

SAMENWERKINGSOVEREENKOMST ONDERSTEUNING MET NOODZAKELIJK VERBLIJF 2018 - 2022

De gemeente Amersfoort, te dezen krachtens machtiging van de burgemeester op grond van artikel 171, tweede lid Gemeentewet, rechtsgeldig vertegenwoordigd door de heer Tigelaar, wethouder, verder te noemen “Amersfoort”,

en

De gemeenten:

- Baarn, te dezen krachtens machtiging van de burgemeester op grond van artikel 171, tweede lid Gemeentewet, rechtsgeldig vertegenwoordigd door, wethouder,
- Bunschoten, te dezen krachtens machtiging van de burgemeester op grond van artikel 171, tweede lid Gemeentewet, rechtsgeldig vertegenwoordigd door, wethouder,
- Leusden, te dezen krachtens machtiging van de burgemeester op grond van artikel 171, tweede lid Gemeentewet, rechtsgeldig vertegenwoordigd door, wethouder,
- Nijkerk, te dezen krachtens machtiging van de burgemeester op grond van artikel 171, tweede lid Gemeentewet, rechtsgeldig vertegenwoordigd door, wethouder,
- Soest, te dezen krachtens machtiging van de burgemeester op grond van artikel 171, tweede lid Gemeentewet, rechtsgeldig vertegenwoordigd door, wethouder,
- Veenendaal, te dezen krachtens machtiging van de burgemeester op grond van artikel 171, tweede lid Gemeentewet, rechtsgeldig vertegenwoordigd door, wethouder,
- Woudenberg, te dezen krachtens machtiging van de burgemeester op grond van artikel 171, tweede lid Gemeentewet, rechtsgeldig vertegenwoordigd door, wethouder,

Tezamen te noemen “Regiogemeenten”,

en Amersfoort en de Regiogemeenten gezamenlijk te noemen “Partijen”,

Overwegende dat:

1. Partijen ieder voor zich op grond van artikelen 1.2.1 onder b en c en 2.2.3 van de Wet maatschappelijke ondersteuning 2015 verantwoordelijk zijn voor het bieden van voorzieningen en het nemen van besluiten onder andere op het gebied van ondersteuning met beschermd wonen en maatschappelijke opvang: (hierna: ondersteuning met noodzakelijk verblijf).
2. Partijen samenwerken op het gebied van ondersteuning met noodzakelijk verblijf en deze samenwerking willen intensiveren;
3. Amersfoort een wettelijke centrumgemeentefunctie hieromtrent heeft;
4. Daarbij wordt uitgegaan van een intensieve samenwerking tussen gemeenten waarin gestreefd wordt naar één regionaal inkoopproces en één regionaal uitvoeringsapparaat. In deze overeenkomst worden de wederzijdse verplichtingen, taken en verantwoordelijkheden nader uitgewerkt.

Komen het volgende overeen:

Artikel 1 Doel van de overeenkomst

Deze overeenkomst heeft tot doel het vastleggen van de afspraken tussen Partijen over de wijze waarop invulling wordt gegeven aan de samenwerking op het gebied van ondersteuning met noodzakelijk verblijf.

Artikel 2 Inwerkingtreding en looptijd

1. Deze overeenkomst treedt in werking op 1 oktober 2018 (en werkt terug tot en met 1 oktober 2018) en heeft een looptijd tot en met 31 december 2021.
2. De overeenkomst kan daarna telkens met 1 jaar worden verlengd.

3. Elke twee jaar wordt deze overeenkomst geëvalueerd. In de evaluatie wordt ingegaan op de verplichtingen van de regiogemeenten en de verplichtingen van de gemeente Amersfoort (artikel 3, 4 en 5).
4. De gemeente Amersfoort initieert deze tweejaarlijkse evaluatie. Alle regiogemeenten leveren hiervoor de nodige input.

Artikel 3 Verplichtingen Regiogemeenten

1. De Regiogemeenten verplichten zich tot:
 - a. Het op basis van het regionale beleidskader opvang en bescherming voorbereiden van het raadsbesluit over de gemeentelijke verordening als bedoeld in artikel 2.1.3. van de Wmo 2015.
 - b. Het vaststellen van nadere regels op basis van en die voortvloeien uit de onder a bedoelde verordening.
 - c. Het ervoor zorg dragen dat Amersfoort over de mandaten beschikt die in het kader van Beschermd Wonen en Opvang zoals bedoeld in de Wmo nodig zijn om de aan haar opgedragen taken adequaat uit te kunnen voeren.
2. De Regiogemeenten spannen zich maximaal in om ervoor te zorgen dat de in het eerste lid bedoelde beleidskader, verordeningen en nadere regels zoveel mogelijk uniform worden vastgesteld.
3. Indien een Regiogemeente inhoudelijk wenst af te wijken van het door Amersfoort aangeleverde voorstel, vindt daarover eerst overleg plaats tussen de Regiogemeenten en Amersfoort. Het college van de Regiogemeente is gehouden om in het college- of raadsvoorstel duidelijk aan te geven wat de verschillen zijn tussen het door Amersfoort aangeleverde voorstel en het door het eigen college voorgelegde voorstel, met een onderbouwing en de (financiële) consequenties daarvan.
4. Indien een Regiogemeente een inhoudelijk afwijkend plan, dan wel afwijkende verordening of nadere regels vaststelt, treden de Regiogemeente en Amersfoort in overleg over de gevolgen daarvan, onverminderd het gestelde in artikel 10, vierde lid.
5. Partijen spannen zich maximaal in om de lokale zorg zodanig in te richten en te organiseren dat zoveel als redelijkerwijs mogelijk is wordt gewaarborgd dat alleen die cliënten naar de opvang of beschermd wonen worden verwezen die daar werkelijk voor in aanmerking komen.

Artikel 4 Verplichtingen Amersfoort

Amersfoort verplicht zich tot:

- a. Het ter beschikking stellen aan de Regiogemeenten van de eigen verordening als bedoeld in artikel 2.1.3. van de Wmo 2015 en de eventuele nadere regels die daarop zijn gebaseerd.
- b. Het, waar nodig, plegen van overleg met maatschappelijke organisaties en ketenpartners over de in het eerste lid artikel 3 bedoelde beleidskader, verordeningen en nadere regels.
- c. Het opstellen en vaststellen van beleidsregels, na overleg met de Regiogemeenten.
- d. Het opdragen van de uitvoering van de taken ten aanzien van de ondersteuning met noodzakelijk verblijf aan de Stichting Sociale Wijkteams Amersfoort (SWA).
- e. Het (onder)mandateren van de bevoegdheden die de SWA nodig heeft om de aan haar opgedragen taken adequaat te kunnen uitvoeren.
- f. Het sluiten van een Dienstverleningsovereenkomst met de SWA over de wijze waarop en de voorwaarden waaronder de SWA haar taken uitvoert en daar verantwoording over aflegt aan Amersfoort.
- g. Het aansturen en houden van toezicht op de uitvoering van de taken door de SWA.
- h. Het afleggen van verantwoording aan de Regiogemeenten over de wijze waarop de SWA haar taken uitvoert.
- i. Het opstellen van halfjaarlijkse financiële en beleidsrapportages.
- j. Het organiseren van periodiek overleg tussen de portefeuillehouders van Partijen.
- k. Het inkopen van de voor de uitvoering van de wettelijke taken noodzakelijke diensten.
- l. Het vertegenwoordigen van de Regiogemeenten in het landelijk portefeuillehoudersoverleg beschermd wonen en opvang.
- m. Het terugkoppelen uit het landelijk portefeuillehoudersoverleg en tussentijds informeren van de Regiogemeenten over nieuwe ontwikkelingen die van invloed kunnen zijn op het beleid en/of op de financiële aspecten daarvan.

Artikel 5 Financiering

1. Ten aanzien van de financiering van de uitvoering van de in artikel 4 beschreven taken geldt het volgende:
 - a. Het onderdeel Opvang kent een eigen budget dat bestaat uit de daarvoor bestemde Rijksbijdrage;
 - b. Het onderdeel Beschermd Wonen kent een eigen budget dat bestaat uit:
 - i. De daarvoor bestemde Rijksbijdrage;
 - ii. De inkomsten die Amersfoort, ook voor wat betreft de Regiogemeenten, ontvangt van het CAK uit de eigen bijdrage van cliënten voor wat betreft de intramurale zorg.
2. Op het bedrag dat de uitkomst is van de optelsom van de in het eerste lid onder a en b genoemde elementen worden de volgende kosten in mindering gebracht:
 - a. de apparaatskosten;
 - b. de uitvoeringskosten van de SWA.
3. Indien het budget ontoereikend is, is Amersfoort aansprakelijk voor het verschil.
4. In het geval van een overschot, mag Amersfoort het overschot houden.

Artikel 6 Begroting

1. Amersfoort legt elk jaar in het eerste overleg na de ontvangst van de meicirculaire, via het BOSD, een specifiek op de uitvoering van de in deze overeenkomst bedoelde taken gerichte begroting voor aan de colleges van de Regiogemeenten, voor het daarop volgende begrotingsjaar.
De begroting is gebaseerd op de uitgangspunten als bedoeld in artikel 5, eerste en tweede lid.

Artikel 7 Communicatie

Partijen stellen gezamenlijk een communicatieplan op voor de communicatie met de media en anderen over de uitvoering van de in deze overeenkomst bedoelde taken, waaronder begrepen communicatie over incidenten en crisissituaties.

Artikel 8 Ambtelijk en bestuurlijke beleidsafstemming en besluitvorming

1. Partijen spreken de intentie uit om zoveel mogelijk uniform beleid vast te stellen.
2. Besluiten met betrekking tot inkoop en het regionale beleidskader worden besproken in het Bestuurlijk Overleg Sociaal Domein. Dit wordt in regionaal verband ambtelijk voorbereid.
3. Na instemming door het BOSD vindt besluitvorming plaats in de colleges dan wel gemeenteraden in de verschillende gemeenten.

Artikel 9 Verantwoording

1. Amersfoort verplicht zich om ten minste een keer per jaar een rapportage op te stellen, waarin verantwoording wordt afgelegd over de uitvoering van de taken zoals die in deze overeenkomst aan Amersfoort zijn opgedragen en over de financiële aspecten die daarbij horen.
2. Vragen of opmerkingen van de colleges van de Regiogemeenten worden schriftelijk aan het college van Amersfoort toegezonden met een afschrift aan alle Regiogemeenten.

Artikel 10 Geschillen

1. Partijen maken onderscheid in geschillen over:
 - a. de inhoud van beleid, zoals dat wordt vastgelegd in beleidsnota's, verordeningen, nadere regels en beleidsregels;
 - b. overige geschillen.
2. Geschillen in het Bestuurlijk Overleg Sociaal Domein over de inhoud van beleidsvoorstellen als bedoeld in het eerste lid onder a, die ter besluitvorming aan het college of de raad moeten worden voorgelegd, worden vastgelegd in het verslag van de vergadering. Elke Partij is bevoegd om een concept voorstel aan zijn college of raad ter besluitvorming voor te leggen. Het gestelde in artikel 3, tweede, derde en vierde lid is daarop van toepassing.
3. Indien een Regiogemeente een voorstel vaststelt dat afwijkt van het voorstel van het Bestuurlijk Overleg, kan Amersfoort:
 - a. Aanvullende kosten in rekening brengen indien de uitvoering van dat afwijkende beleid tot meerkosten leidt;
 - b. Weigeren het afwijkende beleid uit te voeren. In dat geval treden Partijen in overleg over de gevolgen daarvan.

4. Geschillen in het Bestuurlijk Overleg Sociaal Domein over aangelegenheden als bedoeld in lid 1, onder b, waar op bestuurlijk niveau geen oplossing voor wordt gevonden, worden voorgelegd aan de bevoegde rechter van de rechtbank Midden-Nederland.

Aldus overeengekomen te:

Leusden, 2018

.....

Amersfoort, 2018

.....

Veenendaal, 2018

.....

Nijkerk, 2018

.....

Woudenberg, 2018

.....

Bunschoten, 2018

.....

Soest, 2018

.....

Baarn, 2018

.....

MANDAAT

Het college van burgemeester en wethouders van de gemeente Woudenberg

overwegende:

dat op 1 januari 2015 de nieuwe Wet maatschappelijke ondersteuning 2015 (hierna: de Wet) in werking is getreden, welke gemeenten opdracht geeft zorg te dragen voor maatschappelijke ondersteuning, waaronder onder meer het bieden van beschermd wonen en opvang wordt verstaan;

dat de Wet voor het bieden van beschermd wonen en opvang geen formeel onderscheid meer kent tussen centrumgemeenten en regiogemeenten;

dat echter voor opvang en beschermd wonen tussen het Rijk en de VNG is afgesproken de in 2014 bestaande materiële situatie, dus de constructie met de centrumgemeenten, voorlopig te handhaven;

dat de middelen voor opvang en beschermd wonen daarmee voorlopig worden uitgekeerd aan de centrumgemeente Amersfoort;

dat de regiogemeenten met de gemeente Amersfoort een samenwerkingsovereenkomst hebben gesloten over de uitvoering van de Centrale Toegang voor ondersteuning met noodzakelijk verblijf;

dat regiogemeenten wel een schriftelijk mandaat moeten geven om de wethouder van de centrumgemeente Amersfoort bevoegd te maken om, namens hen, besluiten te nemen inzake beschermd wonen;

dat als – zoals de bedoeling is – na verloop van tijd de centrumgemeentenconstructie wordt afgeschaft, de gemeente ook een ander persoon of orgaan mandaat kunnen geven.

gelet op afdeling 10.1.1. van de Algemene wet bestuursrecht;

besluit:

1. mandaat te verlenen, met de bevoegdheid tot het verlenen van ondermandaat, aan de wethouder van de gemeente Amersfoort die belast is met de uitvoering van beschermd wonen en opvang, voor de volgende bevoegdheden:

- de collegebevoegdheden in het kader van artikel 2.3.2, 2.3.3 en 2.3.4 van de Wet indien er sprake is van een behoefte aan beschermd wonen (o.a. het ontvangen van meldingen en het doen van onderzoek);
- de collegebevoegdheid tot het bepalen van de toegang tot een maatwerkvoorziening ten behoeve van beschermd wonen, waaronder begrepen het nemen van beslissingen tot (her)indicatie;
- de collegebevoegdheden in het kader van artikel 2.3.5 van de Wet ten aanzien van het beslissen op aanvragen om een maatwerkvoorziening ten behoeve van beschermd wonen;
- de collegebevoegdheden in het kader van 2.3.6 van de Wet ten aanzien van het beslissen op aanvragen om een maatwerkvoorziening ten behoeve van beschermd wonen;
- de collegebevoegdheden in het kader van 2.3.8 tot en met 2.4.4 van de Wet voor zover er sprake is van een beslissing inzake een maatwerkvoorziening of pgb ten behoeve van beschermd wonen;
- alle collegebevoegdheden in het kader van de verordening maatschappelijke ondersteuning voor zover het een maatwerkvoorziening beschermd wonen betreft;

Aldus vastgesteld in de vergadering van

Burgemeester en wethouders van de gemeente Woudenberg

de secretaris,

de burgemeester

De verwerkersovereenkomst

Verwerkersovereenkomst tussen het College van Burgemeester en Wethouders van de REGIOGEMEENTE Woudenberg verder te noemen de verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door de heer L. de Vos, verder aan te duiden als verwerkersverantwoordelijke en

met

Het College van Burgemeester en Wethouders van de gemeente Amersfoort verder te noemen de verwerker, hierbij rechtsgeldig vertegenwoordigd door de heer H.R. Kuipers, manager afdeling Samen Leven, verder aan te duiden als verwerker

In aanmerking nemende dat:

- partijen een overeenkomst hebben gesloten betreffende de Centrale Toegang voor Ondersteuning met Noodzakelijk verblijf (verder te noemen "hoofdovereenkomst");
- mede ter uitvoering van het bepaalde in artikel 28 lid 3 Algemene Verordening Gegevensbescherming (verder te noemen "AVG") wensen partijen in deze overeenkomst aanvullend een aantal voorwaarden ter zake van de aard van de werkzaamheden en de voorwaarden waaronder die zullen worden uitgevoerd vast te leggen. Deze zijn van toepassing op hun relatie in verband met de genoemde activiteiten in opdracht van en voor de verwerkingsverantwoordelijke;
- De verwerking van gegevens is noodzakelijk voor de uitvoering van de aan verwerker gemandateerde taken als Centrum gemeente op het gebied van ondersteuning met noodzakelijk verblijf op grond van de Wet maatschappelijke ondersteuning. Gestreefd wordt naar één regionaal uitvoeringsapparaat. De Verwerker voert de volgende verwerkersactiviteiten uit:
 - de collegebevoegdheden in het kader van artikel 2.3.2, 2.3.3 en 2.3.4 van de Wet indien er sprake is van een behoefte aan beschermd wonen (o.a. het ontvangen van meldingen en het doen van onderzoek);
 - de collegebevoegdheid tot het bepalen van de toegang tot een maatwerkvoorziening ten behoeve van beschermd wonen, waaronder begrepen het nemen van beslissingen tot (her)indicatie;
 - de collegebevoegdheden in het kader van artikel 2.3.5 van de Wet ten aanzien van het beslissen op aanvragen om een maatwerkvoorziening ten behoeve van beschermd wonen;
 - de collegebevoegdheden in het kader van 2.3.6 van de Wet ten aanzien van het beslissen op aanvragen om een maatwerkvoorziening ten behoeve van beschermd wonen;
 - de collegebevoegdheden in het kader van 2.3.8 tot en met 2.4.4 van de Wet voor zover er sprake is van een beslissing inzake een maatwerkvoorziening of pgb ten behoeve van beschermd wonen;
 - alle collegebevoegdheden in het kader van de verordening maatschappelijke ondersteuning voor zover het een maatwerkvoorziening beschermd wonen betreft;
- de regiogemeente Woudenberg in het kader van deze verwerkersovereenkomst (verder te noemen "overeenkomst") aan te merken is als verwerkingsverantwoordelijke voor de persoonsgegevens en verwerker aan te merken is als verwerker in de zin van artikel 4.7 en 4.8 van de AVG;
- waar in deze verwerkersovereenkomst termen worden gebruikt die overeenstemmen met definities uit artikel 4 van de AVG, wordt aan deze termen de betekenis van de definities uit de AVG toegekend.

Artikel 1 Definities

- 1.1 Bijlagen: aanhangsels bij deze verwerkersovereenkomst, die na door beide partijen te zijn geparafeerd, deel uitmaken van deze verwerkersovereenkomst.
- 1.2 Normen en standaarden: de door de verwerkingsverantwoordelijke vastgestelde normen en standaarden ter zake van methoden, technieken, procedures, projecten, productietekeningen en documentatievoorschriften welke bij de uitvoering van de werkzaamheden door de verwerker zullen worden gevolgd als vastgelegd in bijlage 1.

- 1.3 Toezichthouder: de Autoriteit Persoonsgegevens (AP) is het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens.
- 1.4 (Verwerkings)verantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
- 1.5 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, in opdracht van de verwerker, is, overeenkomstig artikel 28 AVG, een sub-verwerker.

Artikel 2 Ingangsdatum en duur

- 2.1 Deze verwerkersovereenkomst gaat in op 1 oktober en duurt voort zolang de verwerker als verwerker van persoonsgegevens optreedt in het kader van de door de verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens voor de doeleinden zoals omschreven in artikel 3 van Bijlage 2.

Artikel 3 Aard, doeleinden en onderwerp verwerkersovereenkomst

- 3.1 De verwerker verwerkt persoonsgegevens uitsluitend in opdracht van de verwerkingsverantwoordelijke voor de doeleinden zoals omschreven in artikel 3 van Bijlage 2.
- 3.2 De verwerker verwerkt de door of via de verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens uitsluitend in opdracht van de verwerkingsverantwoordelijke in het kader van de uitvoering van SAMENWERKINGSOVEREENKOMST ONDERSTEUNING MET NOODZAKELIJK VERBLIJF 2018 - 2022; dit is de onderliggende hoofdovereenkomst. De door de verwerker uit te voeren werkzaamheden waar deze verwerkersovereenkomst betrekking op heeft alsmede de soorten van persoonsgegevens en de doeleinden van de verwerkingen, worden nader, uitputtend, omschreven in Bijlage 2. De verwerker zal de persoonsgegevens niet voor enig ander doel verwerken, behoudens afwijkende wettelijke verplichtingen.
- 3.3 De verwerker verbindt zich om in het kader van die werkzaamheden de door of via de verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens rechtmatig, behoorlijk, zorgvuldig en op transparante wijze te verwerken.

Artikel 4 Verplichtingen verwerker

- 4.1 De verwerker verwerkt gegevens ten behoeve van de verwerkingsverantwoordelijke, in overeenstemming met diens schriftelijke instructies.
- 4.2 De verwerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens verstrekt onder deze verwerkersovereenkomst komt nimmer bij de verwerker te berusten. Indien een verwerker de doeleinden en middelen van een verwerking bepaalt, wordt die verwerker met betrekking tot die verwerking als verwerkingsverantwoordelijke beschouwd.
- 4.3 De verwerker zal bij de verwerking van persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden, handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de verwerking van persoonsgegevens. De verwerker zal alle redelijke instructies van de contactpersoon, als bedoeld in artikel 13.2, opvolgen, behoudens afwijkende wettelijke verplichtingen. Indien deze afwijkende wettelijke verplichtingen er zijn wordt de verantwoordelijke hiervan, voorafgaand aan de verwerking, schriftelijk op de hoogte gebracht door de verwerker.
- 4.4 De verwerker zal te allen tijde op eerste verzoek van de contactpersoon, als bedoeld in artikel 13.2, de door de verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens met betrekking tot deze verwerkersovereenkomst ter hand stellen.

- 4.5 De verwerker stelt de verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder de rechten van betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering, beperking en dataportabiliteit / overdraagbaarheid van persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet.
- 4.6 De verwerker zal de persoonsgegevens uitsluitend (laten) verwerken binnen de Europese Unie. Verwerking van persoonsgegevens buiten het grondgebied van de Europese Unie is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke en met inachtneming van de toepasselijke wet- en regelgeving.
- 4.7 De verwerker zal, rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verlenen bij het vervullen van diens verplichtingen uit hoofde van artikel 32 tot en met 36 AVG.

Artikel 5 Geheimhoudingsplicht

- 5.1 Personen in dienst van, dan wel werkzaam ten behoeve van de verwerker, evenals de verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht. De medewerkers van de verwerker tekenen hiertoe een geheimhoudingsverklaring.
- 5.2 Indien de verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal de verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal de verwerker de verwerkingsverantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren. Tenzij wettelijke bepalingen dit verbieden.

Artikel 6 Meldplicht datalekken en beveiligingsincidenten

- 6.1 De verwerker zal de verwerkingsverantwoordelijke zo spoedig mogelijk - doch uiterlijk binnen 4 uur na de eerste ontdekking - informeren over alle (vermoedelijke) inbreuken op de beveiliging alsmede andere incidenten die op grond van wetgeving moeten worden gemeld aan de toezichthouder of betrokkene, onverminderd de verplichting de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken.
- 6.2 Verwerker zal voorts, op het eerste verzoek van de verwerkingsverantwoordelijke, schriftelijk binnen 24 uur alle inlichtingen verschaffen die de verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft verwerker in ieder geval de informatie aan de verwerkingsverantwoordelijke zoals omschreven in bijlage 3.
- 6.3 De verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van inbreuken en zal de verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in het plan. Verwerker stelt de verwerkingsverantwoordelijke op de hoogte van materiele wijzigingen in het plan van aanpak.
- 6.4 De verwerker zal het doen van meldingen aan de toezichthouder(s) overlaten aan de verwerkingsverantwoordelijke.
- 6.5 De verwerker zal alle noodzakelijke medewerking verlenen aan het zo nodig, op de kortst mogelijke termijn, verschaffen van aanvullende informatie aan de toezichthouder(s) en/of betrokkene(n). Daarbij verschaft verwerker in ieder geval de informatie, zoals beschreven in bijlage 3, aan de verwerkingsverantwoordelijke.
- 6.6 De verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen waarin minimaal de informatie zoals bedoeld in bijlage 3 is opgenomen, en geeft daar op eerste verzoek van de verwerkingsverantwoordelijke inzage in.

Artikel 7 Beveiligingsmaatregelen

- 7.1 De verwerker neemt alle passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen en de persoonsgegevens welke worden verwerkt ten dienste van de verwerkingsverantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking. De wijze van beveiliging wordt nader omschreven in bijlage 4.
- 7.2 Voor "passende technische en organisatorische maatregelen" en "een passend beveiligingsniveau" handelt de verwerker minimaal conform het richtsnoer "Beveiliging van de persoonsgegevens" van de Autoriteit Persoonsgegevens en de Baseline Informatievoorziening Gemeenten (zie actuele versie hier: www.autoriteitpersoonsgegevens.nl en www.ibdgemeenten.nl).
- 7.3 De verwerker vrijwaart de verwerkingsverantwoordelijke tegen alle aanspraken van subverwerkers, dan wel derden hiermee verband houdende, voor zover veroorzaakt door het niet afdoende treffen door de verwerker van de maatregelen overeenkomstig het in de wet en deze overeenkomst bepaalde.
- 7.4 De door de verwerker te nemen maatregelen zijn er mede op gericht om onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.
- 7.5 Op voorwaarde dat de verwerkingsverantwoordelijke de verwerker hiervan schriftelijk in kennis heeft gesteld, hierbij een redelijke termijn hanterende, stelt de verwerker de verwerkingsverantwoordelijke in de gelegenheid om, op elk door de verwerkingsverantwoordelijke gewenst moment gedurende normale kantooruren en op elke door de verwerkingsverantwoordelijke aan te geven wijze, te controleren of de verwerking van de persoonsgegevens plaatsvindt op de wijze zoals overeengekomen in deze overeenkomst en de hoofdovereenkomst.

Artikel 8 Controle

- 8.1 De verwerkingsverantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens te (doen) controleren. De verwerker is verplicht (de Functionaris van de Gegevenbescherming van) de verwerkingsverantwoordelijke, de Autoriteit Persoonsgegevens, of, de onder geheimhouding, controlerende instantie in opdracht van verwerkingsverantwoordelijke toe te laten en verplicht medewerking te verlenen zodat de controle daadwerkelijk kan worden uitgevoerd. De met deze controle gemoeide kosten zijn voor rekening van de verwerkingsverantwoordelijke.
- 8.2 De verwerkingsverantwoordelijke zal de controle slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan de verwerker.
- 8.3 De verwerker verbindt zich om binnen een door de verwerkingsverantwoordelijke te bepalen termijn de verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie. Hierdoor kan de verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, zich een oordeel vormen over de naleving door de verwerker van deze verwerkersovereenkomst. De verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.
- 8.4 Verwerker staat er voor in, de door de verwerkingsverantwoordelijke of ingeschakelde derde, aangegeven aanbevelingen ter verbetering binnen de daartoe door de verwerkingsverantwoordelijke te bepalen redelijke termijn uit te voeren.
- 8.5 Jaarlijks dient verwerker door middel van een pen- en hacktest, uitgevoerd door een daarin gespecialiseerde derde, aan te tonen dat de applicatie en de infrastructuur waarmee persoonsgegevens worden bewerkt voldoen aan de relevante BIG-normen, en de in deze overeenkomst nader gespecificeerde criteria. De resultaten van deze test dienen te worden overgelegd aan verwerkingsverantwoordelijke. De kosten van de pen-

- en hacktest worden door verwerkingsverantwoordelijke gedragen. De kosten van de eventuele hertest worden door verwerker gedragen.
- 8.6 Naast de jaarlijkse test zal de verwerker eveneens zijn volledige medewerking verlenen aan extra pen- en hacktesten, indien de verwerkingsverantwoordelijke deze laat uitvoeren door een door hem geselecteerde partij, teneinde te bezien of de applicatie en de infrastructuur waarmee de persoonsgegevens worden bewerkt voldoen aan de relevante BIG-normen, en de in deze overeenkomst nader gespecificeerde criteria. De kosten van een pen- en hacktest en de eventuele hertest worden door de verwerkingsverantwoordelijke gedragen. De datum van uitvoering zal in onderling overleg tussen de verwerkingsverantwoordelijke en de verwerker worden bepaald.
- 8.7 De verwerker voert de uitkomsten van de pen- en hacktest en de naar aanleiding daarvan aangegeven aanbevelingen uit binnen de daartoe door de verwerkingsverantwoordelijke te bepalen termijn.
- 8.8 De verwerkingsverantwoordelijke behoudt zich het recht voor om de Informatiebeveiligingsdienst Gemeenten dan wel een andere derde in te schakelen voor ondersteuning en advisering met betrekking tot in het kader van audits en/of in pen- en hacktest aangetroffen bevindingen. De verwerker stemt hiermee in.

Artikel 9 Inschakeling derden

- 9.1 De verwerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande, duidelijk gespecificeerde, schriftelijke toestemming van de verwerkingsverantwoordelijke.
- 9.2 De verwerkingsverantwoordelijke kan aan de schriftelijke toestemming voorwaarden verbinden, op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze verwerkersovereenkomst.
- 9.3 De verwerker garandeert dat deze derden schriftelijk minimaal dezelfde plichten op zich nemen als tussen de verwerkingsverantwoordelijke en de verwerker zijn overeengekomen, waaronder de verplichtingen in verband met een vermoedelijke inbreuk op de beveiliging, en zal de verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in de overeenkomsten met deze derden waarin deze plichten zijn opgenomen.
- 9.4 Wanneer de ingeschakelde derde zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de verwerker - overeenkomstig artikel 28 lid 4 AVG - ten aanzien van de verwerkingsverantwoordelijke volledig aansprakelijk voor het nakomen van de verplichtingen van die ingeschakelde derde.
- 9.5 De verwerker vult na toestemming tot inschakeling van een of meerdere derde(n) Bijlage 2 in. De verwerker zorgt ervoor dat deze Bijlage actueel blijft.

Artikel 10 Wijziging, beëindiging verwerkersovereenkomst en einde opslag persoonsgegevens

- 10.1 Wijziging van deze verwerkersovereenkomst kan slechts schriftelijk plaatsvinden middels een door beide partijen geaccordeerd voorstel.
- 10.2 Zodra de samenwerking is beëindigd, zal de verwerker naar keuze van de verwerkingsverantwoordelijke (i) alle of een door verwerkingsverantwoordelijke bepaald gedeelte van haar in het kader van deze verwerkersovereenkomst ter beschikking gestelde persoonsgegevens aan de verwerkingsverantwoordelijke ter beschikking stellen (ii) de persoonsgegevens en kopieën daarvan die hij van de verwerkingsverantwoordelijke heeft ontvangen op alle locaties vernietigen, in welke vorm dan ook en toont dit aan, tenzij partijen iets anders overeenkomen. De verwerkingsverantwoordelijke kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen nader overeen te komen redelijke termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.

- 10.3 De verwerker zal te allen tijde het in het vorig lid beschreven recht op overdraagbaarheid van gegevens conform artikel 20 AVG waarborgen, zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.
- 10.4 De verwerkingsverantwoordelijke en de verwerker treden met elkaar in overleg over wijzigingen in deze verwerkersovereenkomst als een wijziging in regelgeving of een wijziging in de uitleg van regelgeving daartoe aanleiding geven.
- 10.5 Indien een partij tekortschiet in de nakoming van een overeengekomen verplichting, kan de andere partij haar in gebreke stellen waarbij de nalatige partij alsnog een redelijke termijn voor de nakoming wordt gegund. Blijft nakoming ook dan uit dan is de nalatige partij in verzuim. Ingebrekestelling is niet nodig wanneer voor de nakoming een fatale termijn geldt, nakoming blijvend onmogelijk is of indien uit een mededeling dan wel de houding van de andere partij moet worden afgeleid dat deze in de nakoming van haar verplichting zal tekortschieten.
- 10.6 De verwerkingsverantwoordelijke is gerechtigd, onverminderd hetgeen daartoe bepaald is in de verwerkersovereenkomst en de daarmee samenhangende hoofdovereenkomst, en onverminderd hetgeen overigens in de wet is bepaald, de uitvoering van deze verwerkersovereenkomst door middel van een aangetekend schrijven op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang geheel of gedeeltelijk te ontbinden, nadat verwerkingsverantwoordelijke constateert dat:
- a) de verwerker (voorlopige) surseance van betaling aanvraagt; of
 - b) de verwerker zijn faillissement aanvraagt of in staat van faillissement wordt verklaard; of
 - c) de onderneming van de verwerker wordt ontbonden; of
 - d) de verwerker zijn onderneming staakt; of
 - e) sprake is van een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming van de verwerker die maakt dat het in alle redelijkheid niet van de verwerkingsverantwoordelijke kan worden verwacht dat zij de verwerkersovereenkomst in stand houdt; of
 - f) op een aanmerkelijk deel van het vermogen van de verwerker beslag wordt gelegd (anders dan door de verwerkingsverantwoordelijke); of
 - g) de andere partij (op een andere wijze) aantoonbaar tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze verwerkersovereenkomst en die ernstige toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkende schriftelijke ingebrekestelling.
- 10.7 De verwerker informeert ogenblikkelijk de verwerkingsverantwoordelijke, indien een faillissement dreigt, dan wel surseance van betaling, zodat de verwerkingsverantwoordelijke tijdig kan beslissen de persoonsgegevens terug te vorderen alvorens een faillissement wordt uitgesproken.
- 10.8 De verwerkingsverantwoordelijke is gerechtigd deze verwerkersovereenkomst en de hoofdovereenkomst per direct te ontbinden indien de verwerker te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet en/of de rechtspraak aan de verwerking van de persoonsgegevens worden gesteld.
- 10.9 Indien de verwerkersovereenkomst voortijdig wordt beëindigd, is artikel 9 lid 2 en 3 van overeenkomstige toepassing.

Artikel 11 Aansprakelijkheid

- 11.1 De verwerker is op grond van het bepaalde in artikel 82 AVG aansprakelijk, voor schade of nadeel voortvloeiende uit het niet nakomen van deze verwerkersovereenkomst, daaronder begrepen wanneer bij de verwerking niet wordt voldaan aan de specifiek tot verwerker gerichte verplichtingen van de AVG, of buiten de rechtmatige instructies van verwerkingsverantwoordelijke is gehandeld.
- 11.2 De verwerker vrijwaart de verwerkingsverantwoordelijke voor schade of nadeel voor zover ontstaan door werkzaamheid van de verwerker, waaronder doorberekening van

bestuurlijke boetes van de Autoriteit Persoonsgegevens wegens het niet melden van een datalek .

- 11.3 Indien de verwerker de in artikel 6 van deze verwerkersovereenkomst neergelegde verplichtingen niet of niet-tijdig nakomt en de Autoriteit Persoonsgegevens, of een andere toezichthouder de verwerkingsverantwoordelijke dientengevolge een bestuurlijke boete oplegt, is de verwerker hiervoor aansprakelijk en zal de verwerkingsverantwoordelijke een contractuele boete ter hoogte van hetzelfde bedrag opleggen aan de verwerker. Deze boete is niet vatbaar voor verrekening en opschorting en laat de rechten van de verwerkingsverantwoordelijke op nakoming en schadevergoeding onverlet.

Artikel 12 Toepasselijk recht

- 12.1 Op deze verwerkersovereenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is het Nederlands recht van toepassing.

Artikel 13 Overige bepalingen

- 13.1 Deze verwerkersovereenkomst kan worden aangehaald als 'Verwerkersovereenkomst uitvoering Centrale Toegang ondersteuning met noodzakelijk verblijf'.
- 13.2 De Dienst / sector / cluster beleid & ontwikkeling van de gemeente Woudenberg treedt namens de verwerkingsverantwoordelijke op als contactpersoon.

Aldus in tweevoud opgesteld en getekend de dato

Namens de verwerkingsverantwoordelijke, mevrouw S.T.M. van der Marck, afdelingshoofd beleid & ontwikkeling van de gemeente Woudenberg,

Namens de verwerker de heer H.R. Kuipers, manager afdeling Samen Leven,

Bijlage 1: Beschrijving beveiliging ter uitwerking van artikel 1 lid 2

1. Normenstelsel (kies a of b)
 - a. De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk:
(vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS)
 - b. De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm zoals de BIG of de BIR of vergelijkbaar.
2. De toereikendheid van de informatiebeveiliging blijkt uit:
 - a. Certificering;
 - b. Periodieke externe controles zoals audits of TPM's (bijv. ISAE3xxx SOC type II);
 - c. Een Assurance rapport met conclusie over de bevindingen van de auditor;
 - d. Eigen controles of eigen mededelingen.
3. Uit de certificering of periodieke externe controles of uit de audits of uit de eigen controles blijkt of kan afgeleid worden dat de beveiliging voldoet aan of gelijkwaardig is met de toelichting (bijlage 4) en de daarin omschreven elementen.

LET OP: gemotiveerd afwijken is toegestaan!

Bijlage 2: Omschrijving werkzaamheden ter uitwerking van artikel 3 lid 1, artikel 3 lid 2 en artikel 9 lid 5

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

Naam verwerking	Verwerkings-doeleinden	Categorieën van Betrokkenen	(Bijzondere) Persoonsgegevens	Doorgifte naar derde landen
Uitvoering Centrale Toegang beschermd wonen	• Beoordelen of er sprake is van een behoefte aan opvang of beschermd wonen of opvang (o.a. het ontvangen van meldingen en het doen van onderzoek); • het bepalen van de toegang tot een maatwerkvoorziening ten behoeve van opvang en beschermd wonen, waaronder begrepen het nemen van beslissingen tot (her)indicatie; • het beslissen op aanvragen om een maatwerkvoorziening ten behoeve van opvang en beschermd wonen; • het beslissen inzake een maatwerkvoorziening of pgb ten behoeve van opvang en beschermd wonen; • uitvoeren van de verordening maatschappelijke ondersteuning voor zover het een maatwerkvoorziening beschermd wonen of opvang	Personen – ingezetenen van de gemeente <invullen> - met psychische of psychosociale problemen, die niet in staat zijn zich op eigen kracht te handhaven in de samenleving en die in aanmerking komen voor de Wmo-voorziening beschermd wonen	• NAW • BSN van betrokkene • mailadres • telefoonnummer • groepsnaam • geboortedatum • geheim adres • verblijf adres • postadres • Hulpvraag en beschrijving situatie • Gegevens van de huisgenoten, inwonende ouders, kinderen, echtgenoten • Gegevens betreffende de gezondheid van de client • Gegevens die zijn verzameld op grond van jeugdwet, participatiewet of Wgs alleen na ondubbelzinnige toestemming van de client	Nee

	betreft;			
--	----------	--	--	--

2. Contactgegevens

Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)	Naam: Contactgegevens:
Contactpersoon Verwerker (NB: Ook buiten kantooruren)	Naam: Contactgegevens:
Contactgegevens IBD	Telefoonnummer 070-373 8011

3. Ingeschakelde subverwerkers

Naam en contactgegevens subverwerker	Uitbestede verwerkingen
Stichting Sociale Wijkteams Amersfoort mevrouw T. van Altena, directeur-bestuurder Drentsestraat 14 3812 EH Amersfoort 033 – 469 48 69	Zie kolom Verwerkersdoeleinden in paragraaf 1 van deze bijlage.

NB: Eventuele wijzigingen in bovenstaande tabellen geven partijen op korte termijn aan elkaar door.

Bijlage 3: Inlichtingen om incidenten te beoordelen ter uitwerking van art. 6 lid 1, 2 en 5

De verwerker zal alle inlichtingen verschaffen die de verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft verwerker in ieder geval de volgende informatie aan de verwerkingsverantwoordelijke:

- wat de (vermeende) oorzaak is van de inbreuk;
- wat het (vooralsnog bekende en/of te verwachten) gevolg is;
- wat de (voorgestelde) oplossing is;
- contactgegevens voor de opvolging van de melding;
- aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
- een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
- het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
- de datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen de inbreuk heeft plaatsgevonden);
- de datum en het tijdstip waarop de inbreuk bekend is geworden bij verwerker of bij een door hem ingeschakelde derde of onderaannemer;
- of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
- wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.

Bijlage 4: Toelichting: Maatregelen op basis van de BIG ten aanzien van een verwerker

Deze bijlage is gevuld met een suggestie van gekozen maatregelen uit de BIG en kunnen ook worden uitgebreid of aangepast. Nadruk ligt op de integriteit en exclusiviteit van de gegevens, beschikbaarheidseisen horen bij voorkeur in een SLA¹ thuis.

Deze maatregelen zijn uit de BIG afkomstig en waar mogelijk specifiek gemaakt voor de verwerker. Deze maatregelen gaan uit van het niveau van de BIG. Als de gegevens van de verwerkingsverantwoordelijke hoger geclassificeerd zijn, een hogere risico inschatting hebben (bijzondere persoonsgegevens) of extra maatregelen nodig hebben uit specifieke wetgeving, dan dient deze bijlage te worden uitgebreid.

BIG Nummer	titel	Maatregel verwerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk
6.1.5.1	Geheimhoudin gsovereenkom st	Medewerkers die te maken hebben met persoonsinformatie van de verwerkingsverantwoordelijke dienen een geheimhoudingsverklaring te ondertekenen. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.	x	x		x	x	x
6.1.8.2	Onafhankelijke beoordeling van informatiebeve iliging	Periodieke beveiligingsaudits (minimaal eens per twee jaar) worden uitgevoerd volgens afspraken met de verwerkingsverantwoordelijke.	x	x		x	x	x
6.2.1.7	Identificatie van risico's die betrekking hebben op externe partijen	Over het naleven van de afspraken wordt jaarlijks gerapporteerd aan de verwerkingsverantwoordelijke.	x	x	x	x	x	x
6.2.3.1	Beveiliging behandelen in overeenkomst en met een derde partij	Maatregelen uit de verwerkersovereenkomst zijn geïmplementeerd.	x	x	x	x	x	x
7.2.2.1	Labeling en verwerking van informatie	De verwerker heeft maatregelen genomen zo dat niet geautoriseerden geen kennis kunnen nemen van persoonsgegevens.	x			x	x	x

¹ Zie ook het operationele baseline product 'Handreiking Service Level Agreements' van de IBD.

BIG Nummer	titel	Maatregel verwerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk
8.1.1.2	Rollen en verantwoordelijkheden	Het personeel van de verwerker of derden moeten kennis hebben van de verantwoordelijkheden ten aanzien van de bewerking van de persoonsgegevens voor de verwerkingsverantwoordelijke.	x			x	x	x
8.1.2.1	Screening	Voor personen is een recente Verklaring Omtrent het Gedrag (VOG) vereist met punten die door de verwerkingsverantwoordelijke zijn aangedragen. Tenzij dit centraal in het contract geregeld is.	x			x	x	x
8.3.3.1	Blokking van toegangsrecht en	Toegangsrechten van medewerkers van de verwerker worden direct geblokkeerd als geen toegang voor de bewerking van de persoonsgegevens noodzakelijk is.	x			x	x	x
9.1.2.1	Fysieke toegangsbeveiliging	Toegang tot beveiligde zones of gebouwen waar persoonsgegevens van de verwerkingsverantwoordelijke zich bevinden is alleen mogelijk na autorisatie daartoe.	x	x	x	x	x	x
9.1.3.1	Beveiliging van kantoren, ruimten en faciliteiten	Papieren documenten en mobiele gegevensdragers die persoonsgegevens of andere vertrouwelijke gegevens van de verwerkingsverantwoordelijke bevatten worden beveiligd opgeslagen.	x			x	x	x
10.3.1.1	Capaciteitsbeheer	De ICT-voorzieningen voldoen aan het voor de dienst overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheidseis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van	x	x	x	x	x	x

BIG Nummer	titel	Maatregel verwerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch / database beheer	Helpdesk
		(fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen.						
10.6.1.2	Maatregelen voor netwerken	Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.	x	x			x	x
10.6.1.3	Maatregelen voor netwerken	Bij transport van vertrouwelijke informatie over niet vertrouwde netwerken tussen de verwerker en de verwerkingsverantwoordelijke, zoals over het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe 12.3.1.3.	x	x			x	x
10.6.2.1	Beveiliging van netwerkdiensten	Beveiligingskenmerken, niveaus van dienstverlening en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten door een verwerker.	x				x	x
10.8.2.2	Uitwisselingsovereenkomsten	Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, evenals procedures over melding van incidenten van de verwerker naar de verwerkingsverantwoordelijke.	x			x	x	x
10.8.3.1	Fysieke media die worden getransporteerd	De verwerker neemt maatregelen om vertrouwelijke informatie te beschermen, zoals: • Versleuteling. • Bescherming door fysieke maatregelen, zoals afgesloten containers. • Gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen • Persoonlijke aflevering. • Opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes.	x					
10.10.1.1	Aanmaken auditlogbestanden	Door de verwerker worden rapportages van logbestanden gemaakt die periodiek worden beoordeeld. Deze periode dient te worden gerelateerd aan de mogelijkheid van misbruik en de schade die kan optreden.	x	x		x	x	

BIG Nummer	titel	Maatregel verwerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk
10.10.1.2	Aanmaken auditlogbestanden	Een logregel bevat minimaal: • Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID. • De gebeurtenis (zie 10.10.2.1). • Waar mogelijk de identiteit van het werkstation of de locatie. • Het object waarop de handeling werd uitgevoerd. • Het resultaat van de handeling. • De datum en het tijdstip van de gebeurtenis.	x			x	x	
10.10.1.3	Aanmaken auditlogbestanden	In een logregel wordt in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, et cetera).	x			x	x	
10.10.2.1	Controle van systeemgebruik	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: • Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling: uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore. • Gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases). • Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels. • Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services). • Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of	x	x		x	x	

BIG Nummer	titel	Maatregel verwerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch / database beheer	Helpdesk
		systemen). • Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders.						
10.10.3.3	Bescherming van informatie in logstanden	Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.	x	x		x	x	
10.10.3.5	Bescherming van informatie in logstanden	De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de verwerkingsverantwoordelijke. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.	x	x				
10.10.6.1	Synchronisatie van systeemklokken	Er worden maatregelen genomen om er voor te zorgen dat de logbestanden die verzameld worden aan elkaar te relateren zijn, op basis van het tijdstip waarin ze zijn opgetreden.	x	x	x	x	x	
11.4.2.1	Authenticatie van gebruikers bij externe verbindingen.	Als externe toegang nodig is tot de persoonsgegevens van de verwerkingsverantwoordelijke door eigen personeel, of personeel van de verwerker, dienen geschikte authenticatie methodes te worden gebruikt.	x			x	x	x
11.4.5.5	Scheiding van netwerken	Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).	x			x	x	x
11.5.1.1	Beveiligde inlogprocedures	Toegang tot de persoonsgegevens van de verwerkingsverantwoordelijke wordt verleend op basis van twee-factor authenticatie.				x	x	x

BIG Nummer	titel	Maatregel verwerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk
11.5.1.2	Beveiligde inlogprocedures	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.	x			x	x	x
11.5.1.3	Beveiligde inlogprocedures	Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.	x			x	x	x
11.5.1.4	Beveiligde inlogprocedures	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.	x			x	x	x
11.5.1.5	Beveiligde inlogprocedures	Nadat voor een gebruikersnaam 3 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lock-out op te heffen of het wachtwoord te resetten.	x			x	x	x
11.5.2.1	Gebruikersidentificatie en -authenticatie	Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld, evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.	x			x	x	x
11.5.3.1	Systemen voor wachtwoordbeheer	Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).	x			x	x	x
11.5.5.1	Time-out van sessies	De periode van inactiviteit van een workstation is vastgesteld op maximaal 15 minuten. Daarna wordt de PC vergrendeld. Bij remote desktop sessies geldt dat na maximaal 15 minuten inactiviteit de sessie verbroken wordt.	x			x	x	x
11.5.6.1	Beperking van verbindingstijd	De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis van een wijzigingsverzoek of storingsmelding, met 2-factor authenticatie en tunneling.	x			x	x	x

BIG Nummer	titel	Maatregel verwerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk
11.6.1.1	Beperking van toegang tot informatie	In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.	x			x	x	x
11.6.1.2	Beperking van toegang tot informatie	Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.	x			x	x	x
11.6.1.3	Beperking van toegang tot informatie	Bij extern gebruik vanuit een niet vertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.	x			x	x	x
12.1.1.1	Analyse en specificatie van beveiligingseisen	In projecten ten behoeve van systemen voor de verwerkingsverantwoordelijke wordt een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.	x			x	x	
12.2.1.1	Validatie van invoergegevens	Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, toevoegen van parameters (SQL-Injectie) en inconsistentie van gegevens.	x			x	x	
12.2.2.1	Beheersing van interne gegevensverwerking	Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.	x			x	x	
12.2.3.1	Integriteit van berichten	Er behoren eisen en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.	x	x		x	x	x
12.2.4.1	Validatie van uitvoergegevens	De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijvoorbeeld door check-sums).	x			x	x	x
12.3.1.1	Beleid voor het gebruik van cryptografische beheersmaatregelen	De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.	x	x		x	x	x

BIG Nummer	titel	Maatregel verwerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk
12.3.2.1	Sleutelbeheer	In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.	x	x		X	X	x
12.4.1.1	Beheersing van operationele software	Alleen geautoriseerd personeel kan functies en software installeren of activeren.	x	x		X	X	x
12.5.1.1	Procedures voor wijzigingsbeheer	Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices, zoals ITIL en voor applicaties ASL.	x	x		x	X	x
12.5.2.1	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem	Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen en de beveiliging zoals afgesproken met de verwerkingsverantwoordelijke te niet doen.	x	x		x	x	x
12.5.4.1	Uitlekken van informatie	Op het grensvlak van een vertrouwde en een niet vertrouwde omgeving vindt content-scanning plaats.	x	x	x	X	x	x
12.5.4.2	Uitlekken van informatie	Er dient een proces te zijn om aan de verwerkingsverantwoordelijke te melden dat (persoons) informatie is uitgelekt. (zie 13.1.1)	x	x	x	X	X	x
12.6.1.1	Beheersing van technische kwetsbaarheden	Er is een proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat minimaal het melden van incidenten aan de verwerkingsverantwoordelijke, het uitvoeren van periodieke penetratietests, het uitvoeren van risicoanalyses van kwetsbaarheden en patching van systemen en hardware.	x	x	x	x	X	x
13.1.1.1	Rapportage van informatiebeveiligingsgebeurtenissen	Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen aan de verwerkingsverantwoordelijke vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.	x	x	x	X	X	x
13.1.1.4	Rapportage van informatiebeveiligingsgebeurtenissen	Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan de verwerkingsverantwoordelijke.	x	x	x	X	X	x

BIG Nummer	titel	Maatregel verwerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk
	enissen							
13.1.1.5	Rapportage van informatiebeveiligingsgebeurtenissen	Vermissing of diefstal van apparatuur of media die gegevens van de verwerkingsverantwoordelijke kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.	x	x	x	X	X	x
13.2.3.1	Verzamelen van bewijsmateriaal	Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd in overeenstemming met de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.	x	x	x	x	x	x
15.1.3.1	Bescherming van bedrijfsdocumenten	De registraties van de verwerkingsverantwoordelijke behoren te worden beschermd tegen verlies, vernietiging en vervalsing, in overeenstemming met wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.	x			x	x	
15.1.4.1	Bescherming van gegevens en geheimhouding van persoonsgegevens	De bescherming van gegevens en privacy behoort te worden bewerkstelligd in overeenstemming met relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.	x			X	x	
15.1.6.1	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen. Zie ook 12.3.	x			x	x	
15.2.1.1	Naleving van beveiligingsbeleid en -normen	De verwerker is verantwoordelijk voor uitvoering en beveiligingsprocedures en toetsing daarop (onder andere de jaarlijkse in control verklaring). Conform deze verwerkersovereenkomst en andere contractuele eisen zorgt de verwerker voor het toezicht op de uitvoering van het beveiligingsbeleid ten behoeve van de gegevens van de verwerkingsverantwoordelijke. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door, of vanwege	x	x		X	x	x

BIG Nummer	titel	Maatregel verwerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk
		de verwerkingsverantwoordelijke.						
15.2.2.1	Controle op technische naleving	Informatiesystemen van de verwerker ten behoeve van de verwerkingsverantwoordelijke worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijvoorbeeld kwetsbaarheidsanalyses en penetratietesten.	x	x		x	x	x