Convenant Zorgtafel regio Oost-Brabant

Samenwerking tussen partners binnen de regio Oost-Brabant Slachtoffers Mensenhandel 18 - / 18 +

Context:

Met dit Samenwerkingsconvenant worden afspraken rondom de samenwerking tussen verschillende partijen binnen de Zorgtafel regio Oost-Brabant Slachtoffers Mensenhandel 18- / 18 + (hierna De Zorgtafel) geformaliseerd en vastgelegd. Uit dit Samenwerkingsconvenant blijkt wie, met welk doel en met welke inzet deelneemt aan de Zorgtafel, alsook wie waarover, op welk niveau, regie voert en hoe besluitvorming plaatsvindt.

Convenant samenwerking tussen ketenpartners binnen De Zorgtafel

De ondergetekenden:

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Asten

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Bergeijk

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Bernheze

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Best

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Bladel

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Boekel

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Boxmeer

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Boxtel

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Cranendonck

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Cuijk

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Deurne

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Eersel

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Eindhoven

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Geldrop-Mierlo

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Gemert-Bakel

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Grave

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Heeze-Leende

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Helmond

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente ’s-Hertogenbosch

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Laarbeek

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Landerd

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Meierijstad

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Mill en St. Hubert

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Nuenen

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Oirschot

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Oss

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Reusel De Mierden

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Sint Anthonis

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Sint-Michielsgestel

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Someren

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Son en Breugel

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Uden

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Valkenswaard

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Veldhoven

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Vught

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente Waalre

verder *afzonderlijk* aangeduid als 'Partij' of 'Gemeente',

en

Bijzonder Jeugdwerk, gevestigd te Deurne en kantoorhoudend te Mr. De Jonghlaan 4, hierbij rechtsgeldig vertegenwoordigd door mevr. A. de Wit, adjunct directeur;

Cello, gevestigd te Vught en kantoorhoudend te De Ring 14, hierbij rechtsgeldig vertegenwoordigd door dhr. F. van Beers, voorzitter Raad van Bestuur;

COA Budel-Cranendonck, gevestigd te Budel en kantoorhoudend te Randweg-Oost 32, hierbij rechtsgeldig vertegenwoordigd door dhr. L. ter Hark, locatiemanager;

COA Grave, gevestigd te Rheden en kantoorhoudend te Intendanceplantsoen 1, hierbij rechtsgeldig vertegenwoordigd door [*naam, functie]*

COA Overloon, gevestigd te [*plaatsnaam*] en kantoorhoudend te [*adres*], hierbij rechtsgeldig vertegenwoordigd door [*naam, functie*]

Farent, gevestigd te 's-Hertogenbosch en kantoorhoudend te Rogier van der Weydenstraat 2, hierbij rechtsgeldig vertegenwoordigd door mevr. H. Jacobs, bestuurder;

GGD Brabant-Zuidoost, gevestigd te Eindhoven en kantoorhoudend te Clausplein 10, hierbij rechtsgeldig vertegenwoordigd door mevr. E. Jeurissen, directeur;

GGD Hart voor Brabant vestiging 's-Hertogenbosch, gevestigd te 's-Hertogenbosch en kantoorhoudend te Vogelstraat 2, hierbij rechtsgeldig vertegenwoordigd door *[naam, functie];*

GGZ Oost Brabant Regio Helmond-Peelland, gevestigd te Helmond en kantoorhoudend te Wesselmanlaan 25a, hierbij rechtsgeldig vertegenwoordigd door dhr. H. Hanegraaf, geneesheer-directeur;

GGZ Oost Brabant Land van Cuijk en Noord-Limburg, gevestigd te Boxmeer en kantoorhoudend te Bilderbeekstraat 44, hierbij rechtsgeldig vertegenwoordigd door dhr. H. Hanegraaf, geneesheer-directeur;

GGZ Oost Brabant Regio Oss-Uden-Veghel, gevestigd, te Veghel en kantoorhoudend te Gezondheidslaan 65, hierbij rechtsgeldig vertegenwoordigd door dhr. H. Hanegraaf, geneesheer-directeur;

Humanitas District Zuid, gevestigd te Eindhoven en kantoorhoudend te Zernikestraat 11-13, hierbij rechtsgeldig vertegenwoordigd door dhr. R. Derkx, districtsmanager Humanitas Zuid;

Koninklijke Marechaussee Brigade Brabant-Zuid, gevestigd te Eindhoven en kantoorhoudend te Luchthavenweg 63, hierbij rechtsgeldig vertegenwoordigd door [*naam, functie*];

Koraal locatie De La Salle, gevestigd te Boxtel en kantoorhoudend te Schijndelseweg 1, hierbij rechtsgeldig vertegenwoordigd door mevr. C. Bogers, regiodirecteur Noordoost Brabant;

Leger des Heils, gevestigd te Eindhoven en kantoorhoudend te Raiffeisenstraat 1, hierbij rechtsgeldig vertegenwoordigd door mevr. J. Wisseborn, directeur;

LEV Groep, gevestigd te Helmond en kantoorhoudend te Penningstraat 55, hierbij rechtsgeldig vertegenwoordigd door dhr. J. Ragetlie, bestuurder;

Lumens, gevestigd te Eindhoven en kantoorhoudend te Beemdstraat 29, hierbij rechtsgeldig vertegenwoordigd door mevr. J. Vonk, bestuurder;

Maatschappelijke Opvang Den Bosch, gevestigd te ’s-Hertogenbosch en kantoorhoudend te Aartshertogenlaan 23, hierbij rechtsgeldig vertegenwoordigd door dhr. B. van Eijk, directeur;

MEE regio ’s-Hertogenbosch, gevestigd te ’s-Hertogenbosch en kantoorhoudend te Sint Teunislaan 3, hierbij rechtsgeldig vertegenwoordigd door mevr. Bomhof-Bonekamp, Raad van Bestuur ;

NEOS, Nieuwe Eindhovense Opvang Stichting, gevestigd te Eindhoven en kantoorhoudend te Keizer Karel V Singel 45, hierbij rechtsgeldig vertegenwoordigd door dhr. P. Dijkstra, Voorzitter Raad van Bestuur;

Novadic Kentron, gevestigd te Vught en kantoorhoudend te Hogedwarsstraat 3, hierbij rechtsgeldig vertegenwoordigd door dhr. W. Tibosch, voorzitter Raad van Bestuur;

Ons Welzijn, gevestigd te Oss en kantoorhoudend te Schadewijkstraat 6, hierbij rechtsgeldig vertegenwoordigd door [*naam, functie*];

PlusTeam Geldrop-Mierlo, gevestigd te Geldrop en kantoorhoudend te De Meent 2, hierbij rechtsgeldig vertegenwoordigd door mevr. A. van der Velden, manager;

Oosterpoort, gevestigd te Oss en kantoorhoudend te Kamperfoeliestraat 60, hierbij rechtsgeldig vertegenwoordigd door dhr. G. Schep, bestuurder;

Politie Eenheid Oost-Brabant, gevestigd te ‘s-Hertogenbosch en kantoorhoudend te Vogelstraat 41, hierbij rechtsgeldig vertegenwoordigd door dhr. W. Paulissen, Politiechef Eenheid Oost-Brabant*;*

Reinier van Arkel, gevestigd te ’s-Hertogenbosch en kantoorhoudend te Bethaniestraat 2, hierbij rechtsgeldig vertegenwoordigd door dhr. E. van Doorn, directeur;

Sociom, gevestigd te Cuijk en kantoorhoudend te Zwaanstraat 7, hierbij rechtsgeldig vertegenwoordigd door dhr. R. van der Heijden, directeur-bestuurder;

Stichting Maatschappelijke Opvang Helmond, gevestigd te Helmond en kantoorhoudend te St. Hubertusstraat 2, hierbij rechtsgeldig vertegenwoordigd door mevr. K. de Laat, directeur bestuurder;

Veilig Thuis Brabant Noordoost, gevestigd te ’s-Hertogenbosch en kantoorhoudend te Oude Vlijmenseweg 112, hierbij rechtsgeldig vertegenwoordigd door mevr. T. Hummeling, directeur;

Veilig Thuis Zuidoost-Brabant, gevestigd te Helmond en kantoorhoudend te Sobriëtasplein 102, hierbij rechtsgeldig vertegenwoordigd door mevr. J. Kuijpers, directeur;

Verdihuis, gevestigd te Oss en kantoorhoudend te Kardinaal de Jongstraat 17, hierbij rechtsgeldig vertegenwoordigd door dhr. H. Kremers, directeur;

WIJeindhoven, gevestigd te Eindhoven en kantoorhoudend te Winston Churchilllaan 79, hierbij rechtsgeldig vertegenwoordigd door dhr. L. van Eijndhoven, bestuurder;

hierna afzonderlijk te noemen 'Partij' en gezamenlijk, inclusief de hierboven vermelde colleges van B&W van de genoemde gemeenten, te noemen 'Partijen',

de volgende overwegingen in aanmerking nemende:

- Partijen in het kader van samenwerking op het gebied van zorg aan slachtoffers van mensenhandel De Zorgtafel hebben opgezet;
- Van belang is dat Partijen personele bijdragen blijven leveren in de vorm van partnerbijdragen aan casus-overleggen en/of structurele deelname aan De Zorgtafel;
- Partijen hun eigen bevoegdheden houden met betrekking tot de binnen De Zorgtafel besproken casuïstiek en De Zorgtafel 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 probleemsituaties die binnen de Zorgtafel 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 binnen De Zorgtafel 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 slachtoffers mensenhandel 18 - / 18 + te willen vastleggen in een samenwerkingsconvenant;
- De afspraken rondom de verwerking van persoonsgegevens in het Privacy Protocol Zorgtafel regio Oost-Brabant 18 - / 18 + (hierna 'Privacy Protocol Zorgtafel regio Oost-Brabant) zijn vastgelegd, dat integraal onderdeel is van dit samenwerkingsconvenant;
- Dit samenwerkingsconvenant verder wordt aangehaald als 'het Convenant'.

verklaren te zijn overeengekomen:

Artikel 1. Definities

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

1.1. Aanmelding en Intake: het voordragen van een Casus door één der Partijen en het uitwisselen van informatie, waaronder Persoonsgegevens, tussen de Procesregisseur van De Zorgtafel en de aanmeldende Partij ter toetsing of de Casus in aanmerking komt voor behandeling binnen De Zorgtafel.

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

1.3. Betrokkene: de natuurlijke persoon op wie informatie, waaronder persoonsgegevens zoals beschreven in het Privacy Protocol Zorgtafel regio Oost-Brabant Slachtoffers Mensenhandel 18 - / 18 +, betrekking heeft;

1.4. Casus: een geval of situatie dat of die voldoet aan de criteria voor Zorgtafel-casuïstiek zoals geformuleerd in Bijlage 2, en die is aangemeld bij De Zorgtafel ter beoordeling en eventuele bespreking in het Casusoverleg;

1.5. Casusoverleg: fase waarin overleg plaatsvindt door Partijen gericht op de totstandkoming van een plan van aanpak, afstemming tijdens de uitvoering daarvan, en het beoordelen of de Casus kan worden afgeschaald;

1.6. 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;

1.7. Casusregisseur: de medewerker van een van de Partijen die is belast met de taken zoals geformuleerd in artikel 13;

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

1.9. Managers: de personen die zijn belast met de taken zoals geformuleerd in Artikel 11;

1.10. Partneroverleg: het verband van afgevaardigden van Partijen zoals geformuleerd in Artikel 6;

1.11. 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;

1.12. Procesregisseur: de medewerker van De Zorgtafel die namens een van de Partijen is belast met de werkzaamheden zoals geformuleerd in artikel 12. In de praktijk zal de term ‘Zorgcoördinator Mensenhandel’ worden gebruikt voor het begrip Procesregisseur;

1.13. Regionale Tafel Mensenhandel Oost-Brabant: het verband van afgevaardigden van Partijen zoals geformuleerd in Artikel 4;

1.14. Strategische Regie: de coördinatie van regionale samenwerking binnen De Zorgtafel, verbinding van verschillende ketens en afstemming met andere lokale en regionale samenwerkingsverbanden, organisaties en overlegtafels.

1.15. 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.

1.16. Werkproces: het door het Partneroverleg op grond van Artikel 6.6, onder c, vastgestelde proces voor samenwerking binnen De Zorgtafel, waaronder het proces omtrent en het delen van informatie en het op- en afschalen van een Casus.

Artikel 2. Doel en Functie van De Zorgtafel

2.1. De Zorgtafel is een samenwerkingsverband op het terrein van zorg voor slachtoffers mensenhandel waarin zorgpartners, de politie en de gemeente, onder eenduidige regie, zorg

bieden aan slachtoffers mensenhandel. De doelstelling van de samenwerking is het bieden van zorg aan slachtoffers gericht op het voorkomen van (verder) slachtofferschap, het verwerken van het slachtofferschap en het bieden van perspectief op een bestaan zonder gedwongen prostitutie.

2.2. Om het onder 2.1 geformuleerde doel te bereiken heeft De Zorgtafel drie functies:

a) Het faciliteren en regisseren van casusoverleggen waar casuïstiek wordt besproken;
b) Het functioneren als regionaal expertise samenwerkingsverband voor multidisciplinaire zorg- en veiligheidsproblematiek en vraagbaak voor ketenpartners en professionals;
c) Het signaleren van relevante trends en ontwikkelingen en (strategisch) adviseren van bestuurders en sleutelpartners;

De partners realiseren dit doel door in de vorm van gestructureerd en ad hoc overleg:

- risico's op gedwongen prostitutie en mensenhandel te signaleren en te analyseren;
- zicht te krijgen op de situatie waarin mogelijke slachtoffers verkeren;
- afspraken te maken over de wijze waarop contact kan worden gelegd met (mogelijke) slachtoffers en over de zorg die hen door de partners kan worden geboden;
- de (effecten van) de zorg die aan slachtoffers wordt geboden te monitoren.

Artikel 3. Structuur van De Zorgtafel

3.1. De Zorgtafel kent de volgende structuur:

a. de Regionale Tafel Mensenhandel Oost-Brabant;
b. het Partneroverleg;
c. Het Casusoverleg;
d. de Managers;
e. de Procesregisseur;
f. de Casusregisseur;
g. ondersteunend Personeel.

Artikel 4. De Regionale Tafel Mensenhandel Oost-Brabant

4.1. De Zorgtafel heeft de Regionale Tafel Mensenhandel Oost-Brabant die fungeert als het bestuur van De Zorgtafel. De Regionale Tafel Mensenhandel Oost-Brabant is verantwoordelijk voor de Strategische Regie van De Zorgtafel;

4.2. De Regionale Tafel Mensenhandel Oost-Brabant komt drie keer per jaar bij elkaar. De vergaderingen van de Regionale Tafel Mensenhandel Oost-Brabant vinden in beginsel plaats op locatie van het gemeentehuis van de gemeente Best.

4.3. De Regionale Tafel Mensenhandel Oost-Brabant bestaat uit vertegenwoordigers van een aantal Partijen, te weten:

- de burgemeester van de gemeente Grave, tevens voorzitter van de Regionale Tafel Mensenhandel Oost-Brabant;
- de burgemeester van de gemeente Best;
- een afgevaardigde van de politie, Afdeling Vreemdelingenpolitie Identificatie en Mensenhandel van de eenheid Oost-Brabant;
- een Officier van Justitie van het Openbaar Ministerie;
- de Ketenregisseur Mensenhandel Oost-Brabant, tevens secretaris van de Regionale Tafel Mensenhandel Oost-Brabant;
- een afgevaardigde van het Regiobureau Integrale Veiligheid Oost-Brabant;
- een afgevaardigde van het RIEC Oost-Brabant;
- een afgevaardigde van De Inspectie SZW van het Ministerie van Sociale Zaken en Werkgelegenheid;
- een afgevaardigde namens de zorgcoördinatie;
- een afgevaardigde namens gemeente Eindhoven;
- een afgevaardigde namens gemeente Valkenswaard.

4.4. De leden van de Regionale Tafel Mensenhandel Oost-Brabant zorgen voor voldoende mandaat vanuit de bevoegde persoon in de eigen organisatie om deel te nemen en bindende besluiten te nemen in de Regionale Tafel Mensenhandel Oost-Brabant voor de partij(en) die zij in de Regionale Tafel Mensenhandel Oost-Brabant vertegenwoordigen.

4.5. De secretaris van de Regionale Tafel Mensenhandel Oost-Brabant is verantwoordelijk voor het organiseren van de vergaderingen, het samenstellen van de agenda op basis van inbreng vanuit het Partneroverleg en de leden van de Regionale Tafel Mensenhandel Oost-Brabant en het opstellen en verspreiden van het verslag van de betreffende vergadering.

Artikel 5. Besluitvorming Regionale Tafel Mensenhandel Oost-Brabant

5.1. De Regionale Tafel Mensenhandel Oost-Brabant neemt besluiten over de Strategische Regie binnen De Zorgtafel.

5.2. Besluiten zijn bindend voor alle Partijen die aan dit Convenant deelnemen, voor zover niet strijdig met de wettelijke taken, bevoegdheden en beroepsnormen van Partijen.

5.3. Bij afwezigheid van een lid van de Regionale Tafel Mensenhandel Oost-Brabant 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.

5.4. De secretaris van de Regionale Tafel Mensenhandel Oost-Brabant informeert indien nodig het Partneroverleg schriftelijk over de binnen de Regionale Tafel Mensenhandel Oost-Brabant genomen besluiten.

5.5. De vergaderingen van de Regionale Tafel Mensenhandel Oost-Brabant zijn niet openbaar.

Artikel 6. Partneroverleg

6.1. Partijen binnen De Zorgtafel voeren ter uitvoering van de in artikel 2 bepaalde doeleinden onderling overleg op tactisch niveau: het ‘Partneroverleg’.

6.2. Het Partneroverleg vindt twee keer per jaar plaats en wanneer een Partij hier een verzoek toe indient.

6.3. Het Partneroverleg bestaat uit:

a) één afgevaardigde van iedere Partij of door de Procesregisseur aangewezen Partijen;
b) de Managers van De Zorgtafel; en
c) een secretaris.

6.4. De secretaris is aangewezen door de Regionale Tafel Mensenhandel en valt onder verantwoordelijkheid van de Regionale Tafel Mensenhandel.

6.5. De afgevaardigden van Partijen hebben het mandaat of de machtiging om op tactisch niveau sturing te geven aan de operationele processen van De Zorgtafel en besluiten te nemen met betrekking tot uitvoering van de onder Artikel 6.6 geformuleerde taken.

6.6. Het Partneroverleg heeft de volgende taken:

a) Op tactisch niveau sturing geven aan de operationele processen van De Zorgtafel;
b) Formuleren van voorstellen en vragen ten behoeve van of ter besluitvorming in de Regionale Tafel Mensenhandel Oost-Brabant;
c) In samenwerking met de Managers opstellen van het operationele Werkproces. Een kopie van het door het Partneroverleg vastgestelde Werkproces wordt aan alle Partijen verstrekt;
d) Het afstemmen van externe communicaties;
e) Het netwerk versterken en regionale samenwerking bespreking.

6.7. De secretaris van het Partneroverleg is verantwoordelijk voor het organiseren van de vergaderingen, het samenstellen van de agenda op basis van inbreng van de leden van het Partneroverleg (en eventueel inbreng vanuit de Regionale Tafel Mensenhandel Oost-Brabant) en het opstellen en verspreiden van het verslag van de betreffende vergadering,

alsook het informeren van de Regionale Tafel Mensenhandel Oost-Brabant over de in het Partneroverleg genomen relevante besluiten.

Artikel 7. Besluitvorming Partneroverleg

7.1. Besluiten in het Partneroverleg 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.

7.2. Bij afwezigheid van een lid van het Partneroverleg 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.

7.3. Indien het Partneroverleg niet tot een besluit kan komen, wordt de aangelegenheid ter beslissing voorgelegd aan de Regionale Tafel Mensenhandel Oost-Brabant.

7.4. De secretaris van het Partneroverleg informeert de Regionale Tafel Mensenhandel Oost-Brabant schriftelijk over de in het Partneroverleg genomen relevante besluiten.

7.5. De vergaderingen van het Partneroverleg zijn niet openbaar.

Artikel 8. Het Casusoverleg

8.1. Partijen binnen De Zorgtafel 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.

8.2. Het Casusoverleg bestaat uit afgevaardigden van Partijen, aangewezen door de Procesregisseur conform Artikel 12.

8.3. De afgevaardigden van Partijen hebben het mandaat om op operationeel niveau besluiten te nemen over de behandeling van een Casus.

8.4. 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.

8.5. 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 8.4, onder b.

8.6. De Casusregisseur stemt waar nodig af met de Procesregisseur voor wat betreft de uitvoering van de onder artikel 8.4 genoemde taken.

Artikel 9. Afspraken Casusoverleg

9.1. In het Casusoverleg worden in gezamenlijkheid afspraken gemaakt.

9.2. De vergaderingen van het Casusoverleg zijn niet openbaar. Informatieverstrekking aan derden omtrent hetgeen wordt besproken in het Casusoverleg vindt slechts plaats conform het Convenant, het Privacy Protocol Zorgtafel regio Oost-Brabant, binnen de voor Partijen geldende wettelijke kaders en slechts na voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke zoals bedoeld in het Privacy Protocol Zorgtafel regio Oost-Brabant, die de betreffende informatie oorspronkelijk aan het samenwerkingsverband heeft verstrekt.

Artikel 10. Contactpersonen

10.1. De afgevaardigden in het Partneroverleg, de Regionale Tafel Mensenhandel Oost-Brabant en het Casusoverleg fungeren tevens als contactpersoon voor de secretarissen van de Regionale Tafel Mensenhandel Oost-Brabant c.q. het Partneroverleg, de Managers van De Zorgtafel, de Procesregisseur en indien van toepassing, de Casusregisseur.

Artikel 11. Managers

11.1. Het dagelijks bestuur van De Zorgtafel is belegd bij de Managers van De Zorgtafel ('de Managers').

11.2. De Managers vallen onder de verantwoordelijkheid van gemeente Helmond, Lumens en de Maatschappelijke Opvang Den Bosch (hierna MO Den Bosch).

11.3. De Managers hebben de volgende taken en bevoegdheden:

a. Het vaststellen van de operationele werkprocessen;
b. Het aansturen van personeel;
c. Het optreden als woordvoerder voor De Zorgtafel in overleg met het Partneroverleg;
d. Het informeren van de Regionale Tafel Mensenhandel Oost-Brabant omtrent de voortgang van de samenwerking binnen De Zorgtafel door Partijen door het opstellen van een jaarlijkse rapportage met aantallen casussen die zijn behandeld, aantallen casussen die succesvol zijn afgerond en overige aandachtspunten.

11.4. Geschillen omtrent de uitvoering van de taken door de Managers worden voorgelegd aan de Regionale Tafel Mensenhandel Oost-Brabant.

Artikel 12. Procesregisseur

12.1. De Procesregisseur is bevoegd en verantwoordelijk voor de Procesregie binnen De Zorgtafel.

12.2. 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 binnen De Zorgtafel;
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 gespreksthema'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 De Zorgtafel 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;

12.3. De Procesregisseur werkt voor wat betreft de taken genoemd onder artikel 12.2 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 12.2, onder h, onder de gezamenlijke verantwoordelijkheid van Partijen.

12.4. Geschillen omtrent de uitvoering van zijn taken door de Procesregisseur worden voorgelegd aan de Managers. De Managers kunnen het geschil waar nodig voorleggen aan de Regionale Tafel Mensenhandel Oost-Brabant.

Artikel 13. Casusregisseur

13.1. Conform artikel 8.4, 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.

13.2. De Casusregisseur is belast met het toezicht op de naleving van de afspraken zoals die zijn vastgelegd in het plan van aanpak.

13.3. De Casusregisseur stemt af met de Procesregisseur voor wat betreft de voortgang van het plan van aanpak.

13.4. Geschillen omtrent de uitvoering van taken door een Casusregisseur worden voorgelegd aan de Procesregisseur. Deze kan, indien noodzakelijk, het geschil ter beslechting voorleggen aan het Partneroverleg.

Artikel 14. Ondersteunend Personeel

14.1. De Zorgtafel wordt ondersteund door één of meerdere administratieve medewerkers. Gemeente Helmond, Lumens en MO Den Bosch dragen zorg voor voldoende personele ondersteuning binnen De Zorgtafel. Dit personeel werkt onder de verantwoordelijkheid van Gemeente Helmond, Lumens en MO Den Bosch.

14.2. De Managers kunnen, buiten het inzetten van personeel dat in loondienst is bij Gemeente Helmond, Lumens en MO Den Bosch, besluiten personeel op grond van een dienstverleningsovereenkomst in te zetten. Dit personeel werkt onder verantwoordelijkheid Gemeente Helmond, Lumens en MO Den Bosch.

14.3. De dagelijkse aansturing van het personeel gebeurt door de Managers.

Artikel 15. Uitwisseling van informatie

15.1. Partijen voorzien elkaar van alle noodzakelijke informatie voor het behalen van de doelstellingen van De Zorgtafel 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 De Zorgtafel. 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 16, lid 2.

15.2. Voor zover het de verwerking van persoonsgegevens, waaronder (bijzondere) persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming of de Wet politiegegevens betreft, handelen partijen overeenkomstig het Privacy Protocol Zorgtafel regio Oost-Brabant, in het bijzonder voor wat betreft de daarin vastgelegde doeleinden en grondslagen voor die verwerking.

Artikel 16. Interventie en het gebruik van informatie

16.1. Partijen behouden hun eigen bevoegdheden met betrekking tot de binnen De Zorgtafel besproken Casussen. Afzonderlijk optreden op basis van eigen informatie blijft door samenwerking binnen De Zorgtafel 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.

16.2. 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 Zorgtafel regio Oost-Brabant. Partijen verklaren het Privacy Protocol Zorgtafel regio Oost-Brabant te onderschrijven en daarnaar in het kader van samenwerking binnen De Zorgtafel te zullen handelen.

Artikel 17. Geheimhouding en beveiliging

17.1. Partijen nemen conform de toepasselijke wettelijke bepalingen en ongeacht de duur van dit Convenant strikte geheimhouding in acht over elkaars organisatie, over 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 9.2 en Artikel 15.

17.2. Partijen staan ervoor in dat hun personeel bekend is met de in dit artikel vastgestelde verplichting en de naleving hiervan nakomen.

17.3. 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 binnen De Zorgtafel wordt zorg gedragen door Gemeente Helmond, Lumens en MO Den Bosch, conform het Informatiebeveiligingsbeleid De Zorgtafel, meegeleverd in Bijlage 4. Gemeente Helmond, Lumens en MO Den Bosch stellen de benodigde middelen ter beschikking voor de uitvoering van dat Informatiebeveiligingsbeleid door De Zorgtafel.

17.4. Artikel 12 t/m 14 van het Privacy Protocol beschrijven de beveiliging, geheimhouding en de procedure bij datalekken.

Artikel 18. Financiering en overige bijdragen

18.1. Partijen zijn ieder voor zich verantwoordelijk voor het dragen van financiële lasten voor deelname aan De Zorgtafel in het kader van dit Convenant.

Artikel 19. Communicatie

19.1. Partijen communiceren niet afzonderlijk naar derden over de samenwerking binnen De Zorgtafel in het kader van de uitvoering van dit Convenant, zonder voorafgaande instemming van de andere Partijen en met inachtneming van het bepaalde in Artikel 9.2 en Artikel 15.

19.2. De Managers zien toe op het coördineren van communicatie naar derden en treedt op als woordvoerder voor De Zorgtafel.

Artikel 20. Toetreding

20.1. 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.

20.2. Een organisatie die tot dit Convenant wil toetreden kan daartoe een aanvraag doen bij de Regionale Tafel Mensenhandel Oost-Brabant via de Managers.

20.3. Partijen worden vooraf door de secretaris van de Regionale Tafel Mensenhandel Oost-Brabant op de hoogte gebracht van de voorgenomen toetreding.

20.4. De Regionale Tafel Mensenhandel Oost-Brabant 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 Bijlage 1 bij dit Convenant door die andere organisatie en de voorzitter van de Regionale Tafel Mensenhandel Oost-Brabant.

Artikel 21. Wijzigingen

21.1. De bepalingen in dit Convenant kunnen door de Partijen in gezamenlijk overleg worden gewijzigd. Wijzigingen in dit Convenant worden door de Regionale Tafel Mensenhandel Oost-Brabant 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 de Regionale Tafel Mensenhandel Oost-Brabant.

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

21.3. 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 De Zorgtafel schriftelijk opzeggen met ingang van het tijdstip waarop het gewijzigde Convenant van kracht wordt.

Artikel 22. Aansprakelijkheid

22.1. Zie artikel 25 van het Privacy Protocol.

Artikel 23. Duur, opzegging, beëindiging

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

23.2. De Regionale Tafel Mensenhandel Oost-Brabant kan, zonder rechterlijke tussenkomst en met meerderheid van stemmen, na ingebrekestelling, een Partij met onmiddellijke ingang uitsluiten van de samenwerking binnen De Zorgtafel, indien de afspraken zoals neergelegd in dit Convenant niet door de desbetreffende Partij worden nagekomen.

23.3. 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 24. Opvolging

24.1. Dit Convenant vervangt alle eerdere door Partijen gesloten Convenanten met betrekking tot samenwerking binnen De Zorgtafel.

Artikel 25. Toepasselijk recht

25.1. Op dit Convenant is Nederlands recht van toepassing.

Aldus overeengekomen:

Gemeente Asten
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Bergeijk
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Bernheze
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Best
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Bladel
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Boekel
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Boxmeer
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Boxtel
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Cranendonck
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Cuijk
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Deurne
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Eersel
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Eindhoven
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Geldrop-Mierlo
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Gemert-Bakel
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Grave
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Heeze-Leende
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Helmond
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente ‘s-Hertogenbosch
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Laarbeek
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Landerd
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Meierijstad
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Mill en St. Hubert
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Nuenen
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Oirschot
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Oss
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Reusel De Mierden
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Sint Anthonis
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Sint-Michielsgestel
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Someren
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Son en Breugel
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Uden
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Valkenswaard
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Veldhoven
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Vught
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Gemeente Waalre
in dezen rechtsgeldig vertegenwoordig door: de burgemeester
Datum en plaats:

Bijzonder Jeugdwerk
in dezen rechtsgeldig vertegenwoordig door: mevr. A. de Wit, adjunct directeur
Datum en plaats:

Cello
in dezen rechtsgeldig vertegenwoordig door: dhr. F. van Beers, voorzitter Raad van Bestuur
Datum en plaats:

COA Budel-Cranendonck
in dezen rechtsgeldig vertegenwoordig door: dhr. L. ter Hark, locatiemanager
Datum en plaats:

COA Grave
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

COA Overloon
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

Farent
in dezen rechtsgeldig vertegenwoordig door: mevr. H. Jacobs, bestuurder
Datum en plaats:

GGD Brabant-Zuidoost
in dezen rechtsgeldig vertegenwoordig door: mevr. E. Jeurissen, directeur
Datum en plaats:

GGD Hart voor Brabant
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

GGZ Oost Brabant Regio Helmond-Peelland
in dezen rechtsgeldig vertegenwoordig door: dhr. H. Hanegraaf, geneesheer-directeur
Datum en plaats:

GGZ Oost Brabant Land van Cuijk en Noord- Limburg
in dezen rechtsgeldig vertegenwoordig door: dhr. H. Hanegraaf, geneesheer-directeur
Datum en plaats:

GGZ Oost Brabant Regio Oss-Uden-Veghel
in dezen rechtsgeldig vertegenwoordig door: dhr. H. Hanegraaf, geneesheer-directeur
Datum en plaats:

Humanitas District Zuid
in dezen rechtsgeldig vertegenwoordig door: dhr. R. Derkx, districtsmanager Humanitas Zuid
Datum en plaats:

Koninklijke Marechaussee Brigade Brabant-Zuid
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

Koraal locatie De La Salle
in dezen rechtsgeldig vertegenwoordig door: mevr. C. Bogers, regiodirecteur Noordoost Brabant
Datum en plaats:

Leger des Heils
in dezen rechtsgeldig vertegenwoordig door: mevr. J. Wisseborn, directeur
Datum en plaats:

LEV Groep
in dezen rechtsgeldig vertegenwoordig door: dhr. J. Ragetlie, bestuurder
Datum en plaats:

Lumens
in dezen rechtsgeldig vertegenwoordig door: mevr. J. Vonk, bestuurder
Datum en plaats:

Maatschappelijke Opvang Den Bosch
in dezen rechtsgeldig vertegenwoordig door: B. van Eijk, directeur
Datum en plaats:

MEE regio 's-Hertogenbosch
in dezen rechtsgeldig vertegenwoordig door: mevr. Bomhof-Bonekamp, Raad van Bestuur
Datum en plaats:

NEOS, Nieuwe Eindhovense Opvang Stichting
in dezen rechtsgeldig vertegenwoordig door: dhr. P. Dijkstra, voorzitter Raad van Bestuur
Datum en plaats:

Novadic Kentron
in dezen rechtsgeldig vertegenwoordig door: dhr. W. Tibosch, voorzitter Raad van Bestuur
Datum en plaats:

Ons Welzijn
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

Oosterpoort
in dezen rechtsgeldig vertegenwoordig door: dhr. G. Schep, bestuurder
Datum en plaats:

PlusTeam Geldrop-Mierlo
in dezen rechtsgeldig vertegenwoordig door: mevr. A. van der Velden, manager
Datum en plaats:

Politie Eenheid Oost-Brabant
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

Reinier van Arkel
in dezen rechtsgeldig vertegenwoordig door: dhr. E. van Doorn, directeur
Datum en plaats:

Sociom
in dezen rechtsgeldig vertegenwoordig door: dhr. R. van der Heijden, directeur-bestuurder;
Datum en plaats:

Stichting Maatschappelijke Opvang Helmond
in dezen rechtsgeldig vertegenwoordig door: dhr. J. Feuerrigel, Raad van Bestuur
Datum en plaats:

Veilig Thuis Brabant Noordoost
in dezen rechtsgeldig vertegenwoordig door: mevr. T. Hummeling, directeur
Datum en plaats:

Veilig Thuis Zuidoost-Brabant
in dezen rechtsgeldig vertegenwoordig door: mevr. J. Kuijpers, directeur
Datum en plaats:

Verdihuis
in dezen rechtsgeldig vertegenwoordig door: dhr. H. Kremers, directeur
Datum en plaats:

Wijeindhoven
in dezen rechtsgeldig vertegenwoordig door: dhr. L. van Eijndhoven, bestuurder
Datum en plaats:

Bijlage 1: Toetredingsformulier nieuwe partner tot Convenant

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

overwegende dat:

- Deelname aan het Convenant gelet op de publieke en/of maatschappelijke taak die zichzelf in het kader van de casuïstiek Slachtoffers Mensenhandel 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;
- De Regionale Tafel Mensenhandel Oost-Brabant positief heeft besloten op toetreding van ondergetekende aan het Convenant;

verklaart daartoe het volgende:

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

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

Naam organisatie:
Naam bevoegde functionaris:

…….

Namens de Regionale Tafel Mensenhandel Oost-Brabant:
Naam:

……

Bijlage 2: Criteria Zorgtafel-Casuïstiek

De Zorgtafel behandelt casussen waarin de verbinding tussen de zorg en interventies vanuit de gemeente en haar partners voorwaarde is voor een succesvolle, duurzame aanpak van slachtoffers mensenhandel.

Een casus wordt binnen De Zorgtafel behandelt wanneer deze aan de volgende criteria voldoet:

- Er is sprake van ernstige lokale of gebieds-gebonden veiligheidsproblematiek, die vraagt om een keten-overstijgende aanpak, of;
- De problematiek wordt beïnvloed door en heeft impact op het (gezins-)systeem en/of de directe sociale leefomgeving (of wordt verwacht dat te gaan hebben):
- Samenwerking tussen meerdere ketens (minimaal dwang en drang) is nodig om tot een effectieve aanpak te komen; het is in de reguliere samenwerking tussen partners binnen één keten niet mogelijk om deze problematiek effectief aan te pakken; en:
- Er is sprake van meerdere problemen (multiproblem) die op meer dan één leefgebied spelen.

Opschaling
De Zorgcoördinatoren Mensenhandel van de regio Oost-Brabant kunnen ten alle tijden besluiten om een casus op te schalen naar één van de twee Zorg- en Veiligheidshuizen van de regio Oost-Brabant. Opschaling kan bijvoorbeeld nodig zijn om een doorbraak in een casus te forceren of wanneer casuïstiek op het snijvlak van zorg- en veiligheid moet worden behandeld. Hierover zijn reeds afspraken gemaakt bij het Zorg- en Veiligheidshuis Brabant Zuidoost en het Zorg- en Veiligheidshuis Brabant Noordoost.

Bijlage 3: Informatiebeveiligingsbeleid

Informatiebeveiligingsbeleid Gemeente Helmond dd. december 2019

Gemeente Helmond

Strategisch informatiebeveiligingsbeleid

Gemeente Helmond 2020 – 2024

Aan:	College B&W, Directie Team Bedrijfsvoering
Auteur:	D. Edelaar
Datum:	december 2019
Status:	definitief
Afschrift:	CIO office, DSPO's, Kernteam

Inhoudsopgave

1 Ambitie Informatieveiligheid

Gemeente Helmond ambieert een duurzame, sociale en economisch vitale toekomst. Om dit te realiseren zijn er diverse programma's geformuleerd vanuit de strategische agenda 2019-2025. Het profiel en de ambitie van de gemeente is bepalend voor de informatievoorziening en hiermee bepalend voor de informatieveiligheid. Bij de thema's Sociale Stad, Toekomstgericht Werken en Omgevingswet is de borging van informatieveiligheid van belang. Om de ambitie zoals opgenomen in de strategische agenda waar te maken is een solide inrichting van informatiebeveiliging noodzakelijk. Het bestuur maakt hierbij op basis van risicomanagement bewuste keuzes om informatieveiligheid te borgen en om kwetsbaarheden in de bedrijfsvoering te minimaliseren. Veiligheids- en imagorisico's voor de organisatie en het bestuur - zoals afpersing, diefstal van persoon- en bedrijfsgegevens, uitval van ICT-diensten- worden hiermee verkleind.

Een solide inrichting van informatiebeveiliging aan de voorkant voorkomt gedoe achteraf. Om deze solide inrichting te bereiken, is het noodzakelijk om op het gebied van informatieveiligheid te professionaliseren. Het huidige volwassenheidsniveau van informatiebeveiliging van gemeente Helmond[1] ligt tussen niveau 1 en 2. De ambitie is om in 2024 volwassenheidsniveau 4 te bereiken. Zodra dat niveau bereikt is, heeft de organisatie informatieveiligheid geborgd binnen haar processen. Zij voldoet aan wet- en regelgeving én heeft voldoende kennis om proactief op ontwikkelingen te anticiperen. Zij weet haar risico's te verkleinen tot een acceptabel niveau in lijn met de ambities uit de strategische agenda.

Noodzakelijke randvoorwaarde om deze groei te bereiken, is de beschikbaarheid van kwalitatieve en kwantitatieve resources op de afdelingen. Met de inrichting van een decentrale Informatieveiligheid en privacy organisatie die vanaf juli 2019 is gestart, is een significante, eerste stap gezet. Met deze inrichting groeit de gemeente vanuit organisatieonderdelen en kan integraal worden gewerkt aan het verbeteren van de informatieveiligheid en privacy.

Dit strategische informatiebeveiligingsbeleid 2020-2024 is het kader om gemeentelijke informatie te beschermen en draagt bij aan een verdere professionalisering van informatiebeveiliging.

[1] Resultaten meting 2018: geclassificeerd conform het volwassenheidsmodel NBA-LIO/NOREA

2 Inleiding

Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente. Toegankelijke en betrouwbare informatie én vertrouwelijke omgang met informatie is essentieel voor een gemeente omdat het de basis is voor juist en efficiënt handelen. Gemeente Helmond heeft haar ambities vastgelegd in de strategische agenda en dient hierbij transparant te zijn richting haar inwoners en proactief verantwoording af te leggen aan interne en externe toezichthouders. Dit strategische informatiebeveiligingsbeleid is het kader voor informatiebeveiliging.

2.1 Doel van dit beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor het tactische beleid en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Dit beleid geldt voor de jaren 2020 tot en met 2024 en vervangt het "Informatiebeveiligingsbeleid gemeente Helmond 2015-2019". Het is het bestuurlijk kader om de beschikbaarheid, integriteit en vertrouwelijkheid van de (persoons)gegevens en andere informatie(systemen) te waarborgen, zodat de gemeente voldoet aan relevante wet- en regelgeving. Dit strategische informatiebeveiligingsbeleid is gericht op het :

- Verstevigen van governance
  De verantwoordelijkheid voor informatieveiligheid is primair in de lijn belegd. Dit betekent een centrale rol voor afdelingsmanagers.
- Risico gebaseerd sturen
  Dit betekent dat het management verantwoordelijk is voor het identificeren van de hoogste risico's, het prioriteren van de risico's en het treffen van maatregelen om deze risico's terug te brengen.
- Integratie in de planning- en control cyclus

Dit betekent dat informatieveiligheid dient te worden opgenomen in de integrale P&C-cyclus. Implementatie en verantwoording vindt plaats via de planning zoals opgenomen in de bedrijfsvoering kalender. Er vindt een uniforme verantwoording plaats aan interne en externe toezichthouders.

Dit beleid draagt bij aan een verdere professionalisering van informatieveiligheid en hiermee aan het behalen van de gestelde doelen in de strategische agenda.

2.2 Scope van het strategische informatiebeveiligingsbeleid

Dit beleid is van toepassing op de gehele organisatie, alle gemeentelijke processen, informatie, informatiesystemen en gegevens(verzamelingen) van de gemeente en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Het heeft betrekking op het politiek bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties.
Het borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen.

3 Beleidskader Informatieveiligheid

3.1 Plaats van dit beleid

Het strategisch informatiebeveiligingsbeleid is in lijn met de relevante landelijke en Europese wet- en regelgeving. Het strategisch informatiebeveiligingsbeleid is een onderdeel van het informatiebeleid en bestaat uit de volgende documenten:

1. strategische informatiebeveiligingsbeleid
2. tactische informatiebeveiligingsbeleid
3. specifieke beleidskaders
4. informatiebeveiligingsbeleidsplan(nen)

In het tactische beleid staan onderwerp-specifieke beleidsregels die de implementatie van informatiebeveiliging verplicht stelt. De uitwerking van het strategische en het tactische beleid staat opgenomen in het informatiebeveiligingsplan. Dit plan wordt jaarlijks bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.

Voor bepaalde kerntaken gelden op grond van wet-en regelgeving specifieke (aanvullende) beveiligingseisen[2]. Hiervoor gelden specifieke beleidskaders en/of informatiebeveiligingsplannen. Het onderwerp privacy is in een apart beleid[3] opgenomen.

3.2 Grondslagen

Dit strategische informatiebeveiligingsbeleid is gebaseerd op:

- NEN-ISO/IEC 27001:2017
- NEN-ISO/IEC 27002:2017
- Baseline Informatiebeveiliging Overheid (BIO)[4] en de 10 principes voor informatiebeveiliging (zie hoofdstuk 4).
- De architectuurprincipes van de gemeente (zie paragraaf 3.3)

3.3 Architectuurprincipes

Architectuurprincipes zijn richtinggevend en helpen gemeenten om bewust keuzes te maken bij het inrichten van de gemeentelijke processen, bijhorende informatievoorziening en zijn de basis om informatiebeveiliging te implementeren. De gemeente Helmond volgt hierbij landelijke richtlijnen[5].
De acht GEMMA basisprincipes zijn:

1 Onze gemeente denkt vanuit de positie van de klant.
2 Onze gemeente gebruikt generieke processen en functies.
3 Onze gemeente voert regie over uitbestede diensten.
4 Onze gemeente biedt de klant een goede informatiepositie.
5 Onze gemeente digitaliseert haar diensten en processen.
6 Onze gemeente stelt openbare gegevens als open data beschikbaar.
7 Onze gemeente hergebruikt gegevens.
8 Onze gemeente gaat op een vertrouwde manier met gegevens om.

Deze architectuurprincipes zijn nader uitgewerkt in de informatiearchitectuur[6].

[2] zoals BRP, PNIK, DigiD, SUWI, BAG, BGT, BRO, AVG, Privacy beleid
[3] https://zoek.officielebekendmakingen.nl/gmb-2018-168572.html
[4] uitgebracht door de interbestuurlijke werkgroep Normatiek in 2018
[5] Nederlandse Overheid Referentie Architectuur (NORA) en de daarvan afgeleide Gemeentelijke Model Architectuur (GEMMA).

3.4 Uitgangspunten

De belangrijkste uitgangspunten van dit informatiebeveiligingsbeleid zijn:

1. Dit beleid vormt samen met het tactische informatiebeveiligingsbeleid en het informatiebeveiligingsplan het kader om informatieveiligheid in de organisatie te borgen.
2. Informatiebeveiliging mag niet ten koste gaan van de veiligheid van personen.
3. Het bestuur, de directie en de (afdelings)managers dragen dit beleid uit en sturen op de implementatie van dit beleid.
4. Informatiebeveiliging is georganiseerd. Het management heeft continu aandacht voor het vergroten van het bewustzijn van medewerkers om zo de menselijke schakel te versterken.
5. De rol van de coördinator van informatiebeveiliging (Chief Information Security Officer: CISO), is ingevuld.
6. Regels en verantwoordelijkheden voor het informatiebeveiligingsbeleid zijn vastgesteld.
7. Informatiebeveiliging is een continu verbeterproces. Door organisatiebrede planning, het implementeren van maatregelen, het periodieke controleren én de coördinatie op dit proces is informatieveiligheid binnen de organisatie verankerd.
8. Informatiebeveiliging is een onderdeel van risicomanagement.

3.5 Randvoorwaarden

Belangrijke randvoorwaarden om dit beleid te implementeren zijn:

1. De informatiebeveiligingstaken zijn belegd binnen de bedrijfsprocessen en de benodigde kwalitatieve en kwantitatieve resources zijn beschikbaar gesteld.
2. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures. Medewerkers kennen de beveiligingsprocedures en gebruiken deze procedures. Medewerkers zijn daarnaast op de hoogte van eisen die vanuit wet- en regelgeving aan hun bedrijfsprocessen gesteld worden en kennen deze kaders.
3. Medewerkers gaan verantwoord om met (persoons)gegevens en andere informatie(systemen), spreken elkaar aan op onveilig gedrag en melden mogelijke hiaten direct aan de leidinggevenden.
4. De informatiebeveiliging maakt deel uit van afspraken met ketenpartners en dienstenleveranciers.
5. Kennis en bewustzijn van informatiebeveiliging wordt actief bevorderd en geborgd bij alle lagen binnen de organisatie, ketenpartners en externe partijen.
6. Er zijn voldoende maatregelen geïmplementeerd die zorgen dat kwetsbaarheden in bedrijfsprocessen worden verkleind. Hierdoor worden informatiebeveiligingsincidenten verkleind en de effecten van de incidenten beperkt.
7. Periodiek worden onafhankelijke audits uitgevoerd om vast te stellen of de vereiste maatregelen uit het beleid in voldoende mate zijn geborgd.
8. De digitale weerbaarheid wordt verhoogd door de basis op orde te brengen.
9. Security en privacy by design principes worden toegepast bij innovaties. Denk hierbij aan common ground, internet of things (IoT) en Smart City, kunstmatige intelligentie (AI).

Zolang deze uitgangspunten en randvoorwaarden niet zijn ingericht is de informatieveiligheid niet voldoende geborgd.

6

file:///C:/Users/doriniee/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/brochure%20Informatiearchitectuur%20(1).pdf

4 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van dit informatiebeveiligings-beleid zijn hieronder beschreven.

4.1 Een nieuwe baseline voor informatieveiligheid

De Baseline Informatiebeveiliging Overheid (BIO) is vanaf 2020 het nieuwe normenkader voor de gehele overheid. Deze baseline is ten opzichte van de Baseline Informatiebeveiliging Gemeenten (BIG) meer gericht op risicomanagement. De bestuurders en de (afdelings)managers hebben een prominente rol met betrekking tot informatiebeveiliging en met de komst van de BIO een cruciale rol met betrekking tot risicomanagement. Hierbij maakt het bestuur en het management op voorhand keuzes en continu afwegingen of informatie in bestaande en nieuwe processen adequate beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

De BIO helpt het management bij het nemen van haar verantwoordelijkheid ten aanzien van informatiebeveiliging. In de BIO zijn op basis van de generieke schades en dreigingen voor de overheid standaard basisbeveiligingsniveaus gedefinieerd met bijbehorende verplicht in te richten beveiligingsmaatregelen. Het management bepaalt op basis van een risicoafweging, hoe aan deze beveiligingsmaatregelen kan worden voldaan. Waar naleving (nog) niet volledig mogelijk is, maakt het management de aanwezige risico's inzichtelijk aan hun stakeholders.

Het management legt verantwoording af over de risicoafweging en over de effectieve invulling van de beheersmaatregelen. Deze verantwoording is onderdeel van de bestuurlijke verantwoording over informatiebeveiliging[7]. De BIO biedt hiermee de basis om te zorgen dat informatiebeveiliging geïmplementeerd en geborgd wordt.

4.2 Handvatten voor de rol van de bestuurder

VNG heeft aan het gemeentelijk bestuur de 10 principes van informatiebeveiliging[8] uitgereikt. Deze principes bieden het bestuur handvatten op welke wijze het zijn rol kan invullen bij het borgen van informatiebeveiliging in de gemeentelijke organisatie Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement bij o.a. beveiligingsincidenten met directe gevolgen voor inwoners en/of medewerkers.

De 10 principes zijn:
1 Bestuurders bevorderen een veilige cultuur;
2 Informatiebeveiliging is van iedereen;
3 Informatiebeveiliging is risicomanagement;
4 Risicomanagement is onderdeel van de besluitvorming;
5 Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking;
6 Informatiebeveiliging is een proces;
7 Informatiebeveiliging kost geld;
8 Onzekerheid dient te worden ingecalculeerd;
9 Verbetering komt voort uit leren en ervaring;
10 Het bestuur controleert en evalueert.
Deze 10 principes staan nader uitgewerkt in de uitgewerkte rolverdeling van hoofdstuk 6 en in het tactische informatiebeveiligingsbeleid en het informatiebeveiligingsplan.

[7] Zie hoofdstuk 8

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

5 Communicatie en evaluatie van dit beleid

Na vaststelling van dit beleid door het college wordt dit beleid gepubliceerd en via het lijnmanagement gecommuniceerd met medewerkers en relevante externe partijen. Verdere communicatie momenten zijn uitgewerkt in het informatiebeveiligingsplan.

Het strategische informatiebeveiligingsbeleid geldt voor een periode van 5 jaar en wordt met een frequentie van 5 jaar geëvalueerd of eerder bij belangrijke wijzigingen.

6 Organiseren van informatiebeveiliging

De wijze waarop het informatiebeveiligingsbeleid binnen de gemeente is verankerd, vormt het kader van de borging op informatiebeveiliging. Het vaststellen van een beheerkader is van belang om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te borgen.

Het bestuur, de directie en het afdelingsmanagement spelen een cruciale rol bij het uitvoeren van dit beleid. De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten. Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. Hieronder is toegelicht welke rollen, taken en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn belegd in de organisatie. Overige specifieke rollen behoren te worden uitgewerkt in een bijlage behorende bij de operationele informatiebeveiligingsplannen.

6.1 Gemeenteraad

De gemeenteraad heeft een toezichthoudende rol op basis van de controlerende taak die de Gemeentewet aan de gemeenteraad toekent.

6.2 College van Burgemeesters en Wethouders

Het College van Burgemeester en Wethouders is integraal (politiek) verantwoordelijk voor de borging van informatieveiligheid binnen de gemeente. Zij stelt kaders op voor informatieveiligheid (dit strategische beleid). Bij het onderwerp waardedocumenten is bij wet bepaald dat de bevoegdheid voor het vaststellen van kaders bij de burgemeester ligt in plaats van bij het college. De ambtelijke verantwoordelijkheid op het gebied van informatiebeveiliging is door het college gemandateerd aan de gemeentesecretaris.

Zowel het college van Burgemeester en Wethouders als de Raad (controle functie) kunnen opdracht geven om controle te laten uitvoeren. Het college legt verantwoording af aan de Raad en aan externe toezichthouders. Het college is verantwoordelijk voor de financiën van de gemeente.

6.3 De directie

De directie is ambtelijk verantwoordelijk voor kaderstelling en sturing op tactisch niveau. De directie stuurt hierbij op concernrisico's. De gemeentesecretaris draagt de gemandateerde verantwoordelijkheid voor informatieveiligheid en privacy.

De directie:

- zorgt voor voldoende resources om informatiebeveiliging in de organisatie te borgen.
- adviseert het college van B&W over het vast te stellen strategische beleid.
- zorgt dat het tactische (specifieke) beleid, informatiebeveiligingsplan(nen) en procedures worden opgesteld en vastgesteld.
- draagt het informatiebeveiligingsbeleid uit aan de organisatie en stuurt op concern risico's.

- zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingsmanager (eigenaarschap) en ziet erop toe dat de afdelingsmanagers adequate maatregelen nemen.
- zorgt dat de afdelingsmanagers zich verantwoorden over de stand van zaken van informatieveiligheid binnen hun bedrijfsprocessen en rapporteert periodiek over de status zodat het college hierop kan sturen. Spreekt afdelingsmanager aan op naleving van dit beleid ook als verbetermaatregelen niet tijdig worden doorgevoerd.
- controleert of de getroffen maatregelen overeenstemmen met de gestelde eisen en of deze voldoende bescherming bieden.
- informeert de eindverantwoordelijke portefeuillehouder(s) binnen het College gevraagd en ongevraagd over informatiebeveiliging.
- ziet erop toe dat informatiebeveiligingsonderwerpen n.a.v. de rapportage van de CISO onderdeel zijn van de Planning & Control gesprekken en dat risicovolle onderwerpen worden opgenomen in de auditplannen.
- evalueert periodiek het informatiebeveiligingsbeleid. Voor het strategische beleid geldt een periode van 5 jaar of bij belangrijke wijzigingen.

6.4 Afdelingsmanagers (proceseigenaren)

De afdelingsmanagers (proceseigenaren) zijn operationeel eindverantwoordelijk voor de bedrijfsprocessen. De proceseigenaren zijn hiermee eigenaar van de applicaties binnen dit bedrijfsproces. Daar waar applicaties worden gebruikt in meerdere bedrijfsprocessen geldt dat het bedrijfsproces met het hoogst noodzakelijke beveiligingsniveau leidend is. De afdelingsmanagers kunnen hun verantwoordelijkheid niet delegeren, uitvoerende werkzaamheden wel. De afdelingsmanagers zorgen dat de inrichting van informatiebeveiliging en privacy voldoet aan de vereiste wet- en regelgeving. Hierbij worden zij ondersteund door de Decentrale Security en Privacy Officer (DSPO), de CISO en de Functionaris Gegevensbescherming (FG). Afdelingsmanagers rapporteren over de door hun tactisch- en operationeel uitgevoerde activiteiten aan de directie en bestuur[9].

De afdelingsmanagers:

- stellen specifiek beleid, specifieke informatiebeveiligingsplan(nen) en procedures, op en vast en dragen deze uit.
- sturen op beveiligingsbewustzijn, bedrijfscontinuïteit, privacy en naleving van regels en richtlijnen (gedrag en risicobewustzijn).
- bespreken beveiligingsincidenten en de consequenties die dit heeft voor beleid en te implementeren beheersmaatregelen
- stellen het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid vast.
- signaleren vroegtijdig de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- zorgen ervoor dat actuele risicoanalyse(s) worden uitgevoerd. implementeren de noodzakelijke informatiebeveiliging en privacy maatregelen. Deze beveiligingsmaatregelen bepalen zij op basis van risicomanagement en op basis van de kaders die eigen wet- en regelgeving met zich meebrengen.
- bewaken dat gekozen gegevensbeschermingsmaatregelen uit risicoanalyses worden opgenomen in doorontwikkelplannen. Stellen vast of de getroffen maatregelen aantoonbaar worden nageleefd. Rapporteren hierover in de managementrapportages aan de CISO, de directie en het bestuur. Leveren input voor wijzigingen op maatregelen en procedures.
- Stemmen de inhoudelijke aanpak om informatiebeveiliging te borgen af in het bedrijfsvoeringoverleg met de afdelingen en/ of teams

[9] Zie hoofdstuk 8 Rapportagemomenten

- leveren alle informatie aan die nodig is voor het invullen van de jaarlijkse verantwoordingstraject informatiebeveiliging (ENSIA).

Het management wordt hierbij ondersteund door de Decentrale Security en Privacy Officer.

6.5 Decentrale Security & Privacy Officer

De DSPO ondersteunt de afdelingsmanager bij het beheer, de coördinatie en het advies ten aanzien van de informatieveiligheid en privacy voor zijn/ haar bedrijfsproces. De DSPO is het eerste aanspreekpunt voor de afdelingsmanager, de CISO en de FG en ambassadeur voor informatieveiligheid en privacy binnen dit bedrijfsproces.

De DSPO's zijn binnen de gemeente degenen die kaders stellen op het gebied van domein specifieke informatiebeveiliging en beveiligingsbewustzijn. De DSPO bevordert draagvlak bij het management en medewerkers. Tevens monitort de DSPO of de informatiebeveiliging conform de kaders uitgevoerd wordt. Hij is direct betrokken bij de implementatie hiervan in de lijn en kent de processen en relevante wetgeving. Hij zorgt daarmee dat de organisatie specifieke informatiebeveiliging doorvoert in haar processen, conform wet- en regelgeving.

Verder richt de DSPO zich op de uitvoer en naleving van de (domein specifieke) privacywetgeving. De DSPO stelt een data protection impact assessment (DPIA) op en adviseert bij het gebruik van persoonsgegevens. De DSPO toetst bij gegevensaanvragen op doelbinding, rechtmatigheid, proportionaliteit en andere aspecten vanuit de AVG en privacywetgeving. De DSPO rapporteert periodiek over de informatieveiligheid/ privacy aan de afdelingsmanager, CISO en FG.

6.6 Chief Information Officer

De CIO geeft binnen het directieteam op dagelijkse basis invulling aan de sturende rol door besluitvorming in het college van Burgemeester en Wethouders voor te bereiden en toe te zien op de uitvoering ervan. De informatiebeveiligingstaken die hieruit voortvloeien zijn belegd bij de CISO.

6.7 Chief Information Security Officer

De CISO ondersteunt vanuit een onafhankelijke positie de organisatie met betrekking tot het borgen van informatieveiligheid en heeft de mogelijkheid om rechtstreeks aan de directie en/of portefeuillehouder te rapporteren. De CISO is aangesteld volgens een vastgesteld CISO-functieprofiel.

De CISO is binnen de gemeente degene die kaders stelt op het gebied van informatiebeveiliging die voor de gehele organisatie gelden. De CISO stuurt de organisatie aan met betrekking tot informatiebeveiliging. Hiermee zorgt de CISO ervoor dat de organisatie informatiebeveiliging doorvoert in haar processen, conform wet- en regelgeving. Daarnaast creëert de CISO het draagvlak voor informatiebeveiliging binnen de organisatie. De rol van de CISO is vooral adviserend en coördinerend. De CISO stuurt de DSPO's functioneel aan. De CISO is in het kader van het verantwoordingstraject informatiebeveiliging tevens coördinator ENSIA.

Om aan bovenstaande te kunnen voldoen, heeft de CISO de volgende bevoegdheden:

- gevraagd en ongevraagd onderzoek kunnen doen en advies geven aan het college van B&W / Raad
- mogelijkheid tot direct ingrijpen zonder toestemming vooraf bij beveiligingsincidenten
- beschikt over budget en resources

De CISO is geplaatst binnen de afdeling Informatievoorziening en Automatisering-CIO. De CISO voert geen operationele taken uit. Hiermee is het risico geminimaliseerd dat de eigenlijke taken van de CISO blijven liggen en de onafhankelijke positie in het geding komt. Daarnaast heeft de CISO rechtstreekse toegang tot de portefeuillehouder van informatiebeveiliging.

6.8 Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming (FG) is de interne toezichthouder op het gebied van privacy. De FG houdt toezicht op de wijze waarop de organisatie invulling geeft aan maatregelen om aan de privacywetgeving te voldoen. In het privacy-beleid staan de taken van de FG opgenomen.

6.9 IT Auditor

De IT auditor (concern control) is verantwoordelijk voor het opzetten, uitvoeren van risicoanalyses op het gebied van de naleving van informatiebeveiliging en privacy. De IT auditor initieert audits en toetst hierbij op de naleving van het informatiebeveiligingsbeleid.
Om de verantwoordelijkheden in het informatiebeveiligingsgebied te kunnen vervullen dienen de bovengenoemde rollen op het gebied van informatiebeveiliging competent te zijn en de mogelijkheid te hebben om de ontwikkelingen op het gebied van informatiebeveiliging bij te houden.

7 Communicatie stakeholders

7.1 Stakeholders

De gemeente Helmond onderhoudt contacten met relevante overheidsinstanties (zoals externe toezichthouders), speciale belangengroepen (zoals Informatie Beveiligingsdienst Gemeenten) en interne stakeholders. Een nadere toelichting over het contact met de IBD is opgenomen in paragraaf 7.2. Stakeholders worden periodiek op de hoogte gesteld over de stand van zaken rondom informatiebeveiliging. Het onderwerp informatiebeveiliging is een vast onderdeel op de agenda van bestuur en lijnmanagement met als doel om sturing te kunnen geven. In de onderstaande tabel bij paragraaf 7.3 is opgenomen wat de contactmomenten met stakeholders zijn.

7.2 Aansluiting Informatiebeveiligingsdienst Gemeenten

Eén van de doelen van de IBD[10] is het aan gemeenten leveren van concrete ondersteuning in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
Wij maken indien nodig gebruik van deze ondersteuning. De IBD informeert de gemeente via vastgestelde contactpersonen namelijk de algemeen contactpersoon informatiebeveiliging (ACIB)[11] en de vertrouwde Contactpersoon Informatiebeveiliging (VCIB)[12].

7.3 Contactmomenten stakeholders

Contactmoment	Deelnemers	Frequentie	Doel
opdrachtgever – opdrachtnemer overleg	bestuurlijk opdrachtgever, ambtelijk opdrachtgever, CIO, CISO, FG	per kwartaal	informeren opdrachtgever over proces
informatieveiligheid en privacy overleg	CISO, de DSPO en de FG	per kwartaal	afstemming en coördinatie van informatieveiligheid en privacy onderwerpen: De DSPO heeft vooraf afstemming met de proceseigenaar.

[10] De Informatiebeveiligingsdienst voor gemeenten (IBD) is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING).
[11] Algemene waarschuwingen en informatie met een niet vertrouwelijk karakter
[12] Informatie die vertrouwelijk is van karakter

Contactmoment	Deelnemers	Frequentie	Doel
presentaties ENSIA verantwoording	proceseigenaren, DSPO, CISO en ambtelijk opdrachtgever	per jaar	In beeld brengen risico's in proces en stand van zaken implementatie informatiebeveiliging input voor bestuurlijke rapportage van CISO aan interne en externe toezichthouders, jaarverslag en Raadsinformatiebrief
ICT crisisoverleg	Gemeentesecretaris, CISO, DSPO, CIO, verantwoordelijke voor het domein waar de crisis betrekking op heeft Eventueel lid van het team communicatie, FG	per incident	grip op crisis input voor analyse en rapportage van incident

8 Rapportagemomenten informatiebeveiliging

Periodieke rapportages vloeien voort uit bovengenoemde contactmomenten met stakeholders. Rapportages worden opgesteld van incidenten, het verantwoordingstraject ENSIA en periodieke rapportages over de stand van zaken van de implementatie van informatiebeveiliging (P&C-cyclus). Aangezien het college en de Raad met name een rol spelen in het verantwoordingstraject wordt dit traject in onderstaande paragraaf toegelicht. In het informatiebeveiligingsplan is een detailplanning opgenomen van dit verantwoordingstraject.

8.1 Verantwoordingstraject ENSIA

Ter afsluiting van het jaarlijkse verantwoordingstraject[13] rapporteren de afdelingsmanagers over de risico's binnen hun bedrijfsprocessen en over de stand van zaken van de implementatie van informatiebeveiliging van het afgelopen jaar. De CISO coördineert dit proces en stelt jaarlijks vóór 1 mei aan de hand van de deelrapportages van de afdelingsmanagers een bestuurlijke rapportage op voor de ambtelijke en bestuurlijke opdrachtgever.

Het college van B&W legt met deze bestuurlijke rapportage, een raadsinformatiebrief én met een aparte paragraaf in het jaarverslag verantwoording af aan zijn interne toezichthouder de gemeenteraad én aan de externe toezichthouders (Rijk)[14]. Op deze wijze kan de ambtelijk en de bestuurlijk opdrachtgever en het college sturen op informatiebeveiliging. Zij kunnen hiermee besluiten nemen om informatiebeveiligingsrisico's tot een acceptabel niveau te brengen.

[13] Verantwoording vindt plaats via de landelijk voorgeschreven systematiek ENSIA (Eenduidige Normatiek Single Information Audit)

[14] In de bijlage behorende bij het informatiebeveiligingsplan staat de detailplanning, rolverdeling en benodigde capaciteit opgenomen.

Informatiebeveiligingsbeleid Lumens dd. februari 2019

Inleiding

Lumens is een welzijnsorganisatie. Wij ondersteunen mensen die het (soms) moeilijk vinden om mee te doen met de samenleving. Wij helpen hen hun interesses en talenten te ontdekken en verder te ontwikkelen, om vanuit een stevige basis te kunnen werken naar een zelfstandig en gelukkig bestaan. Dat kan zijn in de vorm van betaald werk, als zelfstandig ondernemer of als vrijwilliger, maar ook in de vorm van een inspirerende en fijne vrijetijdsbesteding.

Wij richten ons vooral op jeugd (www.dynamojeugdwerk.nl) en op de wijken. Vanuit de wijken en de verschillende jeugdculturen, dichtbij en mét bewoners, zorgen we dat kansen worden vergroot én benut. We doen dat omdat we weten dat meedoen werkt. Maar meedoen gaat niet voor iedereen zomaar vanzelf. Soms lukt het gewoon even niet en dan zijn wij er met de juiste ervaring en ervaringsdeskundigen: in sterke verbinding met samenwerkingspartners en met uitzicht op resultaat.

Inspireren Leren Werken
We werken volgens een unieke werkwijze, die sterk verankerd ligt in onze hele organisatie: Inspireren Leren Werken (ILW). De mensen van Lumens weten je te inspireren, zodat jij je interesses en talenten ontdekt. Samen zetten we die om in kennis en ervaring, waarmee je stevige stappen kunt zetten op weg naar een zelfstandig en gelukkig leven.

Om kwaliteit te bieden is een betrouwbare informatievoorziening essentieel. Uitgebreide aandacht voor de beveiliging van de opslag, verwerking en uitwisseling van informatie is continu vereist.
De beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening die ten grondslag ligt aan de dienstverlening van Lumens dient derhalve gewaarborgd te zijn.

Het hebben van een effectief informatiebeveiligingsbeleid is hierdoor noodzaak.

Informatiebeveiliging bij Lumens

Definities

Informatiebeveiliging wordt als volgt gedefinieerd:

Het samenhangend geheel van preventieve, repressieve en herstelmaatregelen alsmede procedures en processen welke de beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen blijvend garanderen met als doel de continuïteit van de bedrijfsvoering te waarborgen en eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald, niveau te beperken.

Informatiebeveiliging richt zich op drie aspecten van de informatievoorziening:

- ✓ **Beschikbaarheid:** het waarborgen dat geautoriseerde gebruikers toegang hebben tot informatie en de informatiesystemen op de gewenste momenten.
- ✓ **Integriteit:** het waarborgen dat de informatie juist en volledig is en de informatiesystemen juiste en volledige informatie opslaan en verwerken.
- ✓ **Vertrouwelijkheid:** het waarborgen dat informatie alleen toegankelijk is voor diegene die hiertoe bevoegd/geautoriseerd is.

Lumens heeft zeer bewust de keuze gemaakt alle ICT-systemen te outsourcen. Daarbij voert Lumens eveneens het beleid dat data zich niet lokaal bevinden op een locatie van Lumens, maar wordt opgeslagen in een door de leverancier gefaciliteerde cloud. Op deze manier kan zoveel mogelijk gewaarborgd worden dat data ten alle tijden beschikbaar zijn voor medewerkers van Lumens.

Als onderdeel van haar Inkoopbeleid vereist Lumens van haar ICT-leveranciers dat zij aantoonbaar in overeenstemming met ISO27001 en/of NEN 7510 werken en een passend, geschreven informatiebeveiligingsbeleid geïmplementeerd hebben. Daarnaast vereist Lumens in haar Inkoopbeleid dat een leverancier eveneens aantoonbaar voldoet aan de veiligheidseisen voor netwerkverbindingen zoals beschreven in NEN7512 en aan de eisen ten aanzien van logging zoals beschreven in NEN7513.

Naast de beveiliging van informatie vindt Lumens de bescherming van privacy van zowel medewerkers als klanten ook heel belangrijk. Om die reden dienen leveranciers accoord te gaan met de standaard verwerkersovereenkomst van Lumens. Deze voorwaarde is ook opgenomen in het Inkoopbeleid van Lumens.

Monitoren

Om te kunnen monitoren dat een leverancier acteert in lijn met bovenstaande is tevens in het Inkoopbeleid opgenomen dat een leverancier desgevraagd haar Informatiebeveiligingsbeleid dient te overleggen. Tevens dient een leverancier beveiligingsincidenten direct aan Lumens te rapporteren. Met leveranciers die over data beschikken die een verhoogd risico vormen voor de bedrijfsvoering van Lumens wordt jaarlijks een evaluatie uitgevoerd. Onderwerpen van evaluatie zijn:: de stand van zaken rondom het informatiebeveiligingsbeleid van leverancier en beveiligingsincidenten en maatregelen die getroffen zijn door leverancier om deze incidenten te voorkomen. De afdeling Facilitair van Lumens stelt vast welke leveranciers hiervoor in aanmerking komen en initieert deze evaluaties.

Verantwoordelijkheden

De bestuurder is eindverantwoordelijk voor het informatiebeveiligingsbeleid.
De manager Bedrijfsvoering is eindverantwoordelijk voor de uitvoering en toepassing van het informatiebeveiligingsbeleid. Operationeel betekent dit dat de afdeling Facilitair zorgt voor het naleven van het Inkoopbeleid en de noodzakelijke monitoring van de leveranciers.

Aanpassing Informatiebeveiligingsbeleid

Jaarlijks evalueren Gemeente Helmond, Lumens en MO Den Bosch het Informatiebeveiligingsbeleid. Het beleid zal daar waar noodzakelijk aangepast worden. Deze evaluatie wordt uitgevoerd door de Kwaliteitsmedewerkers van Gemeente Helmond, Lumens en MO Den Bosch, de Functionarissen Gegevensbescherming en de Managers Bedrijfsvoering. De Functionarissen Gegevensbescherming zorgen er vervolgens voor dat het informatiebeveiligingsbeleid aangepast wordt.

Beleidsdoelstellingen

Lumens hanteert de onderstaande uitgangpunten voor het informatiebeveiligingsbeleid. Deze zijn zowel van toepassing op Lumens als op haar leveranciers.

- Uitgangspunt vormen de doelstellingen van de norm NEN-ISO/IEC 27001 voor zover deze bijdragen aan de informatiebeveiliging van Lumens. **Als een doelstelling op een andere wijze**

wordt gerealiseerd via een alternatieve maatregel, dan is dat toegestaan, mits dit alternatief beschreven is.

- De fysieke en logische beveiliging van de computercentra en bedrijfsgebouwen waar Lumens en haar leveranciers gebruik van maken, is zodanig dat de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en gegevensverwerking zijn gewaarborgd.
- Aanschaf, installatie en onderhoud van geautomatiseerde gegevensverwerkende systemen, alsmede inpassing van nieuwe technologieën, mogen geen afbreuk doen aan het niveau van veiligheid van de totale informatievoorziening.
- Het privacybeleid levert met procedures een bijdrage aan de vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening.
- Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening kan ontstaan.
- Bij de verwerking van gegevens worden maatregelen getroffen om de privacy van klanten en medewerkers te waarborgen.
- Logische toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de systemen, gegevensbestanden en programmatuur van Lumens.
- Bij gegevensverstrekking intern en extern wordt gebruikgemaakt van een gedocumenteerde gegevensclassificatie en worden gegevens verstrekt op basis van ‘need to know’. Medewerkers treffen maatregelen om te voorkomen dat informatie terechtkomt in handen van personen, die deze informatie niet strikt nodig hebben. Ook de toegang tot informatiesystemen wordt volgens dit principe adequaat beveiligd. Voor ICT-beheerders wordt hierop onder duidelijke voorwaarden een uitzondering gemaakt om de dienstverlening niet te belemmeren.
- Datatransport is zodanig met beveiligingsmaatregelen omkleed dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van de gegevens en op de informatievoorziening als geheel.
- Opslag en back up van gegevens zijn zodanig ingericht, dat geen informatie verloren kan gaan.
- Beveiligingsincidenten worden adequaat afgehandeld. Lumens en haar leveranciers houden zich aan afhandeling conform de AVG. Op basis van analyse van incidenten worden waar nodig maatregelen genomen om herhaling te voorkomen.

Informatiebeveiligingsbeleid Maatschappelijke Opvang Den Bosch dd. augustus 2020

Met dit privacy beleid geven we aan hoe wij omgaan met privacy van cliënten, partners én medewerkers

Bij MO Den Bosch verwerken we veel persoonsgegevens van zowel cliënten als (keten)partners en medewerkers. Deze persoonsgegevens verzamelen we voornamelijk voor het goed uitvoeren van onze wettelijke taken als maatschappelijke opvang organisatie. In de doelgroep waar wij mee werken spelen regelmatig veiligheidsissues. Dit vergt goede samenwerking met verschillende partijen, met daarbij een zorgvuldige afweging van het recht op privacy én het recht op passende dienstverlening en veiligheid.

In dit privacy beleid lichten wij toe hoe wij deze afweging maken en onze keuzes borgen. Ons uitgangspunt is dat de regie over de eigen gegevens bij de cliënt zelf ligt. Het is van belang dat onze cliënten, (keten)partners en medewerkers erop kunnen vertrouwen dat MO Den Bosch zorgvuldig en veilig met de persoonsgegevens omgaat.

Dit beleid is van toepassing op de gehele organisatie en op alle processen, onderdelen, objecten en gegevens verzamelingen waarin persoonsgegevens worden verwerkt.

Wij hanteren de uitgangspunten uit de AVG

De uitgangspunten van dit privacy beleid zijn gebaseerd op de uitgangspunten van de AVG:

- Legitimiteit: (er moet een noodzaak zijn) De verwerking van persoonsgegevens vindt uitsluitend plaats voor zover dit wettelijk gerechtvaardigd is;
- Doelbinding: Persoonsgegevens worden alleen verwerkt voor zover dat nodig is om het vastgestelde doel te bereiken; de gegevens mogen niet verwerkt worden voor een ander doel dan waarvoor ze verkregen zijn.
- Subsidiariteit: Het doel kan niet met minder dan de verzamelde gegevens worden bereikt.
- Proportionaliteit: De verzamelde gegevens staan in verhouding tot het doel.
- Kwaliteit: Gegevens zijn juist, nauwkeurig en voldoende actueel.
- Informatieveiligheid: Informatievoorzieningen zijn beveiligd tegen problemen die de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens aantasten.
- Houdbaarheid: Gegevens die niet langer nodig zijn, worden vernietigd of geanonimiseerd.

Wij verwerken enkel persoonsgegevens binnen de grondslagen van de AVG

Alle medewerkers van MO Den Bosch verwerken persoonsgegevens uitsluitend voor zover dit valt binnen hun mandaat en noodzakelijk is de hulpverlening.

Persoonsgegevens mogen alleen worden verwerkt op basis van de volgende grondslagen van 6 van de AVG:

1. Toestemming van de betrokken persoon.
2. De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.
3. De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting.
4. De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen.
5. De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
6. De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

MO Den Bosch verwerkt alleen persoonsgegevens als één van deze grondslagen aanwezig is.

Iedereen binnen MO draagt een verantwoordelijkheid rond privacy

Alle genoemde betrokken personen en partijen dragen een verantwoordelijkheid als het gaat om naleven van dit privacy beleid. Er zijn een aantal specifieke rollen:

- Medewerkers van MO Den Bosch zijn aanspreekbaar op het borgen van de privacy van de klant.
- MO Den Bosch faciliteert haar medewerkers om in hun dagelijks werk de juiste privacy afwegingen te maken. Ook houdt MO Den Bosch in de gaten of medewerkers handelen conform het privacy beleid en sturen zij tussentijds bij. Daarnaast heeft MO Den Bosch een verantwoordingsplicht, dit houdt in dat wij ook kunnen aantonen dat we aan de privacyregels voldoen. Dit blijkt uit:
    - ons actuele en volledige verwerkingsregister rondom privacy incidenten en datalekken;
    - ons openbare privacy statement op onze website;
    - onze manie waarop wij (cliënt)informatie op verwerken en behandelen.
- De directeur van MO Den Bosch is verantwoordelijk voor een adequate toepassing en werking van dit privacy beleid en is de verwerkingsverantwoordelijke.
- De Functionaris Gegevensbescherming ziet toe op een correcte naleving van de privacywet, met als doel het bevorderen dat persoonsgegevens zorgvuldig worden geregistreerd en gebruikt worden en is verantwoordelijk voor het melden van datalekken bij de Autoriteit Persoonsgegevens.
- Security Officer van Reinier van Arkel (MO Den Bosch valt onder de holding Reinier van Arkel) is de spin in het web als het gaat om beveiliging van informatie binnen de instelling: cliëntinformatie, medewerker gegevens en bedrijfsgevoelige informatie.

Privacy beleid cliënten

We maken per situatie een afweging tussen het recht op privacy en het recht op passende dienstverlening o.b.v. vier leidende principes

Ons inziens gaat privacy over méér dan uitwisseling van persoonsgegevens. Daarbij kan de afweging, welke persoonsgegevens in welke situatie gedeeld mogen worden, per situatie verschillen. Het delen van persoons-gegevens vergt altijd een zorgvuldige afweging van het recht op privacy én het recht op passende dienstverlening. Vanuit het *recht op privacy* willen we het delen van gegevens zoveel mogelijk beperken; vanuit het *recht op passende dienstverlening* willen we gegevens kunnen delen wanneer dit de dienstverlening ten goede komt.

Omdat iedere situatie uniek is werken we bij MO Den Bosch volgens **vier leidende principes**:

1. De cliënt heeft zelf regie over zijn eigen dossier

Dit betekent dat de cliënt recht heeft op inzage in zijn dossier. De cliënt kan zijn dossier inzien door in te loggen op de cliëntportaal Carenzorgt van Nedap. Daarnaast kan een cliënt verzoeken om bepaalde gegevens te wijzigen. Indien mogelijk draagt de medewerker samen met de cliënt zorg voor het vullen en actualiseren van het dossier. Voor zover wettelijk mogelijk is, heeft de cliënt zelf de regie welke persoonsgegevens wij verwerken in het dossier en welke gegevens door de medewerker uitgewisseld mogen worden.

2. Gegevens worden alleen vastgelegd en uitgewisseld voor zover noodzakelijk voor passende dienstverlening

De cliënt, diens mogelijkheden tot eigen regie, diens ondersteuningsvraag en de daarvoor benodigde dienstverlening staan steeds weer centraal bij de afweging of vastleggen en/of delen van gegevens noodzakelijk is. Het delen van gegevens vindt uitsluitend plaats met toestemming van de cliënt. De cliënt tekent hiervoor een toestemmingsverklaring.

3. Veiligheid van de cliënt en/of zijn omgeving vormen altijd de ondergrens

Wanneer de veiligheid van de cliënt en/of zijn omgeving in het geding is, grijpt de medewerker in en kan hij ook zonder toestemming van de cliëntgegevens vastleggen of delen met derden. De medewerker doet dit altijd na collegiale consultatie en informeert altijd de cliënt waarom hij heeft besloten zonder toestemming van de cliënt te handelen.

4. De medewerkers zijn open en transparant richting cliënten over de wijze waarop zij omgaan met het vastleggen van gegevens en het delen ervan met derden.

Noodzaak en toestemming van cliënten vormen basis voor gegevens vastlegging en –uitwisseling

Cliëntgegevens zijn nodig voor passende zorgverlening, cliënt heeft altijd recht op inzage

Wij informeren de cliënt tijdens het intakegesprek over de werkwijze van MO Den Bosch. Tijdens dit gesprek informeren wij de cliënt op een duidelijke en begrijpelijke manier welke (persoons)gegevens worden vastgelegd in het cliëntdossier, wat het doel is van het gebruik van deze gegevens, aan wie de organisatie de gegevens eventueel heeft verstrekt, en wat de herkomst is van de gegevens. In het Toestemmingsformulier geven cliënten aan welke relevante personen rondom de cliënt opgenomen mogen worden in het dossier. Het is de verantwoordelijkheid van de cliënt om deze personen te informeren dat zij eventueel gebeld kunnen worden door MO Den Bosch.

Persoonsgegevens worden zo min mogelijk, maar zo veel als nodig, geregistreerd en uitgewisseld. De gegevens die wij in ieder geval registreren zijn: voornaam, achternaam, BSN nummer, geboortedatum, geboorteplaats en nationaliteit. In het elektronisch cliëntendossier wordt het BSN geverifieerd aan de Basisregistratie Persoonsgegevens (BRP).

Cliënten hebben recht op inzage in hun persoonsgegevens

Cliënten hebben vanaf 2020 een eigen inlogportaal waarop zij kunnen inloggen en hun (eigen) dossier kunnen inzien. Cliënten hebben geen recht op informatie over anderen. Ook kunnen zij zelf geen gegevens wijzigen. Zij kunnen met de begeleiders in gesprek over feitelijke onjuistheden in het dossier. De begeleiders kunnen gegevens aanpassen via het medewerkersportaal.

Cliënten hebben recht op correctie en verwijdering van hun persoonsgegevens

Cliënten mogen de medewerker(s) van MO Den Bosch vragen hun persoonsgegevens te verbeteren, aan te vullen, te verwijderen (vernietigingsrecht) of af te schermen. Dat kan wanneer hun persoonsgegevens feitelijk onjuist zijn, onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld of op een andere manier in strijd met een wet worden gebruikt.

Het correctierecht is niet bedoeld voor het corrigeren van professionele indrukken, meningen en conclusies waarmee iemand het niet eens is, voor zover deze ter zake doen. Een verzoek om correctie of verwijdering van gegevens kan worden geweigerd, op het moment dat:

- De gegevens wettelijk moeten worden bewaard;
- Het bewaren van de gegevens noodzakelijk is om de cliënt een goede kwaliteit van dienstverlening te bieden of de cliënt te beschermen, bijvoorbeeld tegen geweld; M.a.w. het aanpassen/verwijderen van het dossier zou goed hulpverlenerschap in de weg staan, bijv. als

het overduidelijk is dat vernietiging van het dossier niet in het belang is van de patiënt. Bijv. informatie die zó cruciaal is voor de hulpverlening, dat de hulpverlener bij vernietiging van de gegevens geen verantwoorde zorg meer kan leveren.

• Het bewaren van de gegevens noodzakelijk is in verband met een gerechtvaardigd belang van MO Den Bosch. Bijvoorbeeld bij een lopende klachtenprocedure. De theoretische kans dat een cliënt in de toekomst een klacht indient valt hier dus niet onder.

Een afwijzing van een vernietigingsverzoek, moet goed worden onderbouwd.

Wij leggen enkel vast/wisselen uit wat noodzakelijk is voor passende dienstverlening

Medewerkers vragen altijd toestemming aan de cliënt (of zijn/haar vertegenwoordiger) voor het uitwisselen van diens gegevens met derden. De cliënt/ vertegenwoordiger tekent hiervoor de Toestemmingsverklaring bij de intake. Voor kinderen tot 12 jaar geeft de ouder met gezag/voogd toestemming. Voor kinderen van 12 tot 16 jaar geldt dat zowel de ouder met gezag/voogd als het kind toestemming moet geven. Kinderen vanaf 16 jaar geven zelf toestemming.

Met alleen toestemming is er nog geen grond om cliëntgegevens te mogen uit te wisselen. Wij leggen cliëntgegevens alleen vast en/of wisselen gegevens uit, wanneer dit noodzakelijk is voor een goede dienstverlening. Elke keer bij het uitwisselen van gegevens dient de afweging gemaakt te worden of gegevensdeling bijdraagt aan het doel dat we willen bereiken.

Indien het noodzakelijk is om gegevens uit te wisselen met derden, streven we naar een driegesprek, waarbij de medewerker samen met de cliënt de gegevens uitwisselt met de derde partij. Hierdoor is de eigen regie van de cliënt optimaal. Als een driegesprek niet lukt, dan wordt de cliënt expliciet om toestemming gevraagd. Dit alles geldt zowel voor schriftelijke uitwisseling van persoonsgegevens als voor mondelinge uitwisseling van persoons-gegevens van cliënten.

Voor het digitaal verzenden van cliëntinformatie gebruiken wij de ‘Veilig Verzenden’ optie binnen Outlook. Een veilige en gebruiksvriendelijke tool om e-mail berichten veilig versleuteld te verzenden en te ontvangen. Privacy- en organisatiegevoelige e-mailberichten zijn dan alleen in te zien door degene voor wie het bericht bedoeld is.

Wanneer de veiligheid van cliënt en/of omgeving in gevaar is, is privacy niet meer leidend

Indien de veiligheid van de cliënt en/of zijn omgeving in het geding is, kan een medewerker kiezen om zonder toestemming of ondanks een bezwaar van de cliënt toch gegevens vast te leggen en/of te delen met andere partijen. Op grond van de wet- en regelgeving rondom de Meldcode Kindermishandeling en Huiselijk Geweld zijn medewerkers in een aantal gevallen hiertoe zelfs verplicht.

Voordat een medewerker hiertoe besluit bespreekt hij de casus met een ander teamlid en/of zijn leidinggevende. Ook informeert hij de cliënt, waar mogelijk, over de stappen die hij gaat ondernemen, ook al heeft deze geen toestemming verleend. De medewerker legt in het cliëntdossier vast waarom hij heeft besloten zonder toestemming van de cliënt te handelen, wie hij hierover heeft gesproken en op welke wijze hij de cliënt heeft geïnformeerd.

In onze hulpverlening is het soms waardevol om cliëntgegevens uit te wisselen met derden, ook wanneer er niet direct sprake is van doelbinding. Bijvoorbeeld bij (cliënt)monitoring, intervisies of casuïstiekbesprekingen. Dit draagt bij aan het vergroten van het lerende vermogen van MO Den Bosch en draagt hierdoor bij aan het verbeteren van onze dienstverlening. Privacy van cliënten komt in deze gevallen nooit in het geding, omdat persoonsgegevens altijd geanonimiseerd worden of omdat een cliënt toestemming geeft om zijn casus te bespreken voor dit doeleinde.

Elke betrokkene heeft het recht een klacht in te dienen of bezwaar te maken tegen de wijze waarop zijn of haar persoonsgegevens worden verwerkt. Dit kan gemeld worden bij de FG.

In ons ECD wordt de informatie veilig en verantwoord geregistreerd
Cliëntgegevens mogen alleen worden geregistreerd en opgeslagen in een veilig en verantwoord registratiesysteem. Per 1-1-2020 gebruiken we ONS (NEDAP) als registratiesysteem. MO Den Bosch ziet toe op zorgvuldig gebruik en inrichting van het systeem.

Een cliëntdossier is niet voor iedereen inzichtelijk. Er is een autorisatiemodel, dat zo is opgesteld dat alleen relevante personen toegang hebben tot dossiers van cliënten. Medewerkers die toegang hebben tot dossiers hebben een geheimhoudingsplicht. Zij delen alleen gegevens met andere partijen in opdracht van- en na toestemming van de cliënt of bij veiligheidsissues.

De receptiemedewerkers en nachtwakers hebben enkel zicht op wie er in zorg zijn en hebben géén inzage in het dossier. Zij hebben dit inzicht nodig in geval een calamiteit of wanneer er sprake is van veiligheidsissues bij mensen die op een hoog-veiligheidsrisico-plek (code rood) verblijven. Zo weten zij wie zij bij een noodgeval, calamiteit of veiligheidsissue, kunnen bellen, of deze persoon verzekerd is, of deze persoon medicatie gebruikt en wie de huisarts is.

We hanteren een log-systeem zodat we kunnen volgen welke medewerker in welk dossier kijkt. Deze wordt geraadpleegd door de systeembeheerder wanneer hier aanleiding toe is.

Wij bewaren cliëntgegevens zolang als noodzakelijk is
Met inachtneming van eventuele wettelijke voorschriften bewaren wij de gegevens, zolang als noodzakelijk is, in het kader van de hulpverlening aan de betrokkene. Als de bewaartermijn is verstreken verwijderen we de betreffende persoonsgegevens uit onze systemen.

Privacy beleid medewerkers

Wij bewaren het personeelsdossier voor de duur die is vastgelegd in wet- en regelgeving
Voor een personeelsdossier gelden specifieke bewaartermijnen. Bij de meeste zaken in een personeelsdossier gelden maximum bewaartermijnen, maar soms is er ook een minimum.

Zaken die maximaal 2 jaar na einde dienstverband bewaard mogen worden

- arbeidsovereenkomsten en wijzigingen (vastgelegd in art. 52 Wet Rijksbelastingen)
- correspondentie over benoemingen, promotie, demotie en ontslag (vastgelegd in art. 52 Wet Rijksbelastingen); NB: deze moeten ook minimaal 2 jaar worden bewaard
- verslagen van functioneringsgesprekken (vastgelegd in de AVG); NB: deze moeten ook minimaal 2 jaar worden bewaard.
- verslaglegging in het kader van de Wet Verbetering Poortwachter (vastgelegd in de AVG)
- VUT-regeling (vastgelegd in art. 52 Wet Rijksbelastingen)
- afspraken over werkzaamheden voor de OR (vastgelegd in Vrijstellingsbesluit Wbp); NB: maximale bewaartermijn geldt hier 2 jaar na einde lidmaatschap, niet na einde dienstverband

Zaken die maximaal 5 jaar na einde dienstverband bewaard mogen worden

- Loonbelastingverklaringen en kopieën van identiteitsbewijzen (vastgelegd in art. 66 lid 4 Uitvoeringsregeling LB)

Zaken die maximaal 7 jaar na einde dienstverband bewaard mogen worden

- Afspraken over salaris en arbeidsvoorwaarden (vastgelegd in Wet Rijksbelastingen)

- Persoonsgegevens werknemers - NAW en Burgerlijke staat (vastgelegd in Wet Rijksbelastingen)

Bijzondere zaken en hun bewaartermijnen

Sollicitatiebrieven, - formulieren, correspondentie omtrent de sollicitatie, getuigschriften en verklaring omtrent gedrag

- Bewaartermijn: maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant
- Ingangsdatum bewaartermijn: na beëindiging sollicitatieprocedure
- Vastgelegd in: AVG

Gegevens over etniciteit en herkomst

- Bewaartermijn: minimaal 5 jaar, geen maximum
- Ingangsdatum: na einde dienstverband
- Vastgelegd in: Wet Samen (Wet Stimulering Arbeidsdeelnamen Minderheden)

Identiteitspapieren van van derden ingeleende vreemdelingen waarvoor een tewerkstellingsvergunning is verleend

- Bewaartermijn: minimaal 5 jaar, geen maximum
- Ingangsdatum: na afloop van het kalenderjaar waarin arbeid door ingeleende vreemdeling is beëindigd
- Vastgelegd in: Wet Arbeid Vreemdelingen

Loonbeslagen

- Bewaartermijn: maximaal tot het moment van opheffing
- Vastgelegd in: Vrijstellingsbesluit Wbp

Beveiligen van persoonsgegevens

Wij hebben verschillende technische en organisatorische maatregelen genomen om de persoonsgegevens die wij verwerken te beveiligen

De FG maakt door middel van melding bij het Autoriteit Persoonsgegevens het bestaan van de gegevens-verwerkingen bekend. Een afschrift van de melding aan de Autoriteit Persoonsgegevens is ter inzage beschikbaar.

We houden rekening met de, qua waarschijnlijkheid en ernst, uiteenlopende risico's voor de rechten en vrijheden van personen. Waar passend omvatten de maatregelen op grond van artikel 32 AVG onder meer het volgende:

- De pseudonimisering en versleuteling van persoonsgegevens;
- Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Wanneer wij persoonsgegevens verwerken of laten verwerken door een derde, zorgen wij ervoor dat passende beveiligingsmaatregelen worden getroffen om de betreffende persoonsgegevens te beschermen tegen de verschillende risico's.

Medewerkers weten wanneer zij een melding moeten doen van een datalek
Als er sprake is van een informatiebeveiligingsincident, waarbij bijvoorbeeld gegevens van personen in verkeerde handen kunnen komen of zijn gekomen, is voor medewerkers duidelijk hoe zij moeten handelen. Dit is vastgelegd in het Protocol Meldplicht en afhandeling van (vermoedelijke) datalekken. Dit protocol bevat een vastgesteld proces van te doorlopen stappen om de eventuele schade of de kans hierop, bij een datalek te beperken en de getroffen perso(o)n(en) te beschermen en te informeren.

Een datalek is een situatie waarbij er sprake is van een 'inbreuk in verband met persoonsgegevens'. Er is sprake van een datalek wanneer persoonsgegevens in handen komen van personen die géén zorg- of medewerker relatie hebben met de betrokken persoon en normaal gesproken ook geen toegang hebben tot deze gegevens.

Een datalek kan zich op verschillende manier voordoen en is niet altijd even ernstig. Voorbeelden van datalekken zijn bijvoorbeeld:

- dossiers die bij onbevoegden terecht komen,
- hackaanvallen waarbij cliëntgegevens gestolen worden,
- een e-mail of fax die aan de verkeerde persoon wordt gestuurd
- het kwijtraken van een laptop of USB-stick waarop een Excel sheet met afspraken staat.
- verlies van een mobiele telefoon met daarin contactgegevens van medewerkers en/of cliënten .

De Functionaris Gegevensbescherming bij Reinier van Arkel verzamelt alle noodzakelijke gegevens om de impact van de melding te bepalen. Hij/zij analyseert het incident en bepaalt of het inderdaad een datalek is of een informatiebeveiligingsincident.

Wij passen de plicht tot het melden van een (vermoeden van een) datalek toe
De plicht tot het melden van een (vermoeden van een) datalek geldt als er sprake is van een aanzienlijke kans op ernstige nadelige gevolgen voor betrokkene, dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het betreft situaties van het (mogelijk) lekken van persoonsgegevens uit bestanden van MO Den Bosch en/of gegevens waarvoor MO Den Bosch verantwoordelijkheid draagt.

Een datalek melden wij direct bij de Autoriteit Persoonsgegevens
MO Den Bosch doet direct een melding doen bij de Autoriteit Persoonsgegevens (via de FG), zodra er sprake is van een ernstig datalek. Indien nodig, wordt het datalek ook gemeld aan de mensen van wie de persoonsgegevens zijn gelekt. Wij houden van alle datalekken een registratie bij.

De toepassing van het privacy beleid wordt regelmatig geëvalueerd en gecontroleerd
Het privacy beleid wordt door de preventiemedewerker regelmatig besproken en geëvalueerd met de verschillende teams.

De Functionaris voor Gegevensbescherming (FG) houdt een verwerkingsregister bij, bestemd voor de inschrijving van verwerkingen van persoonsgegevens
Bij de inschrijving worden in ieder geval de volgende gegevens vermeld:
1. de naam van de verwerking;
2. wie de verantwoordelijke is voor de verwerking;
3. het doel van de verwerking;
4. de groep van personen van wie persoonsgegevens worden verwerkt (betrokkenen);
5. de categorie persoonsgegevens die bij de verwerking worden gebruikt;
6. de ontvangers van de gegevens;

7. de rechtmatige grondslag voor de verwerking van de persoonsgegevens;
8. eventuele verstrekkingen aan andere landen buiten de Europese Economische Ruimte;
9. De verwijderingstermijn die in acht genomen wordt.

De FG houdt toezicht op de volledigheid en rechtmatigheid van de in het register ingeschreven verwerkingen van persoonsgegevens en de daarbij behorende documenten (eventuele verwerkersovereenkomst, Privacy Impact Assessment (PIA), privacystatement, informatieverplichting). Bij wijzigingen van de bij de inschrijving opgenomen gegevens draagt de medewerker zorg voor wijziging hiervan in het register en informeert de FG hierover.