidshuis kent de volgende structuur:
   a. Het Dagelijks Bestuur
   b. Het Algemeen Bestuur;
   c. Het Breed MT;
   d. Het hoofd;
   e. De procesregisseur;
   f. Het casusoverleg;
   g. De casusregisseur;
   h. Ondersteunend personeel.

Artikel 4. Het Dagelijks Bestuur

4.1 Het Zorg- en Veiligheidshuis heeft een dagelijks bestuur. Het Dagelijks Bestuur (DB) richt zich op beheersmatige zaken en heeft een voorbereidende rol bij inhoudelijke strategie.

4.2 Het DB is bestuurlijk verantwoordelijk voor het bureau ZVHRR. In die hoedanigheid heeft het DB:
   - Mandaat voor besluitvorming over beheersmatige kwesties zoals huisvesting en zaken m.b.t. het bureau ZVHRR;

- Verantwoordelijkheid voor (kwaliteit van) functioneren van het Bureau ZVHRR;
- Een rol als sparringpartner en escalatieniveau voor het hoofd van het bureau ZVHRR.

4.3 Het DB bereidt de begroting en financiële verantwoording voor ten behoeve van de besluitvorming in het Algemeen Bestuur (AB).

4.4 Het DB heeft een inhoudelijke betrokkenheid; inhoudelijk voorbereidende rol in agendering AB, jaarprogramma met strategische agenda.

4.5 Het DB komt 4x per jaar bijeen.

4.6 Dit DB bestaat uit:

- Wethouder gemeente Rotterdam (gedelegeerd voorzitter namens burgemeester) & Burgemeester regiogemeente namens de bestuurlijke keten/het sociaal domein
- Politie, Reclassering & OM (vice-voorzitter) namens de justitieketen
- Een zorgpartij als agendalid[1], namens de zorgpartijen, om daarmee de verbinding tussen Zorg en Veiligheid te waarborgen.
- Hoofd Zorg- en Veiligheidshuis, dagelijks leidinggevende ZVHRR, secretaris ZVHRR

4.7 Vergaderingen van het DB zijn niet openbaar.

Artikel 5. Algemeen Bestuur

5.1. Het Zorg- en Veiligheidshuis heeft een Algemeen Bestuur. Het Algemeen Bestuur is verantwoordelijk voor de Strategische Regie van het Zorg- en Veiligheidshuis;

5.2. Het Algemeen Bestuur komt ten minste 2x per jaar bij elkaar. De vergaderingen van het Algemeen Bestuur vinden in beginsel plaats op locatie van het Zorg- en Veiligheidshuis.

5.3. Het Algemeen Bestuur bestaat uit vertegenwoordigers van een aantal partijen, te weten:

- Wethouder Zorg gemeente Rotterdam (gedelegeerd voorzitter namens burgemeester Rotterdam)
- Burgemeester regiogemeente namens de bestuurlijke keten/het sociaal domein
- Politie, Reclassering & OM (vice-voorzitter) namens de justitieketen
- Betrokken zorgpartijen. Deze aansluiting wordt ook doorgetrokken naar deelname op tactisch niveau aan het Breed MT.
- Bestuurlijke vertegenwoordiging vanuit de DVO's Oost, Noord en Zuid West
- Twee wethouders Zorg uit de regio
- Directeuren Halt, Raad voor de Kinderbescherming, Jeugdbescherming Rotterdam Rijnmond, Veilig Thuis
- Directeuren Directie Veiligheid en Maatschappelijke Ontwikkeling Gemeente Rotterdam
- Hoofd Zorg- en Veiligheidshuis, dagelijks leidinggevende Zorg- en Veiligheidshuis, secretaris Zorg- en Veiligheidshuis.
- Agendalid[2]: Raad voor de Rechtspraak, Dienst Justitiële Inrichtingen, Slachtofferhulp, en de directeur William Schrikker Stichting.

5.4. Het Algemeen Bestuur is verantwoordelijk voor het in het kader van de Strategische Regie opstellen van operationele en beleidsmatige kaders voor de opdracht van het Zorg- en Veiligheidshuis in de vorm van een Jaarplan, en beslist over eventueel bijstellen/afwijken van deze kaders. Jaarlijks stelt het Algemeen Bestuur in een Jaarplan een inhoudelijk en financieel beleid vast als opdracht voor het Zorg- en Veiligheidshuis. Dit Jaarplan bevat ten minste de volgende onderdelen:

a) Langetermijnvisie;
b) Prioriteiten voor het betreffende kalenderjaar;

- [1] De zorgpartij (in dit geval Antes) sluit aan als agendalid en neemt alleen deel aan de agendapunten/besprekingen die de voorbereidende rol van het DB in agendering AB, en het jaarprogramma met strategische agenda, betreffen.

[2] Agenda-lid houdt in dat deze partners de agenda krijgen van het regulier AB-overleg en op basis daarvan zelf bepalen wanneer zij willen aansluiten/ een bijdrage leveren/ een punt inbrengen.

c) Begroting en jaarrekening inclusief jaarverslag.

5.5. Het borgen van de kwaliteit van de samenwerking, de plannen van aanpak en de informatiebeveiliging en de evaluatie daarvan;
Het Algemeen Bestuur heeft daarnaast de volgende taken en bevoegdheden:
a. het Werkproces indien nodig op hoofdlijnen aanpassen;
b. besluiten met betrekking tot personeel nemen die het Zorg- en Veiligheidshuis aangaan;
c. besluiten omtrent toetreding van nieuwe organisaties tot dit Convenant.

5.6. De Gemeente(n) en het breed MT ontvangen het Jaarplan ter informatie uiterlijk *4* weken na vaststelling daarvan door het Algemeen Bestuur.

5.7. De secretaris van het Algemeen Bestuur is verantwoordelijk voor het organiseren van de vergaderingen, het samenstellen van de agenda op basis van inbreng vanuit het breed MT en de leden van het Algemeen Bestuur en het opstellen en verspreiden van het verslag van de betreffende vergadering.

Artikel 6. Besluitvorming Algemeen Bestuur

6.1. Het Algemeen Bestuur neemt besluiten over de Strategische Regie in het Zorg- en Veiligheidshuis. Incidentele strategische besluiten komen toe aan het Breed MT.

6.2. Voorafgaand aan het nemen van besluiten vraagt het Algemeen Bestuur om inbreng van partijen.

6.3. Het Algemeen Bestuur houdt bij het nemen van besluiten rekening met de uitkomsten van de overleggen van de Landelijke Stuurgroep Zorg en Veiligheid.

6.4. Besluiten worden genomen met een meerderheid van stemmen en zijn bindend voor alle Partijen die aan dit Convenant deelnemen, voor zover niet strijdig met de wettelijke taken, bevoegdheden en beroepsnormen van partijen. Er wordt gestreefd naar consensus.

6.5. Bij afwezigheid van een lid van het Algemeen Bestuur wordt die Partij verzocht schriftelijk inbreng te leveren rondom de geagendeerde besluiten. Zonder schriftelijke inbreng worden besluiten die deze partij in belangrijke mate kunnen treffen niet genomen, tot die Partij gehoord is.

6.6. Indien het Algemeen Bestuur niet tot een besluit kan komen, wordt de aangelegenheid ter beslissing voorgelegd aan het Dagelijks Bestuur. Dat geldt ook voor gevallen waarin een verhoging van de financiële of personele bijdrage van partijen of beperking van de dienstverlening van het Zorg- en Veiligheidshuis aan de orde is. De Voorzitter kan besluiten de Colleges van Burgemeesters en Wethouders en andere Partijen hiervoor te benaderen. Voor het overige wordt het Algemeen Bestuur door de bevoegde gezagen gemandateerd om besluiten te nemen. De secretaris van het Algemeen Bestuur informeert het Breed Management Team schriftelijk over de in het Algemeen Bestuur genomen besluiten.

6.7. De vergaderingen van het Algemeen Bestuur zijn niet openbaar.

Artikel 7. Het Breed MT

7.1. Partijen in het Zorg- en Veiligheidshuis voeren ter uitvoering van de in artikel 2 bepaalde doeleinden onderling overleg op tactisch niveau: het 'Breed MT'.

7.2. Het Breed MT vindt plaats voorafgaand aan het AB.
Het Breed MT bestaat uit managers op tactisch niveau van de aangesloten partners, het hoofd Zorg- en Veiligheidshuis, dagelijks leidinggevende ZVHRR, secretaris ZVHRR

7.3. De afgevaardigden van Partijen hebben het mandaat of de machtiging om op tactisch niveau sturing te geven aan de operationele processen van het Zorg- en Veiligheidshuis en besluiten te nemen met betrekking tot uitvoering van de onder Artikel 7.5 geformuleerde taken.

7.4 De gemeenten laten zich gezamenlijk vertegenwoordigen door één gemeentelijke afgevaardigde per Districtelijk Veiligheids Overleg (DVO), die door de afzonderlijke gemeenten is gemandateerd om namens hen inbreng te leveren en gemachtigd om besluiten te nemen in het Breed MT. Bestaande taken en verantwoordelijkheden van de vertegenwoordigde gemeenten blijven onverlet. In navolging van de Algemene Verordening Gegevensbescherming kan de verwerkingsverantwoordelijkheid voor de verwerking van persoonsgegevens niet worden gemandateerd of gedelegeerd.

7.5 Het Breed MT heeft de volgende taken:
a) Op tactisch niveau sturing geven aan de operationele processen van het Zorg- en Veiligheidshuis;

b) Formuleren van voorstellen en vragen ten behoeve van of ter besluitvorming in het Algemeen Bestuur;
c) In samenwerking met het hoofdopstellen van het operationele Werkproces. Een kopie van het door het Breed MT vastgestelde Werkproces wordt aan alle Partijen verstrekt;
d) Het afstemmen van externe communicaties.

7.6 De secretaris van het Breed MT is verantwoordelijk voor het organiseren van de vergaderingen, het samenstellen van de agenda op basis van inbreng vanuit het Algemeen Bestuur en de leden van het Breed MT en het opstellen en verspreiden van het verslag van de betreffende vergadering, alsook het informeren van het Dagelijks Bestuur, het Algemeen Bestuur over de in het Breed MT genomen relevante besluiten.

Artikel 8. Besluitvorming Breed MT

8.1. Besluiten in het Breed MT worden genomen met een meerderheid van stemmen en zijn bindend voor alle partijen die deelnemen aan dit Convenant, voor zover niet strijdig met de wettelijke taken, bevoegdheden en beroepsnormen van Partijen. Er wordt gestreefd naar consensus.
8.2. Bij afwezigheid van een lid van het Breed MT wordt die partij verzocht schriftelijk inbreng te leveren rondom de geagendeerde besluiten. Zonder schriftelijke inbreng worden besluiten die deze partij in belangrijke mate kunnen treffen niet genomen, tot die partij gehoord is.
8.3. Indien het Breed MT niet tot een besluit kan komen, wordt de aangelegenheid ter beslissing voorgelegd aan het Algemeen Bestuur.
8.4. De secretaris van het Breed MT informeert het Algemeen Bestuur schriftelijk over de in het Breed MT genomen relevante besluiten.
8.5. De vergaderingen van het Breed MT zijn niet openbaar.

Artikel 9. Het Casusoverleg

9.1. Partijen in het Zorg- en Veiligheidshuis voeren ter uitvoering van de in artikel 2 bepaalde doeleinden onderling overleg op operationeel niveau in het 'casusoverleg'. Het casusoverleg vindt plaats wanneer op basis van Triage wordt besloten een casus in het casusoverleg te bespreken.
9.2. Het casusoverleg bestaat uit afgevaardigden van partijen, aangewezen door de Procesregisseur conform Artikel 13.
9.3. De afgevaardigden van partijen hebben het mandaat om op operationeel niveau besluiten te nemen over de behandeling van een casus. Dit mandaat wordt begrensd door de standaarden voor behoorlijke besluitvorming die gelden in de eigen organisatie.
9.4. Het casusoverleg heeft de volgende taken:
    a. Het aanwijzen van een casusregisseur;
    b. Opstellen van een integraal plan van aanpak;
    c. Komen tot inhoudelijke afspraken in onderlinge samenhang voor de behandeling van de casus, waaronder in ieder geval het bepalen van de rol en informatiebehoefte van iedere betrokken partij om uitvoering te kunnen geven aan het plan van aanpak;
    d. Het bepalen van de criteria voor afschaling, alsook het nemen van besluiten hieromtrent.
9.5. Partijen geven ieder met het oog op hun eigen wettelijke taken en bevoegdheden uitvoering aan de uitkomsten van het casusoverleg, in het bijzonder voor wat betreft de uitwisseling van informatie en de uitvoering van het plan van aanpak zoals vastgesteld op grond van artikel 9.4, onder b.
9.6. De casusregisseur stemt waar nodig af met de procesregisseur voor wat betreft de uitvoering van de onder artikel 9.4 genoemde taken.

Artikel 10. Afspraken Casusoverleg

10.1. In het casusoverleg worden in gezamenlijkheid afspraken gemaakt.
10.2. De vergaderingen van het casusoverleg zijn niet openbaar.
10.3. Informatieverstrekking aan derden omtrent hetgeen wordt besproken in het casusoverleg vindt slechts plaats conform het Convenant, binnen de voor partijen geldende wettelijke kaders en slechts na voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke zoals bedoeld in dit

convenant, die de betreffende informatie oorspronkelijk aan het samenwerkingsverband heeft verstrekt .

Artikel 11. Contactpersonen

11.1. De afgevaardigden in het Breed MT, het Algemeen Bestuur en het casusoverleg fungeren tevens als contactpersoon voor de secretaris van het Algemeen Bestuur c.q. het Breed MT, het hoofd van het Zorg- en Veiligheidshuis, de procesregisseur en indien van toepassing, de casusregisseur.

Artikel 12. Hoofd ZVHRR

12.1. Het Dagelijks Bestuur van het Zorg- en Veiligheidshuis is belegd bij het hoofd van het Zorg- en Veiligheidshuis (het hoofd).

12.2. Het hoofd wordt aangewezen door het Algemeen Bestuur en valt onder de verantwoordelijkheid van de Gemeente Rotterdam.

12.3. Het hoofd heeft de volgende taken en bevoegdheden:

a. Het vaststellen van de operationele werkprocessen in afstemming met het Breed MT;
b. Het toezicht op de naleving en uitvoering van het Jaarplan;
c. het laten opstellen van jaarverslagen;
d. Het informeren van het Dagelijks Bestuur en Algemeen Bestuur omtrent de voortgang van de samenwerking in het Zorg- en Veiligheidshuis door partijen met het oog op het Jaarplan door het opstellen van een jaarlijkse rapportage met aantallen casussen die zijn behandeld, aantallen casussen die succesvol zijn afgerond, overzicht van uitgaven en overige aandachtspunten;
e. Optreden als woordvoerder voor het Zorg- en Veiligheidshuis in overleg met het Breed MT;
f. het hoofd draagt zorg voor de verbinding tussen de deelnemende partijen.

12.4. Voor zaken die tevens onder de verantwoordelijkheid vallen van het DB draagt het hoofd zorg voor de afstemming met het DB.

12.5. Geschillen omtrent de uitvoering van de taken van het hoofd worden voorgelegd aan het dagelijks bestuur. Het dagelijks bestuur adviseert het algemeen bestuur over de afhandeling van het geschil.

Artikel 13. Procesregisseur

13.1. De Procesregisseur is bevoegd en verantwoordelijk voor de procesregie binnen het Zorg- en Veiligheidshuis.

13.2. De Procesregisseur is belast met de volgende taken:

a. Het beoordelen van een casus op geschiktheid voor behandeling in het casusoverleg na aanmelding/intake. Deze beoordeling geschiedt in overleg met de partij die de casus bij de procesregisseur heeft aangedragen;
b. Het faciliteren van de triage ten behoeve van de partij die een casus aanmeldt in het Zorg- en Veiligheidshuis;
c. Het voorbereiden van het casusoverleg, waaronder in ieder geval het zo concreet mogelijk bepalen van het doel van het casusoverleg, het bepalen van het type besluiten dat in het casusoverleg dient te worden genomen en het bepalen van de relevante gesprekstheme's voor het casusoverleg;
d. Het op basis van de onder a. genoemde beoordeling agenderen van een casus in het casusoverleg;
e. Het organiseren van de casusoverleggen, waaronder het aanwijzen van partijen die worden uitgenodigd deel te nemen aan een casusoverleg en het bepalen van de van hen gevraagde inhoudelijke bijdrage aan dat casusoverleg. Alleen die partijen worden uitgenodigd die rechtmatig bij het overleg aanwezig mogen zijn;
f. Het beoordelen of, en zo ja welke informatie voorafgaand aan het casusoverleg door deelnemers aan het casusoverleg kan worden ingezien. Deze beoordeling geschiedt in overleg met de partij die de casus bij het Zorg- en Veiligheidshuis heeft aangemeld of de casusregie heeft, en uitsluitend als de partij die de gegevens heeft verstrekt dat accordeert;
g. Het ondersteunen van de casusregisseur, waaronder het toezien op de naleving van de uitvoering van het in het casusoverleg vastgestelde plan van aanpak door Partijen;
h. Het toezien op de naleving van het vastgestelde werkproces door partijen tijdens het casusoverleg;

13.3. De procesregisseur werkt voor wat betreft de taken genoemd onder artikel 13.2 a tot en met g namens de partij die een casus aanmeldt of de casusregie voert. De procesregisseur werkt voor wat betreft de taak genoemd in artikel 13.2, onder h, onder de gezamenlijke verantwoordelijkheid van partijen.
13.4. Geschillen omtrent het functioneren van de procesregisseur worden voorgelegd aan het hoofd. Het hoofd kan het geschil waar nodig voorleggen aan het Breed MT.

Artikel 14. Casusregisseur

14.1. Conform artikel 9.4, onder a, kan in het casusoverleg een casusregisseur worden aangewezen. De casusregisseur werkt onder de verantwoordelijkheid van de partij tot wie deze behoort. De casusregisseur is doorgaans afkomstig uit de organisatie waar het zwaartepunt van de zorgverlening aan de betreffende betrokkene ligt.
14.2. De casusregisseur is belast met het toezicht op de naleving van de afspraken zoals die zijn vastgelegd in het plan van aanpak.
14.3. De casusregisseur stemt af met de procesregisseur voor wat betreft de voortgang van het Plan van Aanpak
14.4. Geschillen omtrent de uitvoering van taken door een casusregisseur worden voorgelegd aan de procesregisseur. Deze kan, indien noodzakelijk en na afstemming met de leidinggevende van de casusregisseur, het geschil ter beslechting voorleggen aan de betrokken Breed MT-leden.

Artikel 15. Ondersteunend Personeel

15.1. Het Zorg- en Veiligheidshuis wordt ondersteund door één of meerdere procesregisseurs met de verantwoordelijkheden als beschreven onder artikel 13. Het Algemeen Bestuur draagt zorg voor voldoende bezetting van het team procesregie in het Zorg- en Veiligheidshuis. Dit personeel werkt arbeidsrechtelijk onder de verantwoordelijkheid van de gemeente Rotterdam voor zover het personeel ook daadwerkelijk in dienst is van de gemeente Rotterdam.

15.2. Het Zorg- en Veiligheidshuis wordt ondersteund door één- of meerdere administratieve ondersteuners. Deze administratieve ondersteuners voeren ondersteunende werkzaamheden uit ten behoeve van de casus overleggen en de processen binnen het Zorg- en Veiligheidshuis. Hieronder valt het onder andere, maar niet uitsluitend, de ondersteuning bij het plannen van overleggen, het notuleren van de overleggen, ondersteunen bij de administratieve afhandeling van de overleggen, het ondersteunen van de afhandeling van verzoeken en vragen van burgers. Het Algemeen Bestuur draagt zorg voor voldoende bezetting van het team administratieve ondersteuning in het Zorg- en Veiligheidshuis. Dit personeel werkt onder de verantwoordelijkheid van de gemeente Rotterdam.
15.3. Het Zorg- en Veiligheidshuis wordt ondersteund door één- of meerdere stafmedewerkers. Deze stafmedewerkers voeren werkzaamheden uit ten behoeve van de kwaliteit en compliance van de werkzaamheden op het Zorg- en Veiligheidshuis. Onder dit team valt in elk geval:
    a. Één of meerdere stafmedewerkers die o.a. werkzaamheden verrichten op het gebied van (functioneel) beheer en de verantwoordelijkheden hebben bij het ordentelijk toekennen, controleren en beheren van autorisaties en toegangsrechten.
    b. Één of meerdere stafmedewerkers die o.a. werkzaamheden verrichten ten behoeve van de kwaliteit van de werkprocessen, de (rechtmatige) invulling hiervan en de scholing van (externe)medewerkers binnen het Zorg- en Veiligheidshuis om de werkprocessen gericht op het kwalitatief en rechtmatig uitvoeren van de werkzaamheden.
    c. Één of meerdere stafmedewerkers die o.a. werkzaamheden verrichten op het gebied van data-analyse zodat het Zorg- en Veiligheidshuis o.a. (maar niet uitsluitend) kan monitoren of het Zorg- en Veiligheidshuis binnen haar doelstellingen blijft en haar doelstellingen effectief uitvoert.
    d. Één privacy officier die onder andere maar niet uitsluitend verantwoordelijk is voor het monitoren op de compliance met de AVG (samen met de werkgroep privacy), het gevraagd en ongevraagd adviseren van het management op vraagstukken die de privacy van de cliënten van het Zorg- en Veiligheidshuis raken, het uitvoeren van DPIA's (samen met de werkgroep privacy), het voorbereiden van samenwerkingsconvenanten en het coördineren van AVG-verzoeken van burgers.

15.4. De Gemeente Rotterdam draagt zorg voor voldoende bezetting van het team administratieve ondersteuning in het Zorg- en Veiligheidshuis. Dit personeel werkt onder de verantwoordelijkheid van de gemeente Rotterdam.
15.5. Het hoofd kan, buiten het inzetten van personeel dat in loondienst is bij de ketenpartners/deelnemende partij(en), besluiten personeel op grond van een dienstverleningsovereenkomst in te zetten.
15.6. De dagelijkse aansturing van het personeel gebeurt door de dagelijks leidinggevende(n).

Artikel 16. Uitwisseling van informatie

16.1. Partijen voorzien elkaar van alle noodzakelijke informatie voor het behalen van de doelstellingen van het Zorg- en Veiligheidshuis zoals beschreven in artikel 2 en het uitvoeren van hun respectievelijke taken zoals beschreven in dit Convenant, voor zover wettelijk mogelijk. Partijen zijn ieder zelf verantwoordelijk voor het verstrekken van informatie in het Zorg- en Veiligheidshuis. Verder gebruik van die informatie geschiedt onder gezamenlijke verantwoordelijkheid van partijen, slechts voor zover volgens geldende wet- en regelgeving is geoorloofd en met inachtneming van artikel 17, lid 2.
16.2. Voor zover het de verwerking van persoonsgegevens, waaronder (bijzondere) persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming, de Wet justitiële en strafvorderlijke gegevens of de Wet politiegegevens betreft, handelen partijen overeenkomstig het Privacy Protocol, in het bijzonder voor wat betreft de daarin vastgelegde doeleinden en grondslagen voor die verwerking.

Artikel 17. Interventie en het gebruik van informatie

17.1. Partijen behouden hun eigen bevoegdheden met betrekking tot de in het Zorg- en Veiligheidshuis besproken casussen. Afzonderlijk optreden op basis van eigen informatie blijft door samenwerking in het Zorg- en Veiligheidshuis onverlet. Desalniettemin streven partijen naar een zo gezamenlijk mogelijke behandeling van een casus waar noodzakelijk voor het bewerkstelligen van de in artikel 2 geformuleerde doeleinden.
17.2. De partij die de informatie verstrekt bepaalt op welke wijze de informatie door de overige partijen mag worden gebruikt, behoudens hetgeen hierover omtrent de verwerking van persoonsgegevens is bepaald in het Privacy Protocol Integrale Veiligheid en Complexe. Partijen verklaren dat Privacy Protocol te onderschrijven en daarnaar in het kader van samenwerking in het Zorg- en Veiligheidshuis te zullen handelen.

Artikel 18. Geheimhouding en beveiliging

18.1. Partijen nemen conform de toepasselijke wettelijke bepalingen en ongeacht de duur van dit Convenant strikte geheimhouding in acht over elkaars organisatie, over alle informatie die ten behoeve van de uitvoering van dit Convenant bij en/of tussen partijen bekend wordt en vertrouwelijk is, dan wel waarvan mag worden aangenomen dat deze vertrouwelijk is, dan wel persoonsgegevens die worden uitgewisseld, alsmede over al hetgeen waarvan redelijkerwijs is aan te nemen dat bekendmaking daarvan de belangen van de andere Partijen, het privacybelang van de betreffende burger(s) of het algemene maatschappelijk belang zou schaden, voor zover deze informatie niet al openbare informatie betreft als gevolg van openbaarmaking door één of meer der partijen, dan wel anderszins bekend is geworden bij het publiek, behoudens wettelijke verplichtingen en hetgeen is bepaald in Artikel 10.2 en Artikel 16.
18.2. Partijen staan ervoor in dat hun personeel bekend is met de in dit artikel vastgestelde verplichting en de naleving hiervan nakomen.
18.3. Partijen nemen ieder voor zich adequate technische en organisatorische maatregelen om informatie te beschermen tegen verlies of onrechtmatige verwerking, waaronder ten minste het bewaren, verstrekken, verzenden en archiveren van informatie. Voor informatiebeveiliging in het Zorg- en Veiligheidshuis wordt zorg gedragen door de gemeente Rotterdam, conform het Informatiebeveiligingsbeleid Zorg- en Veiligheidshuis Rotterdam-Rijnmond, meegeleverd in bijvoegsel 6. Gemeente Rotterdam, stelt de benodigde middelen ter beschikking voor de uitvoering van dat Informatiebeveiligingsbeleid door het Zorg- en Veiligheidshuis.

Artikel 19. Financiering en overige bijdragen

19.1. Partijen zijn ieder voor zich verantwoordelijk voor het dragen van financiële lasten voor deelname in het Zorg- en Veiligheidshuis in het kader van dit Convenant die niet worden gedekt door de Rijksbijdragen of bijdrage van de Gemeente(n), waaronder in ieder geval het leveren van een afgevaardigde voor het Breed MT, het Algemeen Bestuur en de Casusregisseur en eventuele reis- en verblijfkosten voor die afgevaardigden.

19.2. Het hoofd houdt toezicht op de financiële huishouding van het Zorg- en Veiligheidshuis en rapporteert hierover aan het Algemeen Bestuur.

Artikel 20. Communicatie

20.1. Partijen communiceren niet afzonderlijk naar derden over de samenwerking in het Zorg- en Veiligheidshuis in het kader van de uitvoering van dit Convenant, zonder voorafgaande instemming van de andere partijen en met inachtneming van het bepaalde in Artikel 10.2 en Artikel 16.

20.2. Het hoofd ziet toe op het coördineren van communicatie naar derden en treedt op als woordvoerder voor het Zorg- en Veiligheidshuis.

Artikel 21. Toetreding

21.1. Dit Convenant staat open voor toetreding door andere organisaties die binnen de kaders van hun publieke en/of maatschappelijke taak een bijdrage kunnen leveren aan de in Artikel 2 geformuleerde doeleinden.

21.2. Een organisatie die tot dit Convenant wil toetreden kan daartoe een aanvraag doen bij één van de leden van het Algemeen Bestuur/het MDO/de Partijen.

21.3. Partijen worden vooraf door de secretaris van het Algemeen Bestuur op de hoogte gebracht van de voorgenomen toetreding.

21.4. Het Algemeen Bestuur beslist op het verzoek van toetreding na akkoord te hebben verkregen van alle Partijen. In geval van goedkeuring, vindt toetreding tot het Convenant plaats door middel van ondertekening van Bijvoegsel 1 bij dit Convenant door die andere organisatie en de voorzitter van het Algemeen Bestuur.

Artikel 22. Wijzigingen

22.1. De bepalingen in dit Convenant kunnen door de Partijen in gezamenlijk overleg worden gewijzigd. Wijzigingen in dit Convenant worden door het Algemeen Bestuur besloten. Mondelinge mededelingen, toezeggingen of afspraken welke betrekking hebben op de inhoud van dit Convenant, hebben geen rechtskracht, tenzij deze uitdrukkelijk schriftelijk zijn bevestigd door het Algemeen Bestuur.

22.2. Wijziging van het Convenant vergt het opnieuw ondertekenen door Partijen van het gewijzigde Convenant.

22.3. In geval van wijzigingen, waaronder inbegrepen toetreding van een nieuwe organisatie tot het Convenant, die door een Partij onaanvaardbaar worden ervaren, kan deze Partij deelname aan het Zorg- en Veiligheidshuis schriftelijk opzeggen met ingang van het tijdstip waarop het gewijzigde Convenant van kracht wordt.

Artikel 23. Aansprakelijkheid

23.1. Partijen zetten zich in voor een goede uitvoering van het bepaalde in dit convenant en zullen zich houden aan de dienaangaande in dit convenant gemaakte afspraken.

23.2. Partijen zijn ieder voor zich aansprakelijk voor aanspraken van 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 convenant en de bijbehorende bijlagen.

23.3. 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.

23.4. 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.

23.5. 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 24. Duur, opzegging, beëindiging

24.1. Dit Convenant treedt in werking op de dag van ondertekening door partijen en wordt tenminste aangegaan voor een periode van 3 jaar, waarna het Convenant automatisch iedere keer met een periode van één jaar wordt verlengd, behoudens schriftelijke opzegging door Partijen.

24.2. Het Algemeen Bestuur kan, zonder rechterlijke tussenkomst en met meerderheid van stemmen, na ingebrekestelling, een partij met onmiddellijke ingang uitsluiten van de samenwerking in het Zorg- en Veiligheidshuis, indien de afspraken zoals neergelegd in dit Convenant niet door de desbetreffende Partij worden nagekomen.

24.3. Verplichtingen die naar hun aard zijn bestemd om ook na beëindiging of uitsluiting van het project voort te duren, blijven na beëindigingen van dit Convenant bestaan. Tot deze verplichtingen behoren onder meer die ter zake van geheimhouding.

Artikel 25. Opvolging

25.1. Dit Convenant vervangt alle eerdere door Partijen gesloten Convenanten met betrekking tot samenwerking in het Zorg- en Veiligheidshuis.

Artikel 26. Toepasselijk recht

26.1. Op dit Convenant is Nederlands recht van toepassing.

Privacy Protocol: Zorg- en Veiligheidshuis Rotterdam Rijnmond

Privacy Protocol tussen ketenpartners Zorg- en Veiligheidshuis Rotterdam-Rijnmond

De ondergetekenden: **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 het Zorg- en Veiligheidshuis Rotterdam-Rijnmond (hierna: 'het Zorg- en Veiligheidshuis') hebben opgezet;
- Partijen voor deze samenwerking afspraken hebben vastgelegd in het Convenant 'Samenwerking tussen ketenpartners in Zorg- en Veiligheidshuis Rotterdam-Rijnmond, gesloten op 28-02-2024, (verder: het Convenant), waar dit privacy protocol deel van uitmaakt;
- voor de samenwerking in het Zorg- en Veiligheidshuis de uitwisseling van gegevens, waaronder persoonsgegevens, tussen de partijen noodzakelijk is;
- in het door partijen opgezette Zorg- en Veiligheidshuis persoonsgegevens worden verwerkt ten dienste en onder verantwoordelijkheid van partijen;
- partijen slechts die persoonsgegevens binnen het Zorg- en Veiligheidshuis delen die noodzakelijk zijn voor het doel van de samenwerking;
- op de samenwerking wet-en regelgeving met betrekking tot de bescherming van persoonsgegevens van toepassing is waarbij partijen conform deze wet- en regelgeving willen samenwerken;
- dit privacyprotocol (verder aangeduid als: 'het protocol') de gedragsregels omschrijft bij het verstrekken en verder verwerken van persoonsgegevens door partijen in het kader van de samenwerking op het gebied van integrale veiligheid en complexe multi-problematiek, alsook de verschillende verantwoordelijkheden met het oog op de rechten en plichten uit toepasselijke privacy wet- en regelgeving, belegd;
- met dit protocol reeds invulling wordt gegeven aan de in Artikel 26 van de Europese Algemene Verordening Gegevensbescherming neergelegde verplichting voor partijen om op een transparante wijze hun samenwerkingsafspraken en hun verantwoordelijkheden jegens elkaar en jegens betrokkene vast te leggen;
- dit protocol aansluit bij het bepaalde in het 'Landelijk Kader Veiligheidshuizen' van het Ministerie van Veiligheid en Justitie, vastgesteld in januari 2013 (verder aangeduid als: 'het Landelijk Kader') en het 'Handvat Gegevensuitwisseling in het zorg en veiligheidsdomein – een juridisch handvat voor Zorg- en Veiligheidshuizen', versie 2.3. van juli 2020, (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 uitvoering 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 strafvorderlijk 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 strafvordering, die in een bestand worden Verwerkt (artikel 1 sub a Wjsg, respectievelijk Bjsg);

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 verwerkings-verantwoordelijkheid 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 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 artikel 2 van het convenant, en die is aangemeld bij het Zorg- en Veiligheidshuis ter beoordeling en eventuele bespreking in het casusoverleg;

1.18. Aanmelding en Intake: het voordragen van een casus door één der partijen en het uitwisselen van informatie, waaronder persoonsgegevens, tussen de procesregisseur van het Zorg- en Veiligheidshuis en de aanmeldende partij ter toetsing of de casus in aanmerking komt voor behandeling in het Zorg- en Veiligheidshuis;
1.19. Triage: het proces waarbij relevante partijen worden bevraagd om te komen tot een nadere afweging ten aanzien van de routering van de casus, tot een bepaling van het doel en de thema's van een eventueel casusoverleg, en tot een afweging welke partijen relevant zijn om te betrekken bij een casusoverleg;
1.20. Casusoverleg: fase waarin overleg plaats vindt door partijen gericht op de totstandkoming van een plan van aanpak, afstemming tijdens de uitvoering daarvan, en het beoordelen of casus kan worden afgeschaald;
1.21. Afschaling: fase die volgt op het besluit in het casusoverleg dat de betrokkenheid van het Zorg- en Veiligheidshuis niet langer nodig is, waarin het dossier dat in het systeem van het Zorg- en Veiligheidshuis is aangelegd ten behoeve van procesregie, geschoond wordt van alle niet langer noodzakelijke informatie, en uiteindelijk verdwijnt uit het systeem van het Zorg- en Veiligheidshuis;
1.22. Procesregisseur: de medewerker van het zorg- veiligheidshuis die namens een van de partijen is belast met de werkzaamheden in artikel 13 van het convenant;
1.23. Casusregisseur: de medewerker van een van de partijen die is belast met de taken in artikel 14 van het convenant;
1.24. Hoofd: de persoon die is belast met de taken zoals geformuleerd in Artikel 12 van het convenant;
1.25. Algemeen Bestuur: het verband van afgevaardigden van partijen zoals geformuleerd in Artikel 5 van het Convenant;
1.26. Privacyadviseur: Ieder Zorg- en Veiligheidshuis heeft een medewerker die belast is met privacyadvisering of kan gebruik maken van een privacyadviseur van een gemeente. Deze persoon is ook belast met beleidsontwikkeling over gegevensverwerking en helpt mee met de voorbereiding van audits;
1.27. De privacy-werkgroep: Een werkgroep bestaande uit privacy deskundigen van de deelnemende organisaties voor zover deze organisaties een deskundigen voor deelname aan de werkgroep hebben aangemeld.
1.28. Jaarplan: het door AB op grond van Artikel 5.4 van het convenant vastgestelde plan betreffende de operationele en inhoudelijke kaders en het financieel en inhoudelijk beleid van het Zorg- en Veiligheidshuis;
1.29. Werkprocessen: de door het Breed MT op grond van artikel 7 van het convenant vastgestelde processen voor samenwerking in het Zorg- en Veiligheidshuis, waaronder het proces omtrent en het delen van informatie en het afschalen van een casus;
1.30. 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 strafvordelijke gegevens;
1.32. Bjsg: Besluit justitiële en strafvorderlijke gegevens;
1.33. Wpg: Wet politiegegevens.

Artikel 2. Afzonderlijke en Gezamenlijke Verwerkingsverantwoordelijken

2.1. Partijen in het Zorg- en Veiligheidshuis zijn afzonderlijk verwerkingsverantwoordelijke voor de persoonsgegevens die zij verstrekken aan de procesregisseur ten behoeve van de aanmelding en intake en aan partijen in het kader van triage, casusoverleg, en afschaling.
2.2. Partijen in het Zorg- en Veiligheidshuis zijn conform artikel 26 Algemene Verordening Gegevensbescherming gezamenlijk verwerkingsverantwoordelijken voor de persoonsgegevens die zij, anders dan de verstrekking zoals bedoeld in artikel 2.1, verwerken op locatie of in de informatiesystemen van het Zorg- en Veiligheidshuis in het kader van de samenwerking voor de doeleinden zoals omschreven in artikel 3.

2.3. Verwerking van persoonsgegevens in het Zorg- en Veiligheidshuis door personeel van het Zorg- en Veiligheidshuis geschiedt onder gezag van de partij die de betreffende persoonsgegevens heeft verstrekt. Deze partij wordt voor die verwerking aangeduid als verwerkingsverantwoordelijke.

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 2.3 van het convenant.

3.2. Het verwerken van persoonsgegevens in het Zorg- en Veiligheidshuis vindt plaats met als doel het gezamenlijk door partijen bijdragen aan de veiligheid als onderdeel van het integrale zorg- en veiligheidsbeleid van de gemeente(n). De samenwerking is meer specifiek gericht op het 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 Zorg- en 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 intake, triage, casusoverleg, en afschaling. Voor elk van deze fasen in het werkproces zijn specifieke doelen voor de verwerking van Persoonsgegevens in het Zorg- en Veiligheidshuis van toepassing. Deze doelen zijn gespecificeerd in artikel 2 van het Convenant.

3.4. Partijen verwerken de persoonsgegevens die zij in het kader van de samenwerking onder dit protocol hebben verkregen niet voor andere doeleinden dan de doelen omschreven in artikel 3.2.

3.5. Bij het verwerken van persoonsgegevens in het Zorg- en Veiligheidshuis worden de volgende uitgangspunten in acht genomen:

a. Er is sprake van een strikte doelbinding per fase 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 3 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 Zorg- en Veiligheidshuis, of in de door het AB aangewezen informatiesystemen en conform het concern informatiebeveiligingsbeleid van de gemeente Rotterdam.

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 13 van het Convenant valt.

5.1.3 Voor de verwerking van persoonsgegevens als bedoeld in artikel 5.1.1 zijn van toepassing de grondslag conform de AVG en/of andere wettelijke grondslag, en de wettelijke bepalingen op grond waarvan de aanmeldende partij, dan wel de partij onder wiens verantwoordelijkheid de casusregisseur valt, de casus heeft aangemeld respectievelijk de casusregie voert.

5.1.4 De verantwoordelijke voor de verwerking van persoonsgegevens zoals bedoeld in artikel 5.1.1 betreft de verantwoordelijke zoals bedoeld in artikel 2.2 van dit protocol.

5.2 Verstrekken van persoonsgegevens ten behoeve van aanmelding en intake, triage en casusoverleg

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, triage of casusoverleg worden uitgevoerd.

5.2.3 De grondslag conform de AVG voor het inbrengen van persoonsgegevens als bedoeld in artikel 5.2.1 wordt ontleend aan de eigen taak, en/of de taak van de partij ten behoeve waarvan de werkzaamheden in het kader van aanmelding en intake, triage of casusoverleg 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 casusoverleg

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 het casusoverleg zijn afgesproken
b. het voeren van de casusregie op het plan van aanpak als dat in het casusoverleg is afgesproken

c. 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 een casus en de van toepassing zijnde taken van partijen

6.1 De grondslag voor de verwerking van persoonsgegevens als bedoeld in artikel 5.1.1, is artikel 6 AVG lid 1 sub e, voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de aanmeldende partner, dan wel de partner onder wiens verantwoordelijkheid de casusregisseur valt. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens. 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 AVG lid 1 sub e, voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de aanmeldende partner, dan wel de partner onder wiens verantwoordelijkheid de casusregisseur valt, en/of de verstrekkende partij. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens. De grondslag voor het verstrekken van justitiële, strafvorderlijke en/of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.

6.3 De grondslag voor de verstrekking van persoonsgegevens als bedoeld in artikel 5.3.1, is artikel 6 AVG lid 1 sub e, voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de ontvangende partij en/of de verstrekkende partij. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens. De grondslag voor het verstrekken van justitiële, strafvorderlijke en/of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.

6.4 De onder 6.1, 6.2 en 6.3 bedoelde grondslag kan bij casussen slechts van toepassing zijn indien dit voortvloeit uit de goede uitvoering van de taken en werkzaamheden van partijen, en de verwerking plaats vindt namens of de verstrekking plaats vindt aan een van de onder a t/m m genoemde partijen en voorwaarden:

a. het bestuursorgaan de burgemeester: de goede uitvoering van taken en de uitoefening van bevoegdheden van de burgemeester, waaronder in het bijzonder taken en bevoegdheden op het gebied van Openbare Orde en Veiligheid zoals neergelegd in de Gemeentewet artikel 172.
b. het bestuursorgaan het College van Burgemeester &Wethouders: de goede uitvoering van taken van het College van Burgemeester &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 de wet schuldhulpverlening artikel 3.
c. het Openbaar Ministerie: voor de strafrechtelijke handhaving van de rechtsorde alsmede andere bij de wet vastgestelde taken (artikel 124 Wet op de Rechterlijke organisatie). 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 zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.

De grondslag voor het verstrekken van politiegegevens is gelegen in artikel 20 Wpg. Deze verstrekkingen dienen nader te zijn vastgelegd en is te relativeren aan een concreet doelbinding en thema in de onlosmakelijk bij dit Privacy-protocol behorende en ondertekende Artikel 20 Wpg Beslissingen. De Artikel 20 Beslissingen wordt ondertekend door de gemandateerde politiechef van de Eenheid en in overeenstemming met het bevoegd gezag.
In het kader van dit besluit mogen politiegegevens worden verstrekt die ingevolge de artikelen 8 en 13 van de Wpg worden verwerkt.
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 (BW), waaronder de artt. 1:238 BW, art. 1:240 BW, art. 1:241, art. 1:251a lid BW en de artt. 1:255 juncto 1:257 BW, de artt. 77 Sr tot en met 77gg van het Wetboek van Strafrecht, art. 494 jo. 498 Wetboek van Strafvordering (Sv), art. 810 Rechtsvordering (Rv), art. 3.1 van de Jeugdwet, art. 7.3.11 lid 4 van de Jeugdwet, art. 5van de wet Opneming Buitenlandse Kinderen ter Adoptie(wobka), 25 lid 2 sub 1 WOBKA. Met inachtneming van het Kwaliteitskader 2023 van de Raad voor de Kinderbescherming.
f. Veilig Thuis: de goede uitvoering van de taken van Veilig Thuis, waaronder in het bijzonder taken zoals bedoeld in de Wmo artikel 4.1.1, met inachtneming van nadere bepalingen in de Wmo en 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 geestelijke gezondheidszorg.
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 2 Kaderwet Overige J&V subsidies en artikel 51aa Wetboek van Strafvorderingen jo het Besluit slachtoffers van strafbare feiten artikel 1, 2 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. Doorverwerking geheimhoudingsbepalingen en toepassing toestemmingsvereiste

7.1 Ingevolge de Wet politiegegevens dragen alle ontvangers van politiegegevens op grond van artikel 7 Wpg een geheimhoudingsplicht. Dientengevolge is de ontvanger gehouden om maatregelen te nemen teneinde verstrekte politiegegevens niet ter kennis te doen komen van onbevoegden. Doorverstrekking van politiegegevens vindt slechts plaats voorzover wet- en regelgeving daartoe verplicht of voorzover de taak daartoe noodzaakt.

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 verkrijgen deze schriftelijk vast en informeert Betrokkene dat hij zijn toestemming altijd weer kan intrekken;
d. draagt de partij die toestemming heeft verkregen bij intrekking van die toestemming er zorg voor dat er geen verdere verstrekkingen meer plaats vinden;
e. maakt de betrokken zorg- of hulpverlener een eigen afweging conform de voor hem geldende professionele standaarden, indien toestemming niet verkregen wordt en hij ervan overtuigd is dat zich hier een conflict van plichten voordoet, of goed hulpverlenerschap het verstrekken van persoonsgegevens verlangd.

Artikel 8. Documentatie individuele verstrekkingen

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

Artikel 9. Dataminimalisatie

9.1 Partijen Verwerken niet meer persoonsgegevens dat noodzakelijk met het oog op de in artikel 2.1 van dit protocol geformuleerde doeleinden.

9.2 Ten behoeve van de Intake 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 Bijvoegsel 2 van het convenant. De procesregisseur registreert enkel die persoonsgegevens in het informatiesysteem van het Zorg- en Veiligheidshuis die noodzakelijk zijn voor triage.

9.3 In het casusoverleg 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 casusoverleg tot de gewenste resultaten heeft geleid. Indien wordt besloten dat behandeling van de casus in het Zorg- en Veiligheidshuis niet of niet langer noodzakelijk is, worden de betreffende persoonsgegevens niet langer in het Zorg- en Veiligheidshuis Verwerkt. *De procesregisseur* ziet erop toe dat persoonsgegevens conform artikel 11 worden geanonimiseerd of vernietigd.

9.5 Wanneer de partij die persoonsgegevens in het Zorg- en Veiligheidshuis heeft verstrekt, kennis verkrijgt over de onjuistheid van die persoonsgegevens, informeert die partij de casusregisseur en procesregisseur hierover. De procesregisseur coördineert de eventuele correctie van persoonsgegevens in het Zorg- en Veiligheidshuis.

9.6 Enkel de *procesregisseurs* hebben toegang tot de persoonsgegevens die worden verwerkt op locatie of in het informatiesysteem van het Zorg- en Veiligheidshuis en enkel voor zover noodzakelijk voor hun rol in een specifieke casus.

Artikel 10 Kwaliteit

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

Artikel 11 Bewaren en Vernietigen

11.1 Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor het doel of de doeleinden waarvoor ze worden Verwerkt zoals geformuleerd onder artikel 3 en met inachtneming van artikel 9.

11.2 Persoonsgegevens worden vernietigd zodra de Verwerking daarvan niet langer nodig is voor het doel waarvoor zij zijn Verwerkt, maar uiterlijk binnen *5 jaar na* de aanvang van de verwerking.

11.3 Persoonsgegevens kunnen enkel langer dan de in 11.2 genoemde termijn worden bewaard wanneer hierover door partners een gemotiveerd besluit is genomen en dit gemotiveerde besluit door de procesregisseur in het dossier is opgetekend.

11.4 De in 11.3 bedoelde verlenging kan telkens niet langer dan 2 jaar zijn. Na het verstrijken van deze 2 jaar moeten de partners telkens opnieuw komen met een gemotiveerd besluit en moet dit gemotiveerde besluit opgenomen worden in het dossier door de procesregisseur.

11.5 Tot de in 11.2 en 11.3 bedoelde verlenging kan enkel besloten worden wanneer de motivatie van dit besluit relatie heeft tot de in artikel 2 van het convenant genoemde doelstellingen van het Zorg- en Veiligheidshuis en wanneer partners in hun motivatie aannemelijk kunnen maken dat verlenging noodzakelijk is om deze doelstelling in een specifieke casus te bereiken of te borgen.

11.6 Op casuïstiek die binnen de termijn van 5 jaar wordt afgeschaald is onderstaand autorisatiebeleid van toepassing.

a. Persoonsgegevens blijven tot zes maanden na besluit tot afschaling toegankelijk voor de procesregisseur.
b. Na zes maanden na besluit tot afschaling tot 24 maanden na het besluit tot afschalen worden de rechten voor toegang tot het dossier ingetrokken. Toegang tot het dossier kan enkel hersteld worden wanneer er binnen 24 maanden na het besluit tot afschalen een nieuwe melding binnen komt met betrekking tot de burger op wie het dossier betrekking heeft.
c. Na 24 maanden tot het moment van vernietiging kan het dossier enkel nog geraadpleegd wanneer dit nodig is voor het afhandelen van verzoeken van de burger ten aanzien van zijn of haar persoonsgegevens en voor evaluatie- of onderzoeksdoeleinden wanneer er sprake is van een calamiteit of incident.

11.7 Na het verstrijken van de bewaartermijn bedoeld in artikel 11.1 t/m 11.5 kunnen gegevens, niet zijnde Persoonsgegevens, enkel worden bewaard voor managementdoeleinden.

11.8 Ten behoeve van de triage worden er ook persoonsgegevens verwerkt. Als tijdens de triage blijkt dat de casus NIET naar het ZVHRR door te geleiden dan mogen deze (persoons)gegevens die aan de beslissing ten grondslag hebben gelegen maximaal 1 jaar na deze beslissing worden bewaard om na dit jaar te worden vernietigd. De bewaarde gegevens mogen enkel en alleen worden gebruikt om de beslissing om de casus niet naar het ZVHRR door te geleiden te onderbouwen of het afhandelen van verzoeken van de burger ten aanzien van het gebruik van zijn of haar persoonsgegeven.

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 Bijvoegsel 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 Rotterdam draagt zorg voor de adequate beveiliging van persoonsgegevens die worden verwerkt op locatie en in de informatiesystemen van het Zorg- en Veiligheidshuis en rapporteert hierover aan het algemeen bestuur.

12.4 Het hoofd is verantwoordelijk voor het toezien op de naleving van de beschermingsmaatregelen zoals geformuleerd in concern informatiebeveiligingsbeleid van de gemeente Rotterdam voor de verwerking van persoonsgegevens op locatie en in de informatiesystemen van het Zorg- en Veiligheidshuis en rapporteert hierover aan het algemeen bestuur en is bevoegd aanwijzingen te geven aan Partijen omtrent de juiste omgang met persoonsgegevens in dat verband.

Artikel 13 Geheimhouding

13.1. Eenieder die op grond van dit protocol kennis neemt van persoonsgegevens is verplicht tot geheimhouding daarvan, tenzij de wet tot bekendmaking verplicht. Het hoofd, de manager(s), procesregisseur(s) en eventueel ander ondersteunend personeel van het Zorg- en Veiligheidshuis worden door middel van een geheimhoudingsverklaring tot geheimhouding gebonden.

13.2. Partijen dragen er zorg voor dat iedere medewerker die in de uitvoering van het convenant of dit protocol in aanraking komt met persoonsgegevens geheimhouding van die gegevens waarborgt.

13.3. Alle medewerkers van het Zorg- en Veiligheidshuis, inclusief medewerkers op basis van een dienstverleningsovereenkomst, deelnemers aan casusoverleggen en overige afgevaardigden van partijen die toegang hebben tot persoonsgegevens die onder dit protocol worden verwerkt, beschikken over een positieve Verklaring Omtrent Gedrag, danwel hebben een veiligheidsonderzoek op grond van de voor de eigen organisatie geldende wet- en regelgeving doorlopen.

13.4. Wettelijke geheimhoudingsplichten zijn onverminderd van toepassing op eenieder die strafrechtelijke persoonsgegevens of andere bijzondere persoonsgegevens in het kader van de samenwerking in het Zorg- en Veiligheidshuis ontvangt.

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 verstrekkende 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 lid 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 verstrekkende 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 erop 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 Rotterdam is verantwoordelijk voor het in stand houden van procedures zoals bedoeld in artikel 14.1 voor de Verwerking van Persoonsgegevens op locatie of in de informatiesystemen van het Zorg- en Veiligheidshuis. Het hoofd ziet toe op de naleving van deze procedures in het Zorg- en Veiligheidshuis.

14.3. Partijen stellen de Privacyfunctionaris onverwijld maar uiterlijk binnen 24 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 privacyfunctionaris informeert de procesregisseur waarop deze de partijen informeert middels het partneroverleg 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. *Het hoofd* stuurt een afschrift van de melding aan de Autoriteit Persoonsgegevens aan het Breed MT en het AB.

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. Het hoofd informeert de betrokkene over de inbreuk namens de op de inbreuk betrokken partijen. De beslissing tot melding aan de betrokkene wordt in het partneroverleg genomen. De inhoud van die melding wordt in het partneroverleg afgestemd, danwel door het partneroverleg 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 privacyfunctionaris houdt een overzicht bij van gelijksoortige inbreuken die plaatsvinden op locatie of in de informatiesystemen van het Zorg- en Veiligheidshuis.

Artikel 15 Privacy by Design

15.1. Voorafgaand aan een (nieuwe) Verwerkingen onder dit protocol, of de inzet van nieuwe technologieën voor de Verwerkingen onder dit protocol, voeren partijen middels het partneroverleg een gegevensbeschermingseffectbeoordeling uit conform artikel 35 AVG. De Privacyfunctionaris 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 het AB. Het AB kan hiervoor advies vragen , aan het Breed MT over de voorgenomen nieuwe verwerking zoals bedoeld in artikel 15.1. Het AB 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 het Zorg- en Veiligheidshuis namens de verstrekkende partij, danwel de partij die de casusregie voert, geïnformeerd over het voornemen diens persoonsgegevens verder te verwerken in het kader van samenwerking in het Zorg- en Veiligheidshuis onder dit protocol.

16.2. Het Zorg- en Veiligheidshuis maakt de het tijdstip waarop en de wijze van informeren kenbaar aan de overige bij een casus betrokken Partijen.

16.3. Het hoofd draagt zorg voor het publiceren van een privacy statement op de website van het Zorg- en Veiligheidshuis.

16.4. Alle deelnemende partijen zorgen op hun eigen website voor vermelding van deelname aan het Zorg- en Veiligheidshuis en voor een verwijzing naar de website van het betreffende Zorg- en Veiligheidshuis/de Veiligheidshuizen waaraan zij deelnemen, alsook voor verwijzing naar het Zorg- en Veiligheidshuis convenant(en) en het privacyprotocol(len).

16.5. De onder artikel 16.1 bedoelde informatieverstrekking, alsook het onder artikel 16.3 genoemde privacy statement, bevatten ten minste de volgende informatie:
a. De doeleinden voor de Verwerking van Persoonsgegevens in het Zorg- en Veiligheidshuis zoals beschreven in artikel 3.2.
b. De partijen die deelnemen aan de samenwerking in het Zorg- en Veiligheidshuis;

c. De termijn waarvoor de persoonsgegevens worden opgeslagen en bewaard zoals omschreven onder artikel 11, danwel de criteria voor het bepalen van die termijn;
d. Dat betrokkene verscheidene rechten heeft met betrekking tot de Verwerking van diens persoonsgegevens zoals geformuleerd onder artikel 17 tot en met 21;
e. Indien de verwerking van persoonsgegevens is gebaseerd op toestemming, dat Betrokkene het recht heeft deze te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de Verwerking van de Persoonsgegevens die heeft plaatsgevonden vóór intrekking van de toestemming;
f. Dat betrokkene het recht heeft een klacht in te dienen over de verwerking van zijn of haar persoonsgegevens onder dit Protocol bij het Zorg- en Veiligheidshuis en bij de Autoriteit Persoonsgegevens;
g. Nadere uitleg indien de persoonsgegevens moeten worden verstrekt of verder verwerkt op grond van een wettelijke of contractuele verplichting;
h. Nadere uitleg indien betrokkene verplicht is de persoonsgegevens te verstrekken;
i. Indien sprake is van geautomatiseerde besluitvorming, met inbegrip van profilering, uitleg over de achterliggende logica, het belang van de verwerkingsactiviteiten en de verwachte gevolgen voor de Betrokkene.
j. De contactgegevens van de 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 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 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. 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 door betrokkene ten aanzien van persoonsgegevens die worden verwerkt op locatie of in het informatiesysteem van het Zorg- en Veiligheidshuis worden gecoördineerd door de procesregisseur. De procesregisseur wordt hierbij ondersteund door een administratief medewerker. Het hoofd legt het verzoek via de procesregisseur voor aan het casusoverleg 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 het hoofd hierover zo spoedig mogelijk door die partij in kennis gesteld, opdat deze de beantwoording van het verzoek conform artikel 17.2 kan coördineren. Beantwoording van het verzoek door de partij wordt in het partneroverleg 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 verstrekkende 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 het Wpg loket van de verstrekkende eenheid van de politie. Verzet- en bezwaarschriften tegen verwerking van gegevens worden beoordeeld door de privacyfunctionaris en/of jurist van de verstrekkende 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 Zorg- en 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 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 de termijnen bepaald in de AVG door het hoofd beantwoord namens de verantwoordelijken in overleg met de verantwoordelijken. 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.

18.5. Bij voldoen aan een verzoek als bedoeld in artikel 17.1, verstrekt het hoofd namens de verwerkingsverantwoordelijke aan de betrokkene een kopie van de persoonsgegevens die worden verwerkt.

Artikel 19 Recht op correctie en verwijdering

19.1. Indien de betrokkene op grond van zijn verzoek om inzage een verzoek tot correctie of verwijdering van bepaalde hem of haar betreffende persoonsgegevens zoals bedoeld in artikel 17.1 onder b doet bij het Zorg- en Veiligheidshuis, legt de *procesregisseur* dit verzoek voor aan het partneroverleg met het oog op de beoordeling van het verzoek.

19.2. Onjuiste persoonsgegevens betreffende de betrokkene worden op diens verzoek onverwijld gecorrigeerd.

19.3. Persoonsgegevens betreffende de betrokkene worden zonder onredelijke vertraging op diens verzoek verwijderd wanneer deze:
   a. voor het doel van de verwerking onvolledig of niet ter zake dienend zijn; of
   b. anderszins in strijd met een wettelijk voorschrift worden verwerkt.

19.4. Het hoofd informeert de betrokkene over de beslissing omtrent zijn verzoek tot correctie of verwijdering van hem of haar betreffende persoonsgegevens schriftelijk en gemotiveerd zo spoedig mogelijk, maar uiterlijk binnen 4 weken na ontvangst van het verzoek.

Artikel 20 Recht op verzet

20.1. Indien de Verwerking van persoonsgegevens door partijen is gebaseerd op de grondslagen van artikel 6 Algemene Verordening Gegevensbescherming, kan de betrokkene daartegen te allen tijde verzet aantekenen in verband met zijn bijzondere persoonlijke omstandigheden.

20.2. Indien een verzoek tot verzet door betrokkene bij één der partijen wordt ingediend, informeert die partij onverwijld de procesregisseur en de privacyfunctionaris over het ingediende verzoek.

20.3. De procesregisseur legt het door betrokkene ingeroepen recht tot verzet voor aan het casusoverleg om te beoordeling of het verzoek gerechtvaardigd is en coördineert de afhandeling daarvan.

20.4. Het hoofd informeert de betrokkene over de beslissing zoals bedoeld in artikel 17.3 binnen 4 weken en draagt er zorg voor dat de beslissing binnen deze 4 weken wordt uitgevoerd. Een beslissing om niet, of niet geheel, te voldoen wordt altijd gemotiveerd en kan met het oog op artikel 21 AVG enkel worden gebaseerd op dwingende gerechtvaardigde gronden.

Artikel 21 Recht op overdraagbaarheid van Persoonsgegevens

21.1. Het recht op overdraagbaarheid van persoonsgegevens is niet van toepassing op partijen in het Zorg- en Veiligheidshuis.

Artikel 22 Verwerkers

22.1. Partijen besteden de verwerking van persoonsgegevens onder dit protocol niet uit zonder dat het Algemeen Bestuur tevoren schriftelijk toestemming heeft gegeven over de beoogde verandering inzake de inzet van verwerkers die ten behoeve van het Zorg- en Veiligheidshuis Persoonsgegevens verwerken. Een overeenkomst van opdracht tussen partijen en een door het Algemeen Bestuur 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 wordt voorgeschreven in het informatiebeveiligingsbeleid van de gemeente Rotterdam.

22.2. 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. Het hoofd van het ZVHRR is bevoegd deze overeenkomst namens partijen aan te gaangaan.

22.3. De privacy officer houdt een lijst bij van de overeenkomsten die met schriftelijke toestemming van het hoofd zijn overeengekomen, welke lijst minimaal eenmaal per jaar wordt bijgewerkt. Deze lijst zal beschikbaar worden gehouden ten behoeve van partijen en de toezichthouder.

Artikel 23. Verstrekking aan derden .

23.1. Persoonsgegevens die in het kader van dit protocol worden Verwerkt, worden niet verstrekt aan anderen dan deelnemers aan het casusoverleg, behoudens het bepaalde in Artikel 19 en tenzij partijen hiertoe wettelijk verplicht zijn. Deze verstrekking wordt schriftelijk vastgelegd door het hoofd.

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 registeren hun verwerkingen van persoonsgegevens onder dit protocol in een eigen register van verwerkingsactiviteiten.

24.2. Aanvullend neemt het hoofd de verwerkingen van persoonsgegevens op locatie en in de informatiesystemen van het Zorg- en Veiligheidshuis op in een gezamenlijk register van verwerkingsactiviteiten onder dit protocol ten behoeve van partijen.

24.3. Het register van verwerkingsactiviteiten bevat minimaal de volgende informatie:
   a. De naam en contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken (of diens vertegenwoordiger);
   b. De verwerkingsdoeleinden;
   c. Een beschrijving van de categorieën persoonsgegevens die worden verwerkt;
   d. Een beschrijving 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 overlegruimtes van het Zorg- en Veiligheidshuis en tot de verwerkingen en register van verwerkingen, alsook toegang tot enige andere informatie, voor zover dit noodzakelijk is voor diens toezichthoudende werkzaamheden.

24.5. De privacyfunctionaris van het Zorg- en Veiligheidshuis dient als eerste aanspreekpunt voor de betrokken Functionarissen Gegevensbescherming.

24.6. De Functionarissen Gegevensbescherming van de verwerkingsverantwoordelijken houden toezicht op de naleving van de verplichtingen in dit protocol en zijn bevoegd aanwijzingen te geven aan de manager en procesregisseur.

Artikel 25. Aansprakelijkheid

25.1. Partijen zetten zich in voor een goede uitvoering van het bepaalde in dit protocol en zullen zich houden aan de 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 Gegevensbescherming van de verwerkingsverantwoordelijken houden het hoofd en de procesregisseur toezicht op de naleving van

de verplichtingen in dit protocol en zijn bevoegd aanwijzingen te geven aan medewerkers in het Zorg- en Veiligheidshuis omtrent de uitvoering van het bepaalde in dit protocol.

Artikel 27. Wijzigingen

27.1. De bepalingen in dit protocol kunnen door de partijen in gezamenlijk overleg worden gewijzigd. Wijzigingen in dit protocol worden door het algemeen bestuur besloten. Voorafgaand aan wijzigingen aan het privacy protocol wordt de werkgroep privacy om advies gevraagd. Mondelinge mededelingen, toezeggingen of afspraken welke betrekking hebben op de inhoud van dit protocol, hebben geen rechtskracht, tenzij deze uitdrukkelijk schriftelijk zijn bevestigd door het algemeen bestuur.

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 Zorg- en Veiligheidshuis schriftelijk opzeggen met ingang van het tijdstip waarop het gewijzigde protocol van kracht wordt. Na opzegging van deelname aan het convenant en dit protocol verkrijgt die partij niet langer toegang tot de persoonsgegevens die op locatie of in de informatiesystemen van het Zorg- en Veiligheidshuis worden verwerkt onder dit protocol.

Artikel 28. Toetreding

28.1. Toetreding door andere organisaties tot dit protocol kan enkel wanneer die partij is toegetreden tot het convenant conform Artikel 21 van dat Convenant.

28.2. Partijen worden vooraf door de secretaris van het AB op de hoogte gebracht van de voorgenomen toetreding. Indien de toetredende partij niet staat benoemd in het handvat dient voorafgaand aan de uitwisseling van persoonsgegevens met de toetredende partij een juridische analyse te worden opgesteld conform hoofdstuk 5 van het handvat. De toetredende Partij voert waar nodig de aanbeveling uit die analyse uit, alvorens uitwisseling van persoonsgegevens in het Zorg- en Veiligheidshuis met die partij plaatsvindt.

28.3. In geval van toetreding tot het convenant, vindt toetreding tot het protocol plaats door middel van ondertekening van Bijlage 1 bij dit protocol door die andere organisatie en de voorzitter van het algemeen bestuur.

Artikel 29. Duur, opzegging, beëindiging

29.1. Dit protocol is een onlosmakend onderdeel van het convenant en treedt in werking op de dag van ondertekening door partijen en wordt voor dezelfde duur als het convenant. In geval van verlenging van het convenant wordt dit protocol met een gelijkluidende termijn verlengd.

29.2. *Het algemeen bestuur* kan, zonder rechterlijke tussenkomst en met meerderheid van stemmen, na ingebrekestelling, een partij met onmiddellijke ingang uitsluiten van de samenwerking in het Zorg- en Veiligheidshuis, indien de afspraken zoals neergelegd in dit protocol niet door de desbetreffende Partij worden nagekomen.

29.3. Verplichtingen die naar hun aard zijn bestemd om ook na beëindiging of uitsluiting van het project voort te duren, blijven na beëindigingen van dit Protocol bestaan. Tot deze verplichtingen behoren onder meer die ter zake van geheimhouding en de beveiliging van Persoonsgegevens.

Artikel 30. Opvolging

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

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

31.1. In het kader van een opdracht tot uitvoering van een wetenschappelijk onderzoek zijn partijen gezamenlijk opdrachtgever en worden de specifieke bepalingen uit wet- en regelgeving alsmede de interne voor partijen geldende voorschriften voor wetenschappelijk onderzoek van partijen in acht genomen.

31.2. partijen zullen dit protocol twee jaar na inwerking treden landelijk en regionaal evalueren, waarbij bij voorkeur een audit zal plaatsvinden door een externe onafhankelijke partij.

Artikel 32. Toepasselijk recht

32.1. Op dit Protocol is Nederlands recht van toepassing.

:

Bijvoegsel I bij Privacy Protocol Toetredingsformulier nieuwe partner tot Protocol

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

overwegende dat:

- Deelname aan het convenant en privacyprotocol 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 convenant en protocol geformuleerde doelstellingen, verplicht zich de bepalingen in het convenant en protocol te zullen naleven en verklaart zich in dit kader gerechtigheid tot het uitwisselen van persoonsgegevens met partijen.

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

Naam organisatie:

Naam bevoegde functionaris:

…….

Namens het algemeen bestuur:

Naam:

……

:

Bijvoegsel 2 bij Privacy Protocol Doeleinden verwerking van persoonsgegevens per processtap

Partijen Verwerken in het kader van het Zorg- en Veiligheidshuis voor ieder van onderstaande fasen enkel de Persoonsgegevens die voor die afzonderlijke fase noodzakelijk zijn voor de uitvoering van ieder van de daarbij geformuleerde toepasselijke processtappen: Zie ook bijlage 2 bij het Handvat gegevensuitwisseling bij behandeling van casuïstiek in het zorg- en veiligheidsdomein; Vertaling handvat naar de praktijk – een voorbeeld.

Intake / Aanmelding

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

Triage

* Uitvoeren van een bekendheidscheck bij andere Zorg- en Veiligheidshuizen met gebruikmaking van de applicatie Middenvelder, en in geval van een lopende behandeling in een ander Zorg- en Veiligheidshuis: afstemmen met de desbetreffende procesregisseur over een passende behandeling van de casus."
- Bepalen eerste beeld en verrijken van informatie uit Intake;
- Op basis van informatie van partners komen tot een nadere afweging ten aanzien van de routering van de casus, tot een bepaling van doel en thema's van een eventueel casusoverleg, en tot een afweging welke partners relevant zijn om te betrekken bij een casusoverleg;
- Voorbereiding Casusoverleg.

Casusoverleg

- Opstellen gezamenlijk toestandbeeld door bij het Casusoverleg 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 Zorg- en 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;

:

Bijvoegsel 3 bij Privacy Protocol:

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 handhavingsgegevens, gegevens omtrent bestuursrechtelijke maatregelen of voornemens daartoe

Strafrechtelijke Persoonsgegeven, te weten:

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

Bijzondere Persoonsgegevens:

Bijzondere gegevens worden in principe niet structureel verzameld. Of bijzondere gegevens verzameld worden is ahankelijk van de aard van de individuele casus en welke gegevens noodzakelijk zijn om te verwerken om te kunnen komen tot een plan van aanpak. Wanneer er bijzondere gegevens worden verzameld kan dat op individueel niveau gaan om:

- Gegevens met betrekking tot seksueel gedrag of seksuele gerichtheid
- Gegevens over gezondheid
- Medische gegevens
- Politieke opvattingen
- Ras of etnische afkomst
- Religieuze of levensbeschouwelijke overtuigingen

:

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 handhavingsgegevens 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 Persoonsgegeven, te weten:

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

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

- Gegevens met betrekking tot seksueel gedrag of seksuele gerichtheid
- Gegevens over gezondheid
- Medische gegevens
- Politieke opvattingen
- Ras of etnische afkomst
- Religieuze of levensbeschouwelijke overtuigingen

Bijzondere gegevens worden in principe niet structureel verzameld. Of bijzondere gegevens verzameld worden is afhankelijk van de aard van de individuele casus en welke gegevens noodzakelijk zijn om te verwerken om te kunnen komen tot een plan van aanpak.

Toelichting:

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 Voor een toelichting raadpleeg ook de MvT bij de UAVG p. 33 t/m 38 en de Handleiding AVG van het Ministerie van Justitie en Veiligheid.

Categorie 3:
Categorie Betrokkenen:

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

Persoonsgegevens:

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

Categorie 4:
Categorie Betrokkenen:

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

Persoonsgegevens:
- naam;
- naam organisatie organisatieaanduiding (typering bijv. instelling voor GGZ);
- functie binnen het Zorg- en Veiligheidshuis;
- contactgegevens (zakelijk telefoonnummer, e-mailadres);

Toelichting:

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

:

Bijvoegsel 4: Wettelijke meldrechten en informatieverplichtingen

De beschrijving van meldrechten en informatieverplichtingen is ontleend aan de handreiking 'Wijkteams en het Pettenvraagstuk' die tot stand gekomen is met medewerking van NIP, BPSW en NVO.

Een aantal materiewetten bevatten specifieke bepalingen die een meldrecht of informatieverplichting inhouden voor beroepskrachten of een specifieke categorie beroepskrachten. Dat betekent dat een beroepskracht in specifieke situaties zijn beroepsgeheim mag doorbreken, voor zover dat noodzakelijk is. We geven hier onder een beknopte beschrijving van de volgende meldrechten en informatieverplichtingen[3]:

- meld- en informatierecht bij vermoeden van kindermishandeling/huiselijk geweld
- meldrecht tegenover de Raad voor de Kinderbescherming
- meldrecht om te melden aan de Verwijsindex risicojongeren
- verzoek om informatie van Veilig Thuis of Raad
- informatieplicht bij een ondertoezichtstelling
- verstrekkingsverplichtingen aan het college uit de Jeugdwet en Wmo
- meldplicht bij calamiteiten en geweld

Meld- en informatierecht bij vermoeden van kindermishandeling/huiselijk geweld

In de Wmo 2015 is een meldrecht opgenomen dat ook geldt voor beroepskrachten bij een vermoeden van huiselijk geweld of kindermishandeling. Dit is geregeld in artikel 5.2.6 van de Wmo 2015:

"Derden die beroepshalve beschikken over inlichtingen die noodzakelijk kunnen worden geacht om een situatie van huiselijk geweld of kindermishandeling te beëindigen of een redelijk vermoeden daarvan te onderzoeken, kunnen aan Veilig Thuis deze inlichtingen desgevraagd of uit eigen beweging verstrekken zonder toestemming van degene die het betreft en indien nodig met doorbreking van de plicht tot geheimhouding."

Bij het maken van de afweging om te melden volgt de beroepskracht de stappen van de meldcode Huiselijk Geweld en Kindermishandeling.[4]

Artikel 5.2.6 uit de Wmo 2015 betekent ook dat beroepskracht informatie mag verstrekken aan Veilig Thuis, bijvoorbeeld als deze daar om vraagt in het kader van een onderzoek. Ook als de beroepskracht weet heeft van een lopend onderzoek door Veilig Thuis, en over informatie beschikt waarvan hij denkt dat dit noodzakelijk is in het kader van het onderzoek, mag hij dit verstrekken. In beide gevallen is toestemming van de betrokkene niet nodig.

De beroepskracht moet wel altijd handelen volgens zijn beroepscode. Dat betekent dat hij een afweging maakt over de informatie die hij aan Veilig Thuis wil verstrekken, en het voornemen om een melding te doen vóóraf bespreekt met de inwoner, tenzij dit ernstige risico's met zich me brengt voor de veiligheid van betrokkene of anderen.

---

[3] De beschrijving van meldrechten en informatieverplichtingen is ontleend aan de handreiking 'Wijkteams en het Pettenvraagstuk' en het Kompas van NIP, BPSW en NVO.

[4] https://www.rijksoverheid.nl/onderwerpen/huiselijk-geweld/meldcode.

https://www.rijksoverheid.nl/documenten/publicaties/2018/07/01/toolkit-meldcode-huiselijk-geweld-en-kindermishandeling

:

Meldrecht tegenover de Raad voor de kinderbescherming

Beroepskrachten hebben ook een meldrecht tegenover de Raad voor de Kinderbescherming (RvdK). Dit is geregeld in artikel 1:240 van het Burgerlijk Wetboek:

"Degene die op grond van een wettelijk voorschrift of op grond van zijn ambt of beroep tot geheimhouding is verplicht kan, zonder toestemming van degene die het betreft, aan de raad voor de kinderbescherming inlichtingen verstrekken, indien dit noodzakelijk kan worden geacht voor de uitoefening van de taken van de raad."

Net als het meldrecht aan Veilig Thuis betekent dit artikel dat een beroepskracht die een geheimhoudingsplicht heeft informatie mag verstrekken aan de Raad voor de

Kinderbescherming. Bijvoorbeeld als deze daar om vraagt in het kader van een onderzoek. Ook als de beroepskracht weet heeft van een lopend onderzoek door de Raad voor de

Kinderbescherming, en over informatie beschikt waarvan hij denkt dat deze noodzakelijk is voor het onderzoek, mag hij dit verstrekken. In beide gevallen is toestemming van betrokkene niet nodig.

Ook hier geldt: De beroepskracht moet wel altijd handelen volgens zijn beroepscode. Dat betekent dat hij een afweging maakt over de informatie die hij aan de Raad voor de

Kinderbescherming wil verstrekken, en het voornemen om een melding te doen of informatie te verstrekken vóóraf bespreekt met de betrokkene, tenzij dit ernstige risico's met zich mee brengt voor de veiligheid van betrokkene of anderen.

Meldrecht om te melden aan de Verwijsindex risicojongeren
Iedere gemeente is aangesloten op de Verwijsindex Risicojongeren (VIR). De VIR is een systeem waarin hulpverleners en andere professionals de persoonsgegevens kunnen registreren van een jeugdige of jongvolwassene (tot 23 jaar) waarover zij zich zorgen maken.

Door de meldingen in de VIR weten hulpverleners sneller of een kind bekend is bij een collega, zodat zij samen kunnen overleggen over de beste aanpak. Het doel van de VIR is dan ook: vroegtijdige onderlinge afstemming, zodat hulpverleners jongeren en jongvolwassenen tijdig passende hulp en zorg kunnen verlenen of kunnen bijsturen. Niet iedereen kan een melding doen. Alleen zogeheten meldingsbevoegden mogen melden. De gemeente maakt hiervoor afspraken met instanties die bij een algemene maatregel van bestuur zijn aangewezen.

De VIR is geregeld in de Jeugdwet. Artikel 7.1.4.1 regelt het meldrecht van de meldingsbevoegden:

"Een meldingsbevoegde kan zonder toestemming van de jeugdige of zijn wettelijk vertegenwoordiger en zo nodig met doorbreking van de op grond van zijn ambt of beroep geldende plicht tot geheimhouding, een jeugdige melden aan de verwijsindex indien hij een redelijk vermoeden heeft dat de jeugdige door een of meer van de hierna genoemde risico's in de noodzakelijke condities voor een gezonde en veilige ontwikkeling naar volwassenheid daadwerkelijk wordt bedreigd."

Onder de in de Jeugdwet genoemde risico's vallen onder andere geestelijk, lichamelijk of seksueel geweld, verslaving, en ernstige opgroei of opvoedingsproblemen. In artikel

7.1.4.1.jeugdwet is een limitatieve opsomming opgenomen.

In paragraaf 7.1. besluit jeugdwet staat wie meldingsbevoegd kunnen zijn. Een bevoegde beroepskracht mag een melding doen in de VIR, zonder dat toestemming van de betrokkene of zijn ouders nodig is. Wel houdt de beroepskracht bij het maken van de afweging om te melden rekening met zijn beroepscode en is hij verplicht om de jeugdige of zijn wettelijk vertegenwoordigers te

informeren over de melding.[5] Dat betekent onder andere dat de beroepskracht openheid betracht over zijn voornemen om een melding te doen in de VIR. De beroepsorganisaties NIP en NVO hebben een factsheet over het melden aan de VIR gemaakt.[6]

Het artikel uit de Jeugdwet maakt een melding in de VIR mogelijk, zodat beroepskrachten aan elkaar gekoppeld kunnen worden. Echter, dit betekent niet dat beroepskrachten dan ook automatisch gegevens mogen uitwisselen. Of informatie mag worden uitgewisseld en onder welke voorwaarden hangt samen met de taak op basis waar van de beroepskracht de gegevens heeft gekregen. Is de informatie verkregen in het kader van een behandelrelatie, dan is het beroepsgeheim van toepassing. Informatieuitwisseling is dan slechts mogelijk met toestemming, of als een van de andere verstrekkingsgronden van toepassing is.

Informatieplicht bij Onder Toezichtstelling

Als een jeugdige door de rechter onder toezicht (OTS) is geplaatst hebben alle beroepskrachten een informatieplicht aan de gecertificeerde instelling die de ondertoezichtstelling uitvoert. Dit is geregeld in artikel 7.3.11 vierde lid van de Jeugdwet:

"Derden die beroepshalve beschikken over inlichtingen inzake feiten en omstandigheden die de persoon van een onder toezicht gestelde minderjarige, diens verzorging en opvoeding of de persoon van een ouder of voogd betreffen, welke inlichtingen noodzakelijk kunnen worden geacht voor de uitvoering van de ondertoezichtstelling, verstrekken de gecertificeerde instelling die de ondertoezichtstelling uitvoert, deze inlichtingen desgevraagd of kunnen deze inlichtingen uit eigen beweging aan de gecertificeerde instelling verstrekken, zonder toestemming van de inwoner en indien nodig met doorbreking van de plicht tot geheimhouding op grond van een wettelijk voorschrift of op grond van hun ambt of beroep."

Het betreft hier echt een informatieplicht aan de jeugdbeschermer of gezinsvoogd van de gecertificeerde instelling over informatie die noodzakelijk kan zijn voor de uitvoering van de ondertoezichtstelling. Daarbij kan het gaan over zaken die niet goed gaan. Maar zeker ook over zaken die wel goed gaan en een positieve ontwikkeling laten zien. De beroepskracht kan die informatie verstrekken zonder toestemming, gevraagd en ongevraagd.

De informatieplicht betekent niet dat de beroepskracht verplicht is om een heel dossier of delen daarvan over te dragen. Ook hier geldt: De beroepskracht moet wel altijd handelen volgens zijn beroepscode. Dat betekent dat hij een afweging maakt over de informatie die hij aan noodzakelijk vindt om te verstrekken, en het voornemen om informatie te verstrekken vóóraf bespreekt met de betrokkene, tenzij dit ernstige risico's met zich mee brengt voor de veiligheid van betrokkene of anderen.

Verplichte verstrekkingen aan het college van b&w in de Jeugdwet en Wmo

De Jeugdwet en de Wmo 2015 kennen beiden bepalingen waarmee het wettelijke beroepsgeheim en de geheimhouding uit andere beroepscodes voor sommige partijen worden doorbroken.

[5] 43 Zie Artikel 7.1.5.1 Jeugdwet.

[6] https://www.psynip.nl/wp-content/uploads/2019/09/Verwijsindex-Risicojongeren-VIR-aug-2019.pdf of https://www.nvo.nl/beroepscode-entuchtrecht/veelgestelde-vragen/de-verwijsindex-risicojongeren-vir-wat-mag-u-als-pedagoog-wel-en-niet-.aspx.

:

Artikel 7.4.0 lid 1, 2 en 3 van de Jeugdwet bepalen onder andere dat jeugdhulpaanbieders, aanbieders van preventie, gecertificeerde instellingen, de Raad voor de Kinderbescherming en gekwalificeerde gedragswetenschappers verplicht zijn het college de gegevens te verstrekken die noodzakelijk zijn voor de collegetaken in het kader van de Jeugdwet, waaronder:

a. de toeleiding naar, advisering over, bepaling van of het inzetten van een voorziening op het gebied van de jeugdhulp, en

b. het doen van een verzoek tot onderzoek bij de raad voor de kinderbescherming of de uitvoering van kinderbeschermingsmaatregelen of jeugdreclassering.

De Wmo 2015 bepaalt dat de aanbieder van een maatwerkvoorziening verplicht is om gegevens te verstrekken aan het college van b&w en een aantal andere partijen voor hun taken in het kader van de Wmo 2015. Onder de collegetaken valt o.a. de taak van het college van b&w om een onderzoek te doen als een burger een aanvraag voor een maatwerkvoorziening indient. Dit is geregeld in artikel 5.2.2 van de Wmo 2015:

1. De aanbieder die een maatwerkvoorziening levert en een derde aan wie ten laste van een persoonsgebonden budget betalingen worden gedaan, zijn bevoegd uit eigen beweging en desgevraagd verplicht kosteloos persoonsgegevens van de cliënt, waaronder bijzondere persoonsgegevens, te verstrekken, aan

a. het college, voor zover deze noodzakelijk zijn voor het uitvoeren van artikel 2.1.4, 2.1.4a, 2.1.4b, 2.1.5, 2.3.2, 2.3.9, 2.3.10 of 2.4.3 of de verantwoording van een geleverde maatwerkvoorziening.

In beide gevallen betekenen de artikelen dat de beroepskrachten die onder de genoemde categorieën vallen geen toestemming nodig hebben om gegevens aan het college te verstrekken voor de genoemde taken. Ook hier geldt: De beroepskracht moet wel altijd handelen volgens zijn beroepscode. Dat betekent dat hij een afweging maakt over de informatie die hij aan noodzakelijk vindt om te verstrekken, en het voornemen om informatie te verstrekken vóóraf bespreekt met de betrokkene, tenzij dit ernstige risico's met zich mee brengt voor de veiligheid van betrokkene of anderen.

Meld en informatieplicht bij calamiteiten en geweld in de hulpverlening

Naast het doorbreken van het beroepsgeheim op basis van een meldrecht zoals hiervoor beschreven, bestaat er bij calamiteiten en bij geweld bij de hulpverlening een meldplicht voor aanbieders/werkgevers van jeugdhulp, jeugdbescherming of jeugdreclassering. Dit is geregeld in de Jeugdwet artikel 4.1.8, lid 1:

De jeugdhulpaanbieder en de gecertificeerde instelling doen aan de ingevolge deze wet met het toezicht belaste ambtenaren onverwijld melding van:

a. iedere calamiteit die bij de verlening van jeugdhulp of bij de uitvoering van een kinderbeschermingsmaatregel of jeugdreclassering heeft plaatsgevonden, en

b. geweld bij de verlening van jeugdhulp of de uitvoering van een kinderbeschermingsmaatregel of jeugdreclassering.

In de genoemde situaties is de jeugdhulpaanbieder of gecertificeerde instelling verplicht een melding te doen bij de Inspectie Gezondheidszorg en Jeugd (IGJ). Veel instellingen hebben intern beleid over dit onderwerp. Daarin is vaak vastgelegd hoe te handelen als de professional zelf of zijn collega's te maken krijgen met agressie in de hulpverleningsrelatie, of als ze een grensoverschrijdend gedrag constateren. Meer informatie over het melden bij de inspectie vind je op de website van de IGJ.

:

Artikel 4.1.8 bevat in het tweede lid ook een informatieplicht aan de Inspectie als deze een situatie als hier boven genoemd onderzoekt:

"De jeugdhulpaanbieder, de jeugdhulpverlener en de gecertificeerde instelling verstrekken bij en naar aanleiding van een melding als bedoeld in het eerste lid aan de ingevolge deze wet met toezicht belaste ambtenaren de gegevens, daaronder begrepen persoonsgegevens, gegevens over gezondheid, andere bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard, die voor het onderzoeken van de melding noodzakelijk zijn." Professionals zijn dus verplicht om gegevens te verstrekken die noodzakelijk zijn voor het onderzoek. Dit kan ook gegevens betreffen over de persoon die hulp of jeugdbescherming ontvangt. Zij kunnen deze gegevens verstrekken zonder toestemming, maar maken wel altijd een afweging welke gegevens noodzakelijk zijn om te verstrekken en of zij een inwoner hier over informeren.

Meer informatie over het melden bij de inspectie vind je op de website van de IGJ.

:

Bijvoegsel 5: privacy-werkgroep

1. De privacy-werkgroep bestaat uit privacy deskundigen van de deelnemende organisaties voor zover de deelnemende organisaties een deskundige voor deelname aan de groep hebben aangemeld.
    a. De privacy-werkgroep kent kern-werkgroepleden die bij iedere vergadering aanwezig zijn.
    b. De privacy-werkgroep kent agenda leden die de stukken en agenda ontvangen en op indicatie bij de overleggen aansluiten.
2. De privacy-werkgroep geeft het Hoofd, het Breed MT of het AB gevraagd en/of ongevraagd advies rond privacy gerelateerde vraagstukken.
    a. Het samenwerkingsverband vraagt de privacy-werkgroep minimaal om advies wanneer het samenwerkingsverband nieuwe verwerkingen voornemens is of beleid ontwikkeld waarbij gevoelige gegevens verwerkt gaan worden van burgers die besproken worden binnen het ZVHRR.
    b. Wanneer de privacy-werkgroep advies uitbrengt kan het samenwerkingsverband hier gemotiveerd van afwijken. Wanneer er gemotiveerd wordt afgeweken wordt dit minimaal in notulen vastgelegd en gecommuniceerd met de privacy-werkgroep.
3. De privacy werkgroep fungeert voor de privacy officer van het ZVHRR als aanspreekpunt voor privacy gerelateerde vraagstukken.
4. De privacy officer van het ZVHRR bereidt de agenda en de stukken voor die de privacy-werkgroep nodig heeft om het samenwerkingsverband van kwalitatief goed advies te voorzien.
    a. De privacy-werkgroep streeft naar gedragen adviezen.
    b. Wanneer adviezen niet door de hele privacy-werkgroep gedragen worden wordt dit duidelijk in de stukken opgenomen met een duidelijk gemotiveerd afwijkend advies van de partner.
    c. Bij complexe vraagstukken kan de privacy-werkgroep van buitenaf advies vragen in overleg met het hoofd van het ZVHRR.

:

Bijvoegsel 6: concern informatiebeveiligingsprotocol gemeente Rotterdam

Concern Informatiebeveiligingsbeleid
Gemeente Rotterdam
2021-2023

Strategisch Beleidskader

Voorwoord

Het concern informatiebeveiligingsbeleid van de gemeente Rotterdam heeft als doel het beschermen van gemeentelijke informatie en informatie van burgers, bedrijven en ketenpartners. Het uitgangspunt is dat de bescherming van de informatie aansluit bij de risico's, bedrijfsvoering en relevante wet- en regelgeving. Het college van B en W hecht grote waarde aan dit onderwerp en verwacht hetzelfde van iedere medewerker. Hierbij is ieder individueel verantwoordelijk voor het veilig omgaan met alle informatie.

Dit strategisch informatiebeveiligingsbeleid is richtinggevend ten aanzien van informatie-veiligheid voor de gemeente Rotterdam en de uitwerking op tactisch en operationeel niveau voor toekomstige beleidsstukken, procedures en werkinstructies die gerelateerd zijn aan het vakgebied van informatieveiligheid.

Ten aanzien van informatieveiligheid heeft gemeente Rotterdam de volgende ambitie:

- Het op een veilige manier verwerken van gegevens van burgers en bedrijven door het toepassen van passende organisatorische en technische beveiligingsmaatregelen, zoals vereist in de Algemene Verordening Gegevensbescherming (AVG) en onder andere beschreven in de Baseline Informatiebeveiliging Overheid (BIO);
- Het voor de burgers, bedrijven en ketenpartners een aantoonbaar betrouwbare partner zijn ten aanzien van het onderwerp Informatiebeveiliging;
- Professioneel inrichten van informatiebeveiliging in het concern in relatie met de verantwoordelijkheid van de gemeente inzake eigenaar, leverancier en/of afnemer van gegevens;
- Bijdragen aan het voorkomen en bestrijden van digitale criminaliteit;
- Mede zorgen voor de samenleving bij het optreden van digitale incidenten;
- Integreren van het informatiebeveiligingsbeleid in de diverse veiligheidsgebieden en hierop intensiever samenwerken.

Digitalisering biedt kansen en dreigingen. Dit informatiebeveiligingsbeleid draagt bij aan het identificeren van deze kansen en het beheersbaar maken van dreigingen.

:

Inhoud

1. Inleiding

De informatie van de gemeente Rotterdam vertegenwoordigt in verschillende verschijningsvormen een grote waarde. De informatievoorziening, en dus de waarde van de informatie, van de gemeente Rotterdam wordt blootgesteld aan vele dreigingen, die bovendien voortdurend veranderen en complexer worden. Dit maakt het noodzakelijk om gerichte maatregelen te nemen om de risico's continu te beheersen.

In 2020 hadden meerdere digitale dreigingen en incidenten grote impact op diverse organisaties, wereldwijd. Ook de gemeente Rotterdam had kortstondig last van het beveiligingslek in Citrix, waardoor diverse werkprocessen met verstoringen te maken kregen. Tijdens de Corona crisis is veel gevraagd van vernieuwde manieren van informatie verwerken, waarbij nieuwe digitale dreigingen en risico's hun intrede deden, waarvoor weer nieuwe passende maatregelen (zowel organisatorische als technische) ontwikkeld en geïmplementeerd moesten worden.
In deze situaties werden niet enkel de regels en beleid als uitgangspunt genomen maar meer de aangediende realiteit. Vanuit volwassen vakmanschap is gewerkt om de nieuwe realiteit te interpreteren naar, voor de gemeente, waarde toevoegende activiteiten rondom informatieveiligheid. Deze getoonde veerkracht is een basis onder het nieuwe Rotterdamse werken.

De arena rondom digitale aanvallen wordt niet alleen groter en intensiever, maar ook complexer. Het is daarom onmogelijk om incidenten helemaal te voorkomen. Wat we wél kunnen doen is weerbaarder worden, weten wat we moeten doen wanneer een incident de gemeente treft. Goed voorbereid zijn en klaar staan, dat is de veerkracht van informatieveiligheid Rotterdam en is gedefinieerd als de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen (kunnen) worden door (digitale) dreigingen, te beschermen.

Goed voorbereid zijn betekent voor de eigenaren van de informatiesystemen en -processen continue op de hoogte zijn van de actuele risico's om de juiste maatregelen te treffen ter vermindering/voorkoming/verzekeren van deze risico's. Dit impliceert een risicobereidheidsprofiel. De eigenaren worden hierin ondersteund en geadviseerd door meerdere disciplines, waaronder functionarissen informatiebeveiliging, immers informatiebeveiliging is "maar" één van de kwaliteitsaspecten in informatievoorziening.

Het verder digitaliseren van processen staat hoog op de agenda, de informatiesystemen worden steeds beter, sneller en preciezer. Deze komen steeds meer met elkaar samen, raken met elkaar vervlochten en vormen zo één geheel. Nieuwe technologieën worden uitgeprobeerd en bij succes ingevlochten. Het datagedreven werken neemt een snelle vlucht. Gegevens over alles wat mensen en organisaties doen worden steeds vaker opgeslagen en gebruikt. Zo krijgt iedereen te maken met meer digitalisering en technologie.

De eigenaren van de informatiesystemen moeten op een andere manier aangesproken en betrokken worden vanuit informatiebeveiliging. Niet vanuit een centraal beleid en plan waarin de doelen en oplossingen bedacht en geïmplementeerd zijn, maar door samenwerking aan integrale veiligheid welke het clusterbelang optimaal ondersteunt.

In de nieuwe werkelijkheid blijven de eigenaren van informatiesystemen verantwoordelijk voor de resultaten, de uitvoering, nakoming van regels en de effectiviteit ten aanzien van informatiebeveiliging. Zij worden hierin ondersteund door de functionarissen informatie-veiligheid met ontwikkeling van beleid, kaders en processen. De eigenaren worden geadviseerd inzake dreigingen, risico's en te nemen maatregelen, waarbij waarde-creatie,

veerkracht, heuristiek, leren/ervaren en door-ontwikkelen de uitgangspunten zijn. De inspiratie voor deze samenwerking heeft een relatie met het vermogen om de toekomst te voorzien.
De eigenaren van informatiesystemen kunnen daarmee een voortrekkersrol pakken en leiderschap tonen om vanuit hun proces / informatiesysteem de integrale veiligheid te borgen.
De complementaire benadering van het thema behoeft een nieuwe uitwerking van beleidsvoornemens voor informatiebeveiliging.
De directie(s) en de bestuurder(s) kunnen op basis van deze beleidsvoornemens en de risicobereidheid haar verantwoordelijkheid nemen rondom informatiebeveiliging door inzicht in de dreigingen, risico's en maatregelen.

Met dit informatiebeveiligingsbeleid heeft gemeente Rotterdam het concern brede informatiebeveiligingsbeleid beschreven voor de jaren 2021-2023. Dit beleid sluit aan bij het 'Concern Integraal Beveiligingsbeleid', de kadernota 'Sturen en Verantwoorden Rotterdam 2020' en de VNG resolutie 'Digitale Veiligheid: kerntaak voor de gemeenten' (feb. 2021).

:

2. Aanleiding/context

Dit concern informatiebeveiligingsbeleid 2021-2023 is **richtinggevend en kaderstellend** voor informatieveiligheid en wordt aangevuld met onderwerp specifieke documenten voor informatiebeveiliging op tactisch niveau, waaronder de Regeling ICT- en informatiegebruik, het Meerjarenplan Informatiebeveiliging en uitgewerkt op operationeel niveau in processen en werkinstructies.

2.1 Leeswijzer

Hoofdstuk 2 bevat de uitgangspunten en strategische principes van informatiebeveiliging binnen de gemeente. Hoofdstuk 3 zet de kern van het strategisch beleid uiteen inclusief het raakvlak met andere domeinen. Hoofdstuk 4 beschrijft hoe de taken en verantwoordelijkheden ten aanzien van informatiebeveiliging in gemeente Rotterdam belegd zijn.

2.2 Wat is informatiebeveiliging

Informatiebeveiliging is de verzamelnaam van processen en maatregelen, die ingericht zijn om de *betrouwbaarheid* van gemeentelijke processen, informatiesystemen en de daarin opgeslagen gegevens (zowel digitaal als analoog, tekst, video, geluid) en de organisatie te beschermen tegen al dan niet opzettelijk onheil. Dit betreft:

- Beschikbaarheid (B)/ continuïteit: het zorg dragen voor het beschikbaar zijn van informatie en informatie-verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit (I)/ juistheid: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- Vertrouwelijkheid (V)/ exclusiviteit: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Deze indeling van informatiebeveiliging naar *betrouwbaarheid* wordt kortweg BIV genoemd.

Informatieveiligheid borgt beveiligingsmaatregelen tegen bedreigingen ter voorkoming en vermindering van:

- Onwenselijk verlies van informatie, zowel tijdelijk als permanent;
- Onwenselijke corruptie van informatie, zowel bewust als onbewust;
- Onwenselijke onthulling van informatie, bewust of onbewust.

De Baseline Informatiebeveiliging Overheid (de BIO) omschrijft deze beveiligingsmaatregelen op vier niveaus. Per gedefinieerd bedrijfsbelang zal het juiste niveau passende maatregelen een adequate bescherming bieden. Rotterdam zal standaard voldoen aan Basis Beveiliging Niveau (BBN) 2. Indien de te beschermen belangen een hogere BBN (2+ of 3) eist, wordt via een risicoanalyse bepaald welke passende maatregelen aanvullend getroffen moeten worden.

2.3 Scope

Het concern informatiebeveiligingsbeleid is van toepassing op **alle informatie van de gemeente**, waarvan de gemeente eigenaar, leverancier en/of afnemer is, en worden verwerkt door de processen en onderliggende informatiesystemen van de gemeente, (keten)partners, samenwerkingsverbanden en/of diensten. Het is ook van toepassing op de informatie en dienstverlening welke door externe partijen worden uitgevoerd namens gemeente Rotterdam.

Het concern informatiebeveiligingsbeleid is van toepassing voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de **hele levenscyclus van**

informatie-systemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en informatie. Het heeft ook betrekking op het bestuur, management, alle medewerkers, bezoekers en externe relaties.

Dit informatiebeveiligingsbeleid is **locatie-onafhankelijk** en omvat alle locaties die onder de verantwoordelijkheid vallen van gemeente Rotterdam. De doelstellingen en bestuurlijke principes voor informatiebeveiliging die de gemeente stelt zijn ook van toepassing op momenten wanneer medewerkers zich met informatie van de organisatie buiten deze locaties bevinden. Denk hierbij bijvoorbeeld aan de ambulante medewerkers en het (massaal) thuiswerken.

Het concern informatiebeveiligingsbeleid is een **algemene basis** en dekt tevens **aanvullende beveiligingseisen** uit wetgeving af zoals voor de gemeentelijke basisregistraties, BRP, PNIK en SUWI.

Er zijn **meerdere domeinen** waar informatiebeveiliging raakvlakken mee heeft. Informatie-beveiliging houdt zich bezig met het beveiligen van **alle** (gevoelige) gegevens die binnen de gemeente worden verwerkt. Dit maakt dat het domein privacy, waarbij privacygevoelige gegevens dienen te worden beschermd met passende organisatorisch en technische beveiligingsmaatregelen, raakvlakken heeft met het domein van informatiebeveiliging. Domeinen naast privacy waar ook raakvlakken mee zijn, zijn beschreven in paragraaf 3.6. De beleidsmatige aspecten (wat mag wel en wat mag niet) van deze domeinen vallen buiten de scope van dit concern informatiebeveiligingsbeleid. Waar deze domeinen inhoudelijk betrekking hebben op de informatiebeveiligingscomponent (hoe beschermen we informatie) valt dit binnen de scope van het concern informatiebeveiligings-beleid.

2.4 Dreigingslandschap gemeente Rotterdam

Gemeente Rotterdam heeft te maken met een alsmaar veranderend dreigingslandschap. De arena rondom digitale aanvallen wordt niet alleen groter en intensiever, maar ook complexer. Actoren spelen daarop in en maken misbruik van de actualiteit, zoals de verkiezingen in een land of bij de pandemie. De steeds verdergaande digitalisering leidt tot een verdere vergroting van de aanvalsmogelijkheden. De groep actoren die beschikt over geavanceerde aanvalscapaciteiten groeit. De digitale dreiging is permanent, actoren blijven digitale middelen inzetten voor spionage, verstoring en sabotage om eigen doelen (bijvoorbeeld wraak, geldelijk gewin of ideologie) te bereiken. Digitale incidenten kunnen leiden tot maatschappij-ontwrichtende schade, waar ook gemeente Rotterdam waakzaam en weerbaar voor moet zijn, inclusief de impact die digitale incidenten kunnen hebben op de gemeentelikke organisatie.

Het is onmogelijk om incidenten helemaal te voorkomen. Wat we wél kunnen doen is weerbaarder worden, weten wat we moeten doen wanneer een digitale incident de gemeente treft zodat de negatieve gevolgen zo klein mogelijk worden gehouden. Goed voorbereid zijn en klaar staan, dat is de veerkracht van gemeente Rotterdam op het gebied van informatiebeveiliging. Deze veerkracht en weerbaarheid is gedefinieerd als de activiteiten die nodig zijn om netwerk- en (keten-)informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen (kunnen) worden door cyberdreigingen, te beschermen. Om voorbereid te zijn, onderhoudt gemeente Rotterdam een dreigingsbeeld als continue monitor.

Het onderkennen en kunnen herkennen van dreigingen is randvoorwaardelijk voor een snelle en accurate respons. Om goede risicoafwegingen te kunnen maken en te kunnen prioriteren in de te treffen maatregelen, moet duidelijk zijn wat de meest relevante dreigingen zijn. Het Dreigingsbeeld Informatiebeveiliging Gemeente Rotterdam 2021-2023 biedt hier inzicht in. Vanuit het perspectief van nationale veiligheid liggen de dreigingen vooral op het vlak van (voorbereidingen voor) sabotage en spionage door statelijke actoren. Ook (grootschalige) uitval van digitale diensten, processen of systemen vormt een dreiging. Verder is er de dreiging

:

die uitgaat van criminele actoren die het te doen is om economisch gewin. De dreigingen die een risico vormen voor de nationale veiligheid zien we ook terug op lokaal niveau. De dreiging van binnenuit levert echter het grootste risico op voor gemeente Rotterdam, zowel onbedoeld (door menselijke en/of technische fouten) als opzettelijk (medewerkers met kwade bedoelingen).

Het dreigingsbeeld en de onderliggende dreigingsanalyses die de gemeente hier periodiek op uitvoert, vormt het kloppend hart van het gemeentelijke informatiebeveiligingsproces. En stelt de gemeente beter in staat om haar kennis, aandacht en geld aan de belangrijkste dreigingen en kwetsbaarheden te besteden.

2.5 Doelstellingen Concern Informatiebeveiligingsbeleid

Het concern informatiebeveiligingsbeleid beschrijft de vijf doelstellingen op het gebied van informatiebeveiliging waarmee gemeente Rotterdam zorgt voor geformaliseerde en gestructureerde uitvoering van informatiebeveiliging waarbij de beheersing aantoonbaar is. Deze vijf doelstellingen zijn:

1. • Gemeente Rotterdam beheerst risico's en treft de juiste maatregelen en beschermt hiermee de waarde van de informatie. Er is concreet beleid, heldere principes en werkbare procedures binnen een effectieve en efficiënte informatiebeveiligingsketen.
2. • Processen worden uitgevoerd met passende beveiligingsmaatregelen en risico's worden beheerst, waardoor medewerkers hun werkzaamheden kunnen uitvoeren volgens het informatiebeveiligingsbeleid.
3. • Informatiesystemen zijn voorzien van passende, effectieve en innovatieve beveiligingsmaatregelen.
4. • Informatie van de gemeente is op adequate wijze beveiligd tegen digitale en fysieke invloeden.
5. • Gemeente Rotterdam is aantoonbaar 'in control' en voldoet minimaal aan wet- en regelgeving en normenkaders (waaronder AVG, BRP, BIO en ENSIA).

Deze doelstellingen zijn leidend voor het Meerjarenplan Informatiebeveiliging, waarin een overzicht en prioritering van alle trajecten en activiteiten tot en met 2023 is uitgewerkt langs de indeling van 'beleid', 'uitvoering' en 'control'. Het meerjarenplan ondersteunt hiermee de gemeente Rotterdam in de verantwoordelijkheid op het gebied van informatiebeveiliging.

:

2.6 Doelgroepen

Het concern informatiebeveiligingsbeleid is bedoeld voor iedereen in en rond de gemeentelijke organisatie. In onderstaande tabel zijn de verschillende doelgroepen samengebracht, inclusief de relevantie, en verwijzing naar onderliggende bronnen, van diezelfde doelgroep naar het thema van informatiebeveiliging.

Doelgroep	Relevantie
College van B en W	Integrale verantwoordelijkheid om de gemeentelijke informatiehuishouding veilig te organiseren (1)
Gemeentesecretaris	Eindverantwoordelijk voor beveiligingsbeleid en voor de uitvoering van de organisatie brede vraagstukken ten aanzien van de informatiebeveiliging (2)
Proceseigenaren	Verantwoordelijk voor de beveiliging van het betreffende proces, data, en/of informatiesysteem (2)
Directeuren, afdelingshoofden, teamleiders, projectmanagers en projectleiders	Als eerste lijn verantwoordelijk voor realiseren van de organisatiedoelen, doelmatige inzet van middelen en weloverwogen omgaan met de risico's die de gemeente loopt (3)
Informatiebeveiligings-functionarissen	Als tweede lijn de adviestaak voor informatiebeveiliging aan de eerste lijn (3) Verstrekken van concern brede kaders, methodieken en formats (3) Vaststellen dat de concern brede kaders, methodieken en formats worden toegepast (3)
Financial Audit en Concern Auditing	Vaststellen gezamenlijke functionering eerste en tweede lijn om doelstelling te realiseren (doelmatig en doeltreffend) (3)
Dienstenleveranciers	Organisaties in de markt waaraan de gemeentesecretaris of proceseigenaar een (deel van) de beveiligingstaak in- of uitbesteedt (2)
Medewerkers	Toepassen van de regels en procedures aangaande informatiebeveiliging (2)

Legenda bronnen informatieveiligheid:
(1) VNG resolutie "informatieveiligheid"
(2) BIO, versie 2020
(3) Kadernota 'Sturen en Verantwoorden Rotterdam 2020'

2.7 Besluitvorming

Het concern informatiebeveiligingsbeleid is vastgesteld door het college van B en W voor de periode 2021-2023. Hiermee komt het oude informatiebeveiligingsbeleid (van 2018) te vervallen.

Jaarlijks wordt in het ENSIA-verantwoordingsproces, het informatiebeveiligingsbeleid getoetst op effectiviteit en actualiteit. Uiterlijk 2023 zal het informatiebeveiligingsbeleid, waar nodig, worden aangepast en opnieuw ter vaststelling worden aangeboden. Indien een nieuw informatiebeveiligingsbeleid nog niet is vastgesteld, dan blijft het huidige informatie-beveiligingsbeleid tot dat moment van toepassing.

:

3 Uitgangspunten voor informatiebeveiliging

Dit hoofdstuk beschrijft de uitgangspunten voor informatiebeveiliging die gelden binnen gemeente Rotterdam. De uitgangspunten bestaan uit de strategische doelen die de gemeente zichzelf heeft gesteld en de bestuurlijke principes die de gemeente hanteert om deze doelen te realiseren. Informatiebeveiliging is een thema wat niet op zichzelf staat. De verschillende domeinen waarmee informatiebeveiliging een relatie heeft zijn toegelicht evenals de cruciale rol van een informatieveilige cultuur en informatiebeveiliging bewustwording.

3.1 Strategische doelen informatiebeveiliging

Het concern informatiebeveiligingsbeleid streeft de volgende strategisch doelen na:

1. Het managen van de informatiebeveiliging.
2. Adequate bescherming van informatie en bedrijfsmiddelen.
3. Het minimaliseren van risico's van menselijk gedrag.
4. Het voorkomen van ongeautoriseerde toegang.
5. Het garanderen van correcte en veilige informatievoorzieningen.
6. Het beheersen van de toegang tot informatiesystemen.
7. Het waarborgen van veilige informatiesystemen.
8. Het adequaat reageren op incidenten.
9. Het beschermen van kritieke bedrijfsprocessen.
10. Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
11. Het waarborgen van de naleving van dit beleid.

3.2 Bestuurlijke principes informatiebeveiliging

Het concern informatiebeveiligingsbeleid sluit aan bij de tien bestuurlijke principes[1] die de gemeente Rotterdam toepast, welke de bestuurlijke aanvulling is op het normenkader BIO en gaat over de waarden die de bestuurders hanteren en uitdragen.

Deze principes zijn algemene uitgangspunten die ten grondslag liggen aan de inrichting van de gemeentelijke organisatie. Ze zijn universeel van toepassing en ze vormen zo de uitgangspunten voor het bestuur, directie en management, het concern informatiebeveiligings-beleid, de inrichting ervan en de hieruit voortvloeiende werkwijze van de gemeente.

Als aanvulling op deze tien bestuurlijke principes, onderkent gemeente Rotterdam, de volgende vier bestuurlijke principes voor informatiebeveiliging.

1. De **samenwerking** tussen de informatiebeveiligingsorganisatie en de domeinen waar raakvlakken mee zijn, is cruciaal voor het borgen van een betrouwbare en open omgeving binnen de gemeente.
2. Een belangrijk uitgangspunt van informatiebeveiliging is het principe **security-by-design**. Door security-by-design toe te passen ontwikkelt en implementeert gemeente Rotterdam in een zo vroeg mogelijk stadium passende informatiebeveiligingsmaatregelen. De gemeente schenk bij het ontwikkelen en implementeren van nieuwe processen, applicaties en innovaties (bijvoorbeeld AI, algoritmes en chatbots) aandacht aan bestaande en toekomstige dreigingen en het benoemen en mitigeren van de beveiligingsrisico's. Bij het toepassen van dit uitgangspunt maakt gemeente Rotterdam gebruik van interne en externe standaarden.
3. Bij het toepassen van deze bestuurlijke principes moet altijd worden gezocht naar een goede **balans** tussen informatieveiligheid, gebruiksvriendelijkheid (werkbaarheid) en kosten. Aangezien niet alle risicovolle situaties volledig af te dekken zijn met

[1] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/01/De-10-bestuurlijke-principes-voor-Informatiebeveiliging_20190109.pdf

beveiligingsmaatregelen, legt gemeente Rotterdam de gemaakte keuzes vast ten behoeve van verantwoording en evaluatie.

4. De gemeente Rotterdam werkt zowel **norm- als risico-gebaseerd**. De proceseigenaar, gemandateerd door de concerndirecteur, is verantwoordelijk voor de beveiliging van het betreffende proces, data, en/of informatiesysteem. Het is daarom aan de proceseigenaar om de risicobereidheid te bepalen en daarmee ook te controleren of de maatregelen binnen de organisatie de risico's terugbrengen tot een voor de proceseigenaar acceptabel niveau. Overschrijding van dat niveau vereist expliciete besluitvorming.

3.3 Wet- en regelgeving

De juridische grondslag van het concern informatiebeveiligingsbeleid is terug te vinden in wet- en regelgeving. Wetten en regelingen die van toepassing zijn (niet limitatief): Wet Openbaarheid van Bestuur (WOB), Algemene Verordening Gegevensbescherming (AVG), Wet Computercriminaliteit II, Comptabiliteitswet, Archiefwet, Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007), Wet SUWI, Wet GBA en wet BRP.

Naleving van regels vergt steeds meer externe verantwoording, bijvoorbeeld voor gebruik van DigiD[2], SUWI[3] en BRP[4]. Aanvullend op dit informatiebeveiligingsbeleid kunnen daarom specifieke regels gelden, bijvoorbeeld op grond van de Archiefwet, de wet BRP of SUWI. Rotterdam sluit aan bij de landelijk ingevoerde ENSIA.

Voor alle categorieën informatie is de bewaartermijn bepaald in overeenstemming met wet- en regelgeving, contractuele verplichtingen en bedrijfsmatige eisen.
Bij het (laten) vervaardigen en installeren van programmatuur wordt er voor gezorgd dat de intellectuele eigendomsrechten die daar op rusten niet worden geschonden.

3.4 Normen en standaarden

De ontwikkelingen in de informatietechnologie gaan steeds sneller en de wetgeving rondom de bescherming van persoonsgegevens is aangescherpt. Een breed erkende internationale norm om informatie(systemen) adequaat te beveiligen is vastgelegd in de ISO27001/2. Voor de Nederlandse overheid is deze norm vertaald naar een zogenaamde Baseline Informatiebeveiliging Overheid (BIO[5]) met daarin de regels waaraan alle overheidslagen dienen te voldoen. Door middel van een zelfevaluatie (ENSIA) verantwoorden gemeenten zich over deze norm.

De gemeente past de normen en standaarden toe die als aanvulling op de ISO27001/2 en de BIO dienen, zoals de wereldwijde beveiligingsstandaard IEC 62443 voor industriële controlesystemen (ICS) en veilig software ontwikkelen (SSD, NPR5326 en IEC25010) en voor veilige en toegankelijke websites ontwikkelen. Ook past gemeente Rotterdam standaarden en producten toe welke ontwikkeld zijn door de Informatiebeveiligingsdienst voor gemeenten (IBD) en het Nationaal Cyber Security Centrum (NCSC).

3.5 Strategisch risicomanagement

De kern van strategisch risicomanagement is het bewust komen tot betrouwbaarheidseisen en beveiligingsmaatregelen en het bewust accepteren van beheersbare risico's. Hierbij wordt uitgegaan van het principe "van onbewust risico's lopen naar bewust risico's nemen" (Bron: Concern Integraal Beveiligingsbeleid Rotterdam).
Strategisch risicomanagement is het inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van informatiebeveiliging risico's

[2] DigiD: Naam van het systeem waarmee Nederlandse overheden op internet iemand identiteit verifiëren
[3] SUWI: Wet Structuur Uitvoeringsorganisatie Werk en Inkomen
[4] BRP: Basisregistratie Personen
[5] Zie Staatscourant 2019, nr 26526: https://zoek.officielebekendmakingen.nl/stcrt-2019-26526.html

en benutten van kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes.

Gemeente Rotterdam beschikt over een strategisch risicomanagement proces. Binnen dit proces werken de doelgroepen (zie paragraaf 2.6) samen bij het maken van een weloverwogen keuze en goede balans tussen risico's, maatregelen en dreigingen.

3.6 Overige domeinen

De bestuurlijke principes (zie paragraaf 3.2) hanteert de gemeente Rotterdam ten aanzien van het informatiebeveiliging-domein. Daarnaast onderkent de gemeente Rotterdam de raakvlakken en/of afhankelijkheid met de volgende domeinen waarop informatiebeveiliging een positieve impact heeft. Per domein is een korte toelichting gegeven hoe de gemeente de samenhang met het andere domein ziet vanuit strategisch perspectief:

- ***Privacy***: De verantwoordelijke voor het verwerken van persoonsgevoelige informatie dient te voldoen aan de wettelijke verplichtingen zoals de AVG. Hierbij richt privacy zich specifiek op de risico's die impact hebben voor individuen, voor mensen, voor burgers; om hierbij de rechten en vrijheden van natuurlijke personen te waarborgen.
  Gemeente Rotterdam is als verwerkingsverantwoordelijke verplicht om passende organisatorische en technische beveiligingsmaatregelen te treffen, in lijn met de artikelen 5, 24 en 25 en 32 van de AVG. Daarnaast moet gemeente Rotterdam kunnen laten zien dat de juiste organisatorische en technische maatregelen zijn genomen om de persoonsgegevens te beveiligen.
  Om veilig persoonsgegevens te verwerken maakt gemeente Rotterdam onder andere gebruik van privacy-by-design en beveiligingsmaatregelen zoals het autoriseren van toegang, het loggen van applicatie-gebruik en het risico-bewustzijn van de medewerkers. Daarnaast heeft gemeente Rotterdam de werkprocessen waarin persoonsgegevens worden verwerkt, vastgelegd in een verwerkingsregister.
- ***Informatiebeheer***: De verantwoordelijke voor het verwerken, opslaan en verwijderen van informatie past de kaders en richtlijnen van informatiebeheer toe. Om dit veilig te doen is informatiebeheer afhankelijk van de beveiligingsmaatregelen die hiervoor ontwikkeld zijn. Denk hierbij aan het versiebeheer, het maken en terug zetten van backups, het veilig archiveren van maatregelen en het toepassen van de wettelijke bewaartermijnen.
- ***Architectuur***: De verantwoordelijke van een proces hanteert architectuur principes om de voorgestelde aanpassingen te toetsen tegen de bestaande principes, richtlijnen en modellen van de gemeente. Hiermee borgt architectuur dat veranderingen in lijn met de gemeentelijke afspraken getoetst en beschreven zijn. Zo ook op het gebied van informatiebeveiliging. Informatiebeveiligingsarchitectuur is hiermee de set van samenhangende modellen en principes die efficiënt en flexibel richting geeft aan het implementeren van het concern informatiebeveiligingsbeleid, zodat de gemeente de juiste beveiligingsmaatregelen treft en onderhoud.
- ***Fysieke veiligheid***: De verantwoordelijke van het pand of de ruimte verschaft alleen geautoriseerde toegang tot panden of ruimtes waar gevoelige informatie fysiek of digitaal aanwezig is. De verantwoordelijke van het pand of de ruimte neemt maatregelen op basis van risicoafweging tot het beschermen van de aanwezige informatie conform de eisen uit het concern informatiebeveiligingsbeleid.
- ***Personele veiligheid***: De verantwoordelijke zorgt ervoor dat medewerkers veilig hun taak kunnen uitvoeren. De verantwoordelijke zorgt ook voor het borgen van de betrouwbaarheid en integriteit van de medewerkers, zodat bewust foutief menselijk handelen zoveel mogelijk wordt voorkomen.

- ***Business continuity management (BCM)***: De verantwoordelijke van een proces draagt zorg voor het tijdige herstel van de werking van zijn proces in geval van een onderbreking als gevolg van een incident of calamiteit. Waar het gaat over de continuïteit van informatie voorziening worden de maatregelen genomen conform het concern informatie-beveiligingsbeleid.
- ***Softwareontwikkeling***: De verantwoordelijke van een proces hanteert bij het ontwikkelen, het testen en het onderhouden van software, de normen en standaarden om te komen tot blijvend veilige software.
- ***ICT beheer:*** De verantwoordelijke voor een proces draagt zorg voor de het veilig beheer van applicaties, systemen en informatie. Het veilige beheer omvat een ruim scala aan on-premise systemen en onderdelen (zoals koppelingen) met de (externe) cloudoplossingen.
- ***ICS/OT en IOT:*** De verantwoordelijke van een proces houdt rekening met additionele veiligheidseisen die gesteld worden aan zogeheten Operational Technology (OT). Dit is een overkoepelende term voor onder andere Industrial Control Systems (ICS), Supervisory control and data acquisition systemen (SCADA), Programmable Logic Controllers (PLC), (Industrial) Internet of Things toepassingen (IIot/IoT) en sensoren. Hieronder vallen bijvoorbeeld systemen voor het bedienen van bruggen, sluizen, gemalen, tunnels, verkeerslichten, camera's, parkeergarages, liften, toegangspoorten, (straat)verlichting en sensoren die enkel gebruikt worden voor dataverzameling. De gevolgen van een incident m.b.t. OT kunnen eerder levensbedreigend en/of maatschappij verstorend/ontwrichtend zijn dan van een incident m.b.t. kantoorautomatisering.
- ***Cyber Resilience***: De verantwoordelijke van een proces draagt zorg voor de cyber resilience ervan. Digitalisering en nieuwe technologieën bieden grote maatschappelijke en economische kansen. Tegelijkertijd zorgen deze ontwikkelingen ook voor dreigingen en kwetsbaarheden. Nieuwe technieken, diensten en aanbieders maken dat de maatschappelijke afhankelijkheid van internet en ICT-middelen steeds groter wordt en dat de fysieke en digitale wereld steeds meer verweven raken. Gemeente Rotterdam krijgt naast fysieke crises ook te maken met digitale crises of crises met een digitale component. Bij cyber resilience, oftewel digitale weerbaarheid, gaat het om de veerkracht van een organisatie en haar digitale systemen en processen. Cyber resilience wordt uitgedrukt in de snelheid en effectiviteit waarmee een organisatie zich weet te herstellen na een incident[6]. Waar het gaat over de weerbaarheid van het proces worden de maatregelen genomen conform het concern informatiebeveiligingsbeleid.

Het concern informatiebeveiligingsbeleid van gemeente Rotterdam is eveneens van toepassing binnen al deze domeinen.

3.7 Verhogen Digitale Weerbaarheid

Informatieveiligheid is een zaak van alle medewerkers. Zij zijn cruciaal om de digitale weerbaarheid van de gemeente te verhogen. Om dit te ondersteunen zijn de aandachtpunten:

De mens centraal

De toegenomen afhankelijkheid van internet in het maatschappelijke en zakelijke verkeer, de voortschrijdende digitalisering van de dienstverlening, het toegenomen gebruik van sociale netwerken en de opslag van informatie in de cloud, creëren nieuwe beveiligingsrisico's voor de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. De mens is een belangrijke schakel in het grotere geheel van informatiebeveiliging. De mate waarin medewerkers zich bewust zijn van de dreigingen die aan het cyberlandschap en de gemeentelijke processen, informatiesystemen en informatie verbonden zijn en veilig gedrag vertonen, bepaalt de sterkte en zwakte van deze schakel.

[6] https://www.nctv.nl/actueel/nieuws/2019/10/01/cybersecurity-woordenboek-maakt-lastige-terminologie-begrijpelijk

Attitude en gedrag

De meeste inbreuken op de vertrouwelijkheid en integriteit van de gegevens worden veroorzaakt door onbewust verkeerd handelen. Om het risico op dit onbewust en ongewenst verkeerd handelen te bestrijden, zet de gemeente in op het creëren van een goede veiligheidscultuur; een cultuur waar medewerkers risico's en bedreigingen meewegen als onderdeel van hun dagelijkse routine. Om een goede veiligheidscultuur binnen de gemeente op te bouwen, is een structurele cultuurverandering nodig. Een verandering waarbij het juiste gedrag wordt bevorderd en er een open cultuur ontstaat waarin men elkaar aanspreekt op fout en goed gedrag. Het uiteindelijk doel is om een informatieveilige en privacy-veilige cultuur te bouwen die in het DNA van gemeente Rotterdam verankerd is. Dit is niet gemakkelijk te realiseren, aangezien het een langdurig proces is waarvoor een integrale aanpak en veel deskundige inzet nodig zijn.

Informatiebeveiliging cultuur

Organisatorische en technische maatregelen om informatie te beveiligen werken alleen als bestuur, management en medewerkers de noodzakelijke houding en gedrag vertonen. Gedrag heeft te maken met iets ongrijpbaars als de 'organisatiecultuur'. Een gestructureerde aanpak maakt het ongrijpbare toch hanteerbaar. Maar het vereist wel een voortdurend proces, dat zijn basis vindt in een duidelijke strategie en een verdere uitwerking in een concreet stappenplan. Het voorbeeldgedrag door het management is daarbij van wezenlijk belang, van boven naar beneden.

Informatiebeveiliging is van iedereen, medewerkers zijn zich bewust van de waarde en de gevoeligheid van de informatie. Het management ondersteunt continue het veilig werken en het daarbij horende gedrag om gezamenlijk de kans op een datalek, hack of incident te voorkomen. Veilig werken wordt beloond, medewerkers schromen zich niet om onveilige situaties te bespreken of te melden, de middelen om veilig te werken zijn beschikbaar sluiten aan bij de behoefte van de medewerkers om veilig te werken.

Het veilig werken wordt rondom deze middelen en het gedrag structureel ondersteund door gedragsregels, continue doorlopende bewustwordingscampagnes, e-learning en berichten over actuele en nieuwe dreigingen.

Crisis oefeningen

Crisisoefeningen zijn een goede manier om met digitale dreigingen en weerbaarheid van de organisatie aan de slag te gaan. Hierbij leren we gezamenlijk, doen we ervaringen op en zijn we uiteindelijk beter voorbereid op potentiële ontwrichting bij een incident. Door met regelmaat te oefenen en het ervaren van een crisis, verhogen we de digitale weerbaarheid. Goed voorbereid zijn als gemeente is dan ook van cruciaal belang, om digitale ontwrichting te voorkomen en om alle digitale dienstverlening veilig en bereikbaar te houden.

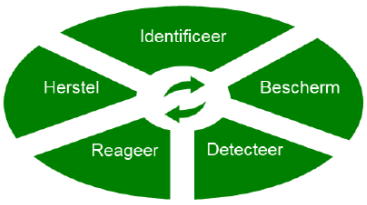
:

4 Organisatie van informatiebeveiliging

Dit hoofdstuk beschrijft hoe de taken en verantwoordelijkheden ten aanzien van informatiebeveiliging in gemeente Rotterdam belegd zijn. Binnen deze methodiek is het managementsysteem voor informatiebeveiliging leidend. De beschreven taken en verantwoordelijkheden sluiten aan bij het 'Concern Integraal Beveiligingsbeleid' en het binnen de gemeente bekende Three Lines-model. In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO, DISO's, Security Management, Security Operations Center (SOC) e.a.) ondersteunt, adviseert, coördineert, monitort en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

4.1 Managementsysteem

Binnen gemeente Rotterdam is informatiebeveiliging ingericht als een continu verbeterproces en sluit aan op de bestuurlijke P&C cyclus. Dit managementsysteem van informatiebeveiliging, in het vakgebied ook wel Information Security Management System (ISMS) genoemd, bestaat uit een vijftal stappen: Identificeer, Bescherm, Detecteer, Reageer en Herstel.



Titel: Gemeente Rotterdam - Informatieveiligheid is een continu proces

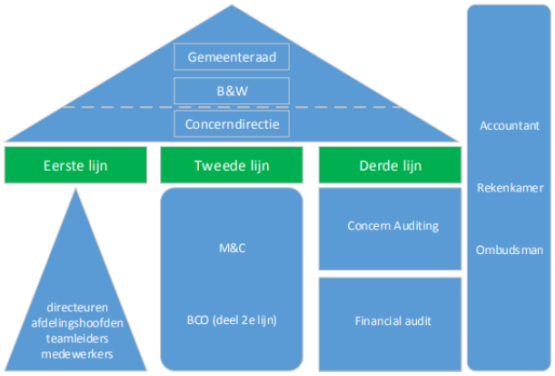
Met het doorlopen van de stappen Identificeer en Bescherm verlaagt de gemeente de kans van het optreden van een incident of kwetsbaarheid. De stappen Detecteer, Reageer en Herstel stelt de gemeente in staat de impact bij het optreden van een incident of kwetsbaarheid te verlagen.

Met dit management systeem werkt de gemeente aan de best mogelijk invulling van en maatregelen voor een *betrouwbare* informatievoorziening. Het concern brede ISMS ondersteunt het college van B en W en de concerndirectie in het maximaal 'in control' zijn van de informatieveiligheid.

Door periodieke controle en verantwoording, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het concern informatiebeveiligingsbeleid vormt samen met het Meerjarenplan Informatiebeveiliging het fundament onder een betrouwbare informatievoorziening. In het Meerjarenplan Informatiebeveiliging wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van externe ontwikkelingen in wet- en regelgeving, dreigingen, op basis van interne eisen aan vernieuwing van digitalisering, bevindingen naar aanleiding van uitgevoerde risicoanalyses en uit registraties in het incidentenregister.

4.2 Verschillende rollen en verantwoordelijkheden

De verschillende rollen en verantwoordelijkheden ten aanzien van informatiebeveiliging zijn conform het Three-Lines model[7] beschreven en geïmplementeerd binnen de gemeente.



Bron: Kadernota Sturen en Verantwoorden Rotterdam 2020

De first line (hierna: de eerste lijn) wordt gevormd door alle functionarissen die hiërarchisch of functioneel andere medewerkers aansturen en namens hen verantwoording afleggen. De eerste lijn, de concerndirectie en het management binnen de clusters zijn verantwoordelijk voor de resultaten, de uitvoering, nakoming van regels en de effectiviteit ten aanzien van informatiebeveiliging.

De second line (hierna: de tweede lijn) wordt gevormd door functionarissen die, onafhankelijk zijn van de eerste lijn. De tweede lijn, de informatieveiligheid-gebaseerde functies binnen de gehele informatiebeveiligingsketen zijn verantwoordelijk voor het stellen van kaders en regels. Alsmede voor advisering inzake informatieveiligheid en voor het op een objectieve wijze voeren van toezicht op en rapporteren over de uitvoering, het management, de beheersing en de verslaglegging van informatiebeveiligingsrisico's.

De third line (hierna: de derde lijn) wordt gevormd door de Functionaris Gegevensbescherming (FG) en de afdelingen Financial Audit en Concern Auditing. De derde lijn, is de onafhankelijk rol binnen de gemeente die verantwoordelijk is voor het geven van een onafhankelijk oordeel over de mate van functioneren van de interne informatiebeveiligingsmaatregelen. De derde lijn heeft verder een coördinerende rol richting de externe auditor en de toezichthouders.

4.3 Controle en verantwoording

Dit concern informatiebeveiligingsbeleid is een verantwoordelijkheid van het bestuur van gemeente Rotterdam. De bestuurders en concerndirecteuren van gemeente Rotterdam zullen volgens de strategische principes voor informatiebeveiliging en het concern brede management systeem richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

De concerndirectie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan de bestuurlijke portefeuillehouders. De concerndirectie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit concern informatiebeveiligingsbeleid.

[7] Kadernota 'Sturen en Verantwoorden Rotterdam 2020'

De gemeente verantwoordt zich jaarlijks over informatiebeveiliging middels de ENSIA-systematiek, gebaseerd op de normen die gelden voor de overheid, de BIO. De aangestelde ENSIA-coördinator zorgt ervoor dat de informatie die nodig is voor het beantwoorden van de audit-vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke proceseigenaren. De proceseigenaren leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten. Op basis van ENSIA vindt enerzijds de verantwoording aan de gemeenteraad plaats via een collegeverklaring informatiebeveiliging. Anderzijds vindt verantwoording plaats richting de toezichthouders van de ministeries inzake informatiebeveiliging van de BRP, SUWI, DigiD, BAG, ed..

Bron: VNG-realisatie; ENSIA

Middels deze verantwoording worden het college van B en W van gemeente Rotterdam en de gemeenteraad geïnformeerd. De betrokkenheid van het Gemeentebestuur is essentieel, en laat zien dat de gemeente Rotterdam informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

4.4 Afwijkingen van bestaand beleid en regelgeving

De implementatie van maatregelen kost in veel gevallen geld en/of tijd van de medewerkers en de gemeente. Omdat dit schaarse middelen zijn, kan het voorkomen dat bepaalde en dus benodigde beveiligingsmaatregelen niet of onvoldoende (tijdig) kunnen worden geïmplementeerd.

Afwijkingen van het concern informatiebeveiligingsbeleid en informatiebeveiligingsmaatregelen worden door de proceseigenaar inclusief een advies van de informatiebeveiligingsfunctionaris ter beoordeling voorgelegd aan de desbetreffende cluster directeur en bij cluster overstijgende impact aan de concerndirectie. De toegestane afwijkingen zullen aan een termijn van maximaal één jaar zijn gebonden. Voor het verstrijken van deze termijn dient de herbeoordeling plaats te vinden en ter beoordeling worden voorgelegd aan de cluster en/of concerndirectie.

Het desbetreffende cluster zorgt ervoor dat de besluitvorming rond deze afwijkingen goed gedocumenteerd wordt en steeds voor audits toegankelijk is. De informatiebeveiligingsfunctionaris bewaakt het totaaloverzicht en ziet er op toe dat de termijnen zorgvuldig bewaakt en gehandhaafd worden.

:

Bijlage A: Relevante documenten en bronnen

Relevante documenten en bronnen	Vindplaats	URL
Algemene Verordening Gegevensbescherming (AVG)	Website Wetten.nl Website gemeente Rotterdam	wetten.nl - Regeling - Uitvoeringswet Algemene verordening gegevensbescherming - BWBR0040940 (overheid.nl) https://www.rotterdam.nl/bestuur-organisatie/uw-gegevens/
Baseline Informatiebeveiliging Overheid (BIO)	Website VNG	https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/
Collegetargets 2018-2022	Website gemeente Rotterdam	https://www.rotterdam.nl/bestuur-organisatie/collegetargets-2018-2022/
Concern Informatiebeheerbeleid Rotterdam	Intranet gemeente Rotterdam	Wet- en regelgeving - RIO (rotterdam.nl)
Concern Integraal Beveiligingsbeleid Rotterdam		
Kadernota 'Sturen en Verantwoorden Rotterdam 2020'	Intranet gemeente Rotterdam	Kaders, beleid en richtlijnen - RIO (rotterdam.nl)
VNG resolutie 'Digitale Veiligheid: kerntaak voor de gemeenten'	Website VNG	https://vng.nl/nieuws/meer-prioriteit-voor-beveiliging-digitale-systemen-gemeenten
Regeling ICT- en informatiegebruik	Website Bestuurlijk Informatiesysteem Rotterdam	https://www.bis.rotterdam.nl/dossiers/43022
Meerjarenplan Informatiebeveiliging		
Informatiebeveiligingsbeleid (2018)	Website Raadsinformatie gemeente Rotterdam	https://rotterdam.raadsinformatie.nl/document/6124517/1#search="informatiebeveiligingsbeleid"
De 10 bestuurlijke principes voor informatiebeveiliging	Website VNG	https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf
ISO 27001 en 27002	Website NEN	https://www.nen.nl/ict/cyber-privacy/informatiebeveiliging
IEC 62443	Website NEN	https://www.nen.nl/
IEC25010	Website NEN	https://www.nen.nl/
NPR5326	Website NEN	https://www.nen.nl/
Verwerkingsregister gemeente Rotterdam	Website gemeente Rotterdam	https://www.rotterdam.nl/bestuur-organisatie/verwerkingsregister/
VNG-realisatie; ENSIA	Website VNG	https://www.vngrealisatie.nl/ensia

:

Ondertekening Convenant en Privacy protocol Samenwerking tussen ketenpartners Zorg- en Veiligheidshuis Rotterdam-Rijnmond, vastgesteld in het Algemeen Bestuur dd. 28-02-2024:

Ondergetekenden:

Naam organisatie:
Gemeente Albrandswaard

Vertegenwoordigd door bestuurder/directielid:

burgemeester drs. Jolanda de Witte

Handtekening: