Behorende bij de Raamovereenkomst Beveiligingsdienstverlening – Veiligheid & Gastvrijheid op opvanglocaties voor Oekraïense ontheemden

Ondergetekenden

De gemeente Hilversum, waarvan het college van Burgemeester en Wethouders de verwerkingsverantwoordelijke is, te dezen rechtsgeldig vertegenwoordigd door heer of mevrouw persoonsnaam, functie
hierna verder aangeduid als: "**Verwerkingsverantwoordelijke**",

en

Bedrijf gevestigd te adres + plaatsnaam, KvK nummer <nummer> te dezen rechtsgeldig vertegenwoordigd door de heer of mevrouw, persoonsnaam , functie,
hierna verder aangeduid als: "**Verwerker**",

hierna afzonderlijk te noemen "Partij", of gezamenlijk "Partijen"

Overwegen het volgende:

a) Partijen hebben op <datum ondertekening> de Raamovereenkomst Beveiligingsdienstverlening – Veiligheid & Gastvrijheid op opvanglocaties voor Oekraïense ontheemden (hierna: Hoofdovereenkomst) gesloten, op grond waarvan Verwerker de volgende diensten levert aan Verwerkingsverantwoordelijke:
b) Het verzorgen van beveiligingsdienstverlening op de gemeentelijke opvanglocaties voor Oekraïense ontheemden, waaronder fysieke beveiliging, toegangscontrole, toezicht, signalering en registratie van veiligheidsincidenten, de-escalerend optreden, rapportage en afstemming met het locatiemanagement en andere betrokken partijen, voor zover deze werkzaamheden onderdeel uitmaken van de Hoofdovereenkomst.
c) Voor zover Verwerker bij de uitvoering van deze diensten namens Verwerkingsverantwoordelijke persoonsgegevens verwerkt, vindt deze verwerking plaats overeenkomstig de Hoofdovereenkomst en deze Verwerkersovereenkomst.
d) Verwerker verwerkt voor de uitvoering van de Hoofdovereenkomst Persoonsgegevens voor Verwerkingsverantwoordelijke;
e) Op de verwerking van Persoonsgegevens door Verwerker zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing;
f) Partijen willen in aanvulling op de AVG en de UAVG de volgende afspraken over de verwerking van Persoonsgegevens vastleggen in deze verwerkersovereenkomst (hierna: de Verwerkersovereenkomst).

Komen het volgende overeen:

Artikel 1 Definities

1.1 Begrippen uit de AVG en de UAVG die in deze Verwerkersovereenkomst worden gebruikt, hebben dezelfde betekenis.

1.2 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die onlosmakelijk deel uitmaken van deze Verwerkersovereenkomst.

Artikel 2 Ingangsdatum en duur

2.1 Deze Verwerkersovereenkomst gaat in op het moment dat de Hoofdovereenkomst tot stand is gekomen, tenzij Partijen anders overeenkomen.

2.2 Deze Verwerkersovereenkomst eindigt op het moment dat Verwerker de verwerking van Persoonsgegevens op grond van de Hoofdovereenkomst heeft beëindigd en de afspraken over het teruggeven en/of wissen van Persoonsgegevens zijn nagekomen.

2.3 Wanneer Partijen een (nieuwe) Verwerkersovereenkomst overeenkomen, betekent dat dat de oude Verwerkersovereenkomst komt te vervallen.

Artikel 3 Onderwerp van deze Verwerkersovereenkomst

3.1 Verwerker verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke voor de uitvoering van de Hoofdovereenkomst en uitsluitend overeenkomstig schriftelijke instructies van Verwerkingsverantwoordelijke, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke wettelijke bepaling hem tot verwerking verplicht. In dat geval zal Verwerker Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, daarvan zonder onredelijke vertraging in kennis stellen, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

3.2 De door Verwerker uit te voeren verwerkingen staan beschreven in tabel 1 van Bijlage 1.

Artikel 4 Inhoudelijke afspraken

4.1 Beveiligingsmaatregelen

Verwerker zorgt voor passende technische en organisatorische maatregelen om de Persoonsgegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG. De wijze waarop Verwerker de passende technische en organisatorische maatregelen aantoont, staat in Bijlage 2.

4.2 Audits

Verwerker verleent alle benodigde medewerking aan audits uitgevoerd door een gecertificeerde auditor over de nakoming van de afspraken binnen deze Verwerkersovereenkomst en Bijlagen, tenzij Verwerker door middel van een geldige certificering, die periodiek door een geaccrediteerde instelling wordt getoetst, heeft aangetoond dat Verwerker de gemaakte afspraken nakomt. De kosten van deze audit worden gedragen door Verwerkingsverantwoordelijke (zowel eigen kosten als kosten van Verwerker), tenzij de auditor één of meer tekortkomingen van niet ondergeschikte aard van Verwerker constateert die ten nadele zijn van Verwerkingsverantwoordelijke.

4.3 Verwerking buiten de EER

Verwerker mag Persoonsgegevens buiten de Europese Economische Ruimte (laten) verwerken wanneer is voldaan aan de voorwaarden van artikel 45 en 46 AVG. Wanneer er sprake is van een verwerking buiten de EER, dan stelt Verwerker Verwerkingsverantwoordelijke daarvan vooraf op de hoogte.

4.4 Geheimhouding

Personen die werken voor (sub)Verwerker en (sub)Verwerker zelf, moeten Persoonsgegevens waarmee zij werken geheimhouden. De personen die werken voor Verwerker en subverwerkers hebben daarom een geheimhoudingsverklaring getekend, of zich op een andere manier schriftelijk gebonden aan de geheimhouding.

4.5 Subverwerkers

De ten tijde van het afsluiten van deze Verwerkersovereenkomst bekende subverwerkers vermeldt Verwerker in tabel 3 van Bijlage 1. Verwerkingsverantwoordelijke verleent hierbij algemene toestemming voor de inschakeling van subverwerkers. Verwerker houdt na de start van de werkzaamheden Verwerkingsverantwoordelijke op de hoogte van de beoogde inschakeling van nieuwe subverwerkers. Bij de inschakeling van subverwerkers blijven de artikelen 28.2 en 28.4 AVG onverkort van kracht.

4.6 Rechten van betrokkenen

Als een betrokkene een beroep doet op zijn rechten zoals genoemd in artikel 12 t/m 22 AVG, helpt Verwerker Verwerkingsverantwoordelijke om daarop binnen de wettelijke termijnen een beslissing te nemen.

4.7 Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging

Op verzoek van Verwerkingsverantwoordelijke werkt Verwerker altijd mee aan een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG.

Artikel 5 Inbreuk in verband met Persoonsgegevens

5.1 Verwerker zal Verwerkingsverantwoordelijke zonder onredelijke vertraging, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens. Verwerker vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen.

5.2 In geval van een Inbreuk neemt Verwerker zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen en houdt de Verwerkingsverantwoordelijke hiervan voortdurend op de hoogte.

5.3 Verwerker heeft een gedetailleerd logboek van de Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat inzien, wanneer deze daarom vraagt.

5.4 Verwerkingsverantwoordelijke beslist of de Inbreuk moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene. Verwerker ondersteunt de Verwerkingsverantwoordelijke waar nodig bij de melding aan de toezichthoudende autoriteit en/of Betrokkene.

Artikel 6 Aansprakelijkheid

6.1 Eventuele in de Hoofdovereenkomst overeengekomen beperkingen van de aansprakelijkheid hebben ook betrekking op de Verwerkersovereenkomst.

Artikel 7 Beëindigen verwerkersovereenkomst

7.1 Partijen moeten in de Hoofdovereenkomst afspraken maken over de beëindiging van de Hoofdovereenkomst en de daaruit voortvloeiende teruggave en wissing van Persoonsgegevens.

7.2 De geheimhouding geldt ook nog na beëindiging van deze Verwerkersovereenkomst.

Artikel 8 Overige bepalingen

8.1 Op deze overeenkomst is Nederlands recht van toepassing. Alle geschillen, ook als alleen één Partij vindt dat er een geschil is, zullen in eerste instantie worden voorgelegd aan dezelfde bevoegde rechter als genoemd in de Hoofdovereenkomst.

Ondertekening

Aldus overeengekomen en in tweevoud ondertekend,

Ingangsdatum: ……

De Gemeente Hilversum	Naam organisatie
De burgemeester van de gemeente Hilversum	
namens deze: naam, functie	namens deze: naam, functie
plaats: ……..	plaats: ……
datum: ……..	datum: ……..

BIJLAGE 1 – OVERZICHT VAN TE VERWERKEN PERSOONSGEGEVENS, CONTACTGEGEVENS PARTIJEN EN INGESCHAKELDE SUBVERWERKERS

1. Naam verwerking, doeleinden, categorieën van betrokkenen, categorieën persoonsgegevens en eventuele doorgifte naar derde landen

De Verwerker verwerkt, voor zover noodzakelijk voor de uitvoering van de Hoofdovereenkomst en uitsluitend voor zover hij daarbij namens de Verwerkingsverantwoordelijke handelt, persoonsgegevens in het kader van de beveiligingsdienstverlening op de gemeentelijke opvanglocaties voor Oekraïense ontheemden.

De verwerking heeft uitsluitend betrekking op persoonsgegevens die noodzakelijk zijn voor het uitvoeren van de overeengekomen beveiligingswerkzaamheden, waaronder toegangscontrole, toezicht, incidentregistratie, veiligheidsrapportages, operationele overdracht en communicatie met het locatiemanagement.

De volgende tabel bevat de voorziene verwerkingen. De feitelijke inrichting, gebruikte systemen en eventuele aanvullende verwerkingen worden vóór aanvang van de dienstverlening door Partijen vastgesteld.

Naam verwerking / dienst	**Verwerkingsdoeleinden**	**Categorieën van betrokkenen**	**(Bijzondere) persoonsgegevens**	**Verwerkingslocatie**	**Doorgifte-instrument**	**Aanvullende maatregelen**
Toegangscontrole en bezoekersregistratie	Het controleren en registreren van toegang tot opvanglocaties, het voorkomen van onbevoegde toegang en het waarborgen van de veiligheid.	Bewoners, bezoekers, medewerkers, leveranciers en overige aanwezigen.	Naam, datum en tijdstip van bezoek, bezoekdoel of contactpersoon en overige strikt noodzakelijke identificerende gegevens.	Gemeentelijke opvanglocaties en eventuele registratiesystemen van de Verwerker, voor zover vastgesteld.	Niet van toepassing indien geen doorgifte buiten de EER plaatsvindt. Eventuele doorgifte nader vast te stellen.	Toegangsbeperking, gegevensminimalisatie, beveiligde registratie en bewaartermijnen volgens instructies van de gemeente.
Incidentregistratie en veiligheidsrapportage	Het registreren, opvolgen en evalueren van veiligheidsinci	Bewoners, bezoekers, medewerkers en overige bij	Naam of andere noodzakelijke identificeren	Gemeentelijke opvanglocaties en de daarvoor aangewezen rapportage- of	Niet van toepassing indien	Beperkte toegang, vertrouwelijke behandeling, beveiligde

	denten en het informeren van bevoegde contactpersonen.	incidenten betrokken personen.	de gegevens, datum, tijdstip, locatie, feitelijke incidentomschrijving en genomen maatregelen. Incidenteel kunnen gevoelige of bijzondere persoonsgegevens voorkomen, uitsluitend voor zover rechtmatig en noodzakelijk.	registratiesystemen.	geen doorgifte buiten de EER plaatsvindt. Eventuele doorgifte nader vast te stellen.	overdracht, feitelijke verslaglegging en beperking van gevoelige gegevens.
Dagrapportages en operationele overdracht	Het waarborgen van continuïteit, informatieoverdracht en opvolging van relevante veiligheidszaken tussen beveiligingsdiensten en locatiemanagement.	Bewoners, bezoekers, medewerkers en overige betrokkenen.	Alleen noodzakelijke identificerende gegevens en relevante feitelijke bijzonderheden over veiligheid en incidenten.	Gemeentelijke opvanglocaties en de overeengekomen rapportagesystemen.	Niet van toepassing indien geen doorgifte buiten de EER plaatsvindt. Eventuele doorgifte nader vast te stellen.	Rolgebaseerde toegang, beveiligde overdracht en beperking van de gegevens tot hetgeen noodzakelijk is.
Communicatie en escalatie bij incidenten	Het afstemmen van veiligheidsmaatregelen, het	Contactpersonen van de gemeente, locatiemanagement,	Naam, functie, zakelijke contactgegevens en	Gemeentelijke opvanglocaties en de overeengekomen	Niet van toepassing indien	Beveiligde communicatie, beperkte verspreiding en uitsluitend

en calamiteiten	melden van incidenten en het ondersteunen van een adequate opvolging.	medewerkers, bewoners en overige direct betrokkenen.	uitsluitend noodzakelijke incidentgerelateerde gegevens.	communicatievoorzieningen.	geen doorgifte buiten de EER plaatsvindt. Eventuele doorgifte nader vast te stellen.	informatieverstrekking aan bevoegde ontvangers.

1.1 Uitgangspunten voor de verwerking

1. De Verwerker verwerkt persoonsgegevens uitsluitend voor de doeleinden die voortvloeien uit de Hoofdovereenkomst en deze Verwerkersovereenkomst, overeenkomstig de gedocumenteerde instructies van de Verwerkingsverantwoordelijke.
2. De Verwerker verwerkt niet meer persoonsgegevens dan noodzakelijk voor de uitvoering van de overeengekomen beveiligingswerkzaamheden.
3. Bijzondere persoonsgegevens, waaronder gezondheidsgegevens, worden niet standaard geregistreerd. Indien dergelijke gegevens bij een incident noodzakelijkerwijs worden verwerkt, gebeurt dit uitsluitend voor zover daarvoor een geldige juridische grondslag en, indien vereist, een toepasselijke uitzondering op het verwerkingsverbod bestaat.
4. Gegevens over strafrechtelijke feiten of vermoedens daarvan worden uitsluitend verwerkt voor zover dit wettelijk is toegestaan en noodzakelijk is voor de betreffende verwerking.
5. De Verwerker verstrekt persoonsgegevens uitsluitend aan personen of organisaties die daartoe bevoegd zijn en voor zover deze verstrekking noodzakelijk en rechtmatig is.
6. De Verwerker gebruikt persoonsgegevens niet voor eigen commerciële doeleinden of andere doeleinden die buiten de gedocumenteerde instructies van de Verwerkingsverantwoordelijke vallen.
7. De Verwerker past passende technische en organisatorische beveiligingsmaatregelen toe, rekening houdend met de aard van de persoonsgegevens, de risico's voor betrokkenen en de omstandigheden van de verwerking.
8. De Verwerker bewaart persoonsgegevens niet langer dan noodzakelijk. De concrete bewaartermijnen en verwijderafspraken worden vóór de betreffende verwerking vastgesteld overeenkomstig de instructies van de Verwerkingsverantwoordelijke en de toepasselijke wet- en regelgeving.
9. Doorgifte van persoonsgegevens buiten de Europese Economische Ruimte vindt uitsluitend plaats indien dit is toegestaan op grond van de AVG, de vereiste waarborgen zijn getroffen en aan de toepasselijke contractuele voorwaarden is voldaan.

10. Indien tijdens de uitvoering aanvullende categorieën persoonsgegevens of nieuwe verwerkingen noodzakelijk blijken, worden deze vooraf beoordeeld en, waar nodig, schriftelijk in dit overzicht verwerkt.

1.2 Nog vast te stellen gegevens

Voorafgaand aan de betreffende verwerking leggen Partijen de volgende gegevens vast:

- De daadwerkelijk gebruikte registratiesystemen en applicaties.
- De fysieke en digitale verwerkingslocaties.
- De concrete bewaartermijnen en verwijderprocedures.
- De eventuele inzet van subverwerkers.
- De eventuele doorgifte van persoonsgegevens buiten de EER en de toepasselijke waarborgen.
- De aanvullende beveiligingsmaatregelen die nodig zijn gelet op de aard en risico's van de verwerking.

2. Contactgegevens

2.1 Contactpersoon Verwerkingsverantwoordelijke

Organisatie: Gemeente Hilversum
Contactpersoon: Privacyteam Hilversum
E-mailadres: privacy@hilversum.nl
Telefoonnummer: 14 035.

Melden van datalekken

Datalekken en beveiligingsincidenten waarbij persoonsgegevens betrokken zijn, worden onverwijld gemeld overeenkomstig de meldprocedure en termijnen uit de Verwerkersovereenkomst.

De gemeente beschikt over een datalekformulier via haar gemeentelijke website.

Buiten kantooruren

In noodsituaties buiten kantooruren kan contact worden opgenomen via de Informatiebeveiligingsdienst voor gemeenten (IBD), overeenkomstig de gemeentelijke incidentprocedure.

2.2 Contactpersoon Verwerker

Organisatie: <naam Opdrachtnemer>
Contactpersoon: <naam en functie>
E-mailadres: <in te vullen>
Telefoonnummer: <in te vullen>
Telefoonnummer buiten kantooruren / 24/7 bereikbaar: <in te vullen>
E-mailadres voor datalekken en beveiligingsincidenten: <in te vullen>

De Verwerker zorgt ervoor dat de opgegeven contactgegevens actueel zijn en dat meldingen van datalekken en beveiligingsincidenten tijdig kunnen worden ontvangen en opgevolgd, ook buiten reguliere kantooruren.

2.3 Contactgegevens Informatiebeveiligingsdienst voor gemeenten (IBD)

Organisatie: Informatiebeveiligingsdienst voor gemeenten – IBD-CERT
Telefonische bereikbaarheid: 24/7
Telefoonnummer: 070-204 55 11
E-mailadres: incident@ibdgemeenten.nl

Via de IBD kunnen de vertrouwde contactpersonen van gemeente Hilversum worden geïnformeerd overeenkomstig de geldende incidentprocedure.

De contactgegevens en werkwijze worden vóór vaststelling van deze bijlage door de gemeente gecontroleerd.

3. Ingeschakelde subverwerkers

De Verwerker verstrekt vóór aanvang van de betreffende persoonsgegevensverwerking een actueel overzicht van alle subverwerkers die namens hem persoonsgegevens verwerken ten behoeve van de uitvoering van de Hoofdovereenkomst.

Indien geen subverwerkers worden ingezet, wordt dit uitdrukkelijk vermeld.

Naam en contactgegevens subverwerker	**KvK-nummer**	**Uitbestede verwerkingen**	**Toepassing / geautomatiseerd systeem**	**Verwerkingslocatie**	**Doorgifte-instrument**	**Aanvullende maatregelen**
<in te vullen door Verwerker>	<in te vullen>	<in te vullen>	<in te vullen>	<in te vullen>	<in te vullen / niet van toepassing>	<in te vullen>
<in te vullen door Verwerker>	<in te vullen>	<in te vullen>	<in te vullen>	<in te vullen>	<in te vullen / niet van toepassing>	<in te vullen>
<in te vullen door Verwerker>	<in te vullen>	<in te vullen>	<in te vullen>	<in te vullen>	<in te vullen / niet van toepassing>	<in te vullen>

Indien geen subverwerkers worden ingezet:

☐ Verwerker verklaart dat voor de in deze bijlage beschreven persoonsgegevensverwerkingen geen subverwerkers worden ingezet.

3.1 Voorwaarden voor inzet van subverwerkers

1. De inzet van subverwerkers vindt uitsluitend plaats overeenkomstig de bepalingen van de Verwerkersovereenkomst en artikel 28 AVG.

2. De Verwerker zorgt ervoor dat aan subverwerkers passende contractuele verplichtingen worden opgelegd, waaronder verplichtingen inzake vertrouwelijkheid, beveiliging, ondersteuning bij datalekken en naleving van de toepasselijke privacywetgeving.
3. De Verwerker blijft tegenover de Verwerkingsverantwoordelijke verantwoordelijk voor de nakoming van de aan de subverwerker opgelegde verplichtingen.
4. Wijzigingen in het overzicht van subverwerkers worden tijdig doorgegeven overeenkomstig de afspraken in de Verwerkersovereenkomst.
5. Het enkele feit dat een onderneming als onderaannemer beveiligingswerkzaamheden verricht, betekent niet automatisch dat deze onderneming een subverwerker is. Dit wordt bepaald door de feitelijke verwerking van persoonsgegevens.

NB: Substantiële wijzigingen in de bovenstaande tabellen worden door Partijen tijdig aan elkaar doorgegeven en, waar nodig, schriftelijk verwerkt in deze bijlage.

BIJLAGE 2 – AANTONEN PASSEND NIVEAU VAN BEVEILIGING

Behorende bij de Verwerkersovereenkomst inzake de Raamovereenkomst Beveiligingsdienstverlening – Veiligheid & Gastvrijheid op opvanglocaties voor Oekraïense ontheemden

Verwerkingsverantwoordelijke: Gemeente Hilversum
Verwerker: <naam Opdrachtnemer>
Aanbestedingskenmerk: 1993097
Datum: <in te vullen>

1. Normenstelsel

De Verwerker draagt zorg voor een passend niveau van informatiebeveiliging bij de verwerking van persoonsgegevens in het kader van de Hoofdovereenkomst.

De beveiligingsmaatregelen worden afgestemd op de aard, omvang, context en doeleinden van de verwerking en de risico's voor de rechten en vrijheden van betrokkenen, overeenkomstig artikel 32 AVG.

In de Aanbestedingsleidraad, paragraaf 3.7.2.3, is bepaald dat de Inschrijver beschikt over een gecertificeerd managementsysteem voor informatiebeveiliging volgens NEN-EN-ISO/IEC 27001 of een toegestaan gelijkwaardig certificaat of bewijs.

De Verwerker geeft hieronder aan welk normenstelsel wordt toegepast.

☐ **De Verwerker werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten:**

NEN-EN-ISO/IEC 27001 of gelijkwaardig, overeenkomstig paragraaf 3.7.2.3 van de Aanbestedingsleidraad.

Naam normenstelsel: <in te vullen>
Certificerende instantie: <in te vullen, indien van toepassing>
Certificaatnummer: <in te vullen, indien van toepassing>
Geldigheidsdatum certificaat: <in te vullen, indien van toepassing>

☐ **De Verwerker werkt volgens een algemeen erkende overheidsnorm, zoals BIO2, of een vergelijkbaar normenstelsel, te weten:**

<in te vullen, indien van toepassing>

☐ **De Verwerker werkt volgens een andere norm of een gelijkwaardig stelsel van informatiebeveiligingsmaatregelen, te weten:**

<in te vullen, indien van toepassing>

Toelichting op de toepasselijkheid van het normenstelsel op de dienstverlening en gebruikte systemen:

<in te vullen door Verwerker>

2. Toereikendheid van de informatiebeveiliging

De Verwerker toont aan dat de getroffen technische en organisatorische beveiligingsmaatregelen passend zijn voor de persoonsgegevensverwerkingen zoals beschreven in Bijlage 1.

De Verwerker geeft hieronder aan met welke documenten of bewijsstukken de toereikendheid van de informatiebeveiliging wordt onderbouwd.

☐ Verwerker verstrekt een actueel en geldig certificaat en, voor zover relevant en beschikbaar, de bijbehorende Verklaring van Toepasselijkheid (VvT).

☐ Verwerker verstrekt rapportages van periodieke externe controles, zoals audits, penetratietesten of Third Party Mededelingen (TPM's), bijvoorbeeld ISAE- of SOC-rapportages.

☐ Verwerker verstrekt een assurance-rapport van een onafhankelijke auditor, bijvoorbeeld een auditor die is aangesloten bij NOREA.

☐ Verwerker verstrekt een beschrijving van eigen controles en de toegepaste beveiligingsmaatregelen, inclusief de wijze waarop de werking daarvan wordt gecontroleerd.

☐ Verwerker verstrekt andere gelijkwaardige bewijsstukken, te weten:

<in te vullen>

2.1 Beschrijving van de beveiligingsmaatregelen

Voor zover deze maatregelen relevant zijn voor de in Bijlage 1 opgenomen verwerkingen, beschrijft de Verwerker hoe invulling wordt gegeven aan de volgende onderwerpen:

a. Toegangsbeveiliging en autorisatie

Toegang tot persoonsgegevens is beperkt tot medewerkers die deze gegevens voor hun werkzaamheden nodig hebben. De Verwerker past passende autorisatieprocedures toe en beoordeelt toegangsrechten periodiek.

b. Vertrouwelijkheid en geheimhouding

Medewerkers die toegang hebben tot persoonsgegevens zijn gebonden aan passende geheimhoudingsverplichtingen. De Verwerker zorgt ervoor dat medewerkers worden geïnstrueerd over de zorgvuldige omgang met persoonsgegevens.

c. Beveiliging van systemen en gegevens

De Verwerker treft passende maatregelen ter bescherming tegen ongeoorloofde toegang, verlies, wijziging en openbaarmaking van persoonsgegevens. Hieronder kunnen onder meer versleuteling, beveiligde verbindingen, systeembeheer, logging en passende toegangsbeveiliging vallen.

d. Incidenten en datalekken

De Verwerker beschikt over procedures voor het herkennen, registreren, onderzoeken, beperken en melden van informatiebeveiligingsincidenten en datalekken.

Datalekken worden overeenkomstig de Verwerkersovereenkomst onverwijld aan de Verwerkingsverantwoordelijke gemeld, zodat de gemeente tijdig kan beoordelen of melding aan de Autoriteit Persoonsgegevens of betrokkenen noodzakelijk is.

e. Continuïteit en beschikbaarheid

De Verwerker treft passende maatregelen om de beschikbaarheid van relevante informatie en systemen te waarborgen en de dienstverlening bij verstoringen zo spoedig mogelijk te kunnen herstellen.

f. Bewaartermijnen en verwijdering

De Verwerker zorgt ervoor dat persoonsgegevens worden bewaard en verwijderd overeenkomstig de vastgestelde bewaartermijnen en gedocumenteerde instructies van de Verwerkingsverantwoordelijke.

g. Controle en evaluatie

De Verwerker controleert en evalueert periodiek de werking van de getroffen beveiligingsmaatregelen en treft waar nodig verbetermaatregelen.

h. Beveiliging bij inzet van subverwerkers

De Verwerker beoordeelt of eventuele subverwerkers passende beveiligingsmaatregelen treffen en ziet erop toe dat de relevante verplichtingen contractueel worden vastgelegd.

2.2 Nadere toelichting door Verwerker

Toegepast normenstelsel en reikwijdte:

<in te vullen door Verwerker>

Gebruikte systemen voor persoonsgegevensverwerking:

<in te vullen door Verwerker>

Beschrijving van relevante technische en organisatorische maatregelen:

<in te vullen door Verwerker>

Wijze waarop de werking van de beveiligingsmaatregelen wordt gecontroleerd:

<in te vullen door Verwerker>

Eventuele aanvullende maatregelen vanwege de aard van de opvanglocaties en de betrokken persoonsgegevens:

<in te vullen door Verwerker>

3. Aansluiting bij goedgekeurde gedragscode

☐ De Verwerker is aangesloten bij een door een bevoegde toezichthoudende autoriteit goedgekeurde gedragscode als bedoeld in artikel 40 AVG.

Naam gedragscode:

<in te vullen>

Toezichthoudende of verantwoordelijke instantie:

<in te vullen>

☐ Niet van toepassing.

4. Wijzigingen en actualisatie

1. De Verwerker informeert de Verwerkingsverantwoordelijke tijdig over substantiële wijzigingen in het toegepaste normenstelsel, de certificeringsstatus of de technische en organisatorische beveiligingsmaatregelen.

2. De Verwerker informeert de Verwerkingsverantwoordelijke eveneens wanneer sprake is van omstandigheden die een wezenlijke achteruitgang van het beveiligingsniveau kunnen veroorzaken.
3. De Verwerker houdt de beveiligingsmaatregelen gedurende de looptijd van de Hoofdovereenkomst passend bij de aard en risico's van de persoonsgegevensverwerkingen.
4. Indien wijzigingen in de dienstverlening of persoonsgegevensverwerkingen daartoe aanleiding geven, beoordelen Partijen of aanvullende maatregelen noodzakelijk zijn.
5. De Verwerkingsverantwoordelijke kan overeenkomstig de Verwerkersovereenkomst om informatie of bewijsstukken verzoeken om de naleving van de overeengekomen beveiligingsverplichtingen te controleren.

NB: Uit de certificering, de periodieke controles, audits of de overige verstrekte bewijsstukken moet blijken, of redelijkerwijs kunnen worden afgeleid, dat het beveiligingsniveau passend is voor de verwerkingen zoals opgenomen in Bijlage 1.

Substantiële wijzigingen in bovenstaande gegevens en relevante achteruitgang van de beveiligingsmaatregelen worden door Partijen tijdig aan elkaar doorgegeven.