

Verwerkersovereenkomst AVG
behorend bij hoofdovereenkomst Dienstverlening
Minicontainers

kenmerk 2020-SB-010

Interne Bedrijven Concerninkoop

Postadres Postbus 10080, 3505 AB Utrecht

Bezoekadres Stadsplateau 1, 3521 AZ Utrecht

E-mail: concerninkoop@utrecht.nl

Partijen:

1. De gemeente Utrecht, te dezen rechtsgeldig vertegenwoordigd door <.....> in <zijn/haar> hoedanigheid van <.....>, hierna te noemen: 'Verantwoordelijke',

en

2. <.....>, statutair gevestigd te <.....>, te dezen rechtsgeldig vertegenwoordigd door <.....>, in <zijn/haar> hoedanigheid van <.....>, hierna te noemen: 'Verwerker',

overwegen dat:

- I deze overeenkomst onderdeel uitmaakt van de Raamovereenkomst Dienstverlening Minicontainers Gemeente Utrecht met kenmerk 2020-SB-010 (hierna: de Hoofdovereenkomst);
- II Verantwoordelijke '(verwerkings)verantwoordelijke' is en Verwerker 'verwerker' zoals bedoeld in de Algemene Verordening Gegevensbescherming (hierna: AVG);
- III Verwerker persoonsgegevens verwerkt in opdracht van Verantwoordelijke in het kader van de uitvoering van de Hoofdovereenkomst met als leveren van dienstverlening Minicontainers.
- IV deze verwerking persoonsgegevens en handelingen betreft zoals aangegeven in **bijlage X**. Hiervoor maakt Verwerker gebruik van <invullen bij gunning> [middelen/systeem /applicatie benoemen];
- V de AVG de Verantwoordelijke de plicht oplegt om ervoor te zorgen dat de Verwerker voldoende waarborgen biedt ten aanzien van:
 - technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen van persoonsgegevens, en
 - melding van een beveiligingsinbreuk dan wel datalek, welke leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die Verwerker verwerkt;
- VI de AVG de Verantwoordelijke verplicht om hiervoor een overeenkomst te sluiten met de Verwerker;
- VII namens Verantwoordelijke <naam en contactgegevens> optreedt als contactpersoon en namens Verwerker <naam en contactgegevens>.

en spreken het volgende af:

1. Definities

- 1.1 In deze Verwerkersovereenkomst gelden de definities uit artikel 4 AVG.
- 1.2 Indien in deze Verwerkersovereenkomst wordt gesproken van de Raamovereenkomst, wordt hiermee verwezen naar de Raamovereenkomst en (eventuele) nadere overeenkomsten.

2. Reikwijdte en duur

- 2.1. Deze Verwerkersovereenkomst gaat in op het moment van ondertekening en de looptijd is gelijk aan de duur van de Raamovereenkomst. Dit is slechts anders als partijen iets anders overeenkomen of als Verwerker ook na beëindiging van de Raamovereenkomst nog optreedt als Verwerker van persoonsgegevens, zoals bedoeld in overweging III. In dat laatste geval blijft deze Verwerkingsovereenkomst gelden zolang de Verwerker deze werkzaamheden verricht.
- 2.2. Verplichtingen welke naar hun aard bedoeld zijn om ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van de Verwerkersovereenkomst gelden. Dit ziet in ieder geval op de bepalingen betreffende geheimhouding, aansprakelijkheid en het toepasselijk recht.

3. Onderwerp van deze Verwerkersovereenkomst

- 3.1. De Verwerker verwerkt de door of via Verantwoordelijke ter beschikking gestelde persoonsgegevens uitsluitend in opdracht van de Verantwoordelijke in het kader van de uitvoering van de Raamovereenkomst. De door of namens de Verwerker uit te voeren werkzaamheden waar deze Verwerkersovereenkomst betrekking op heeft worden omschreven in **bijlage 2**. Verwerker zal de persoonsgegevens niet voor enig ander doel dan daar genoemd verwerken, behoudens afwijkende wettelijke verplichtingen.
- 3.2. De Verwerker verbindt zich om in het kader van die werkzaamheden de door of via de Verantwoordelijke ter beschikking gestelde persoonsgegevens zorgvuldig te verwerken.

4. Verplichtingen Verwerker

- 4.1. Verwerker voldoet aan het in **bijlage 1** genoemde normenkader.
- 4.2. De Verwerker neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens welke worden verwerkt ten dienste van de Verantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onzorgvuldig, ondeskundig of ongeoorloofd gebruik, in ieder geval door inachtneming van de maatregelen zoals aangegeven in **bijlage 1**. De te nemen maatregelen zullen steeds, met inachtneming van de stand der techniek en de kosten gemoeid met de implementatie en de uitvoering van de maatregelen, een passend beschermingsniveau verzekeren, met inachtneming van de risico's die het verwerken van de persoonsgegevens en de aard daarvan meebrengen.
- 4.3. De Verwerker verwerkt gegevens ten behoeve van de Verantwoordelijke, in overeenstemming met diens schriftelijke instructies.
- 4.4. De Verwerker heeft geen zeggenschap over de door de Verantwoordelijke ter beschikking gestelde persoonsgegevens. Zo neemt Verwerker 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 komt nooit bij de Verwerker te berusten.

- 4.5 De Verwerker verwerkt de persoonsgegevens zorgvuldig en in overeenstemming met de toepasselijke wet- en regelgeving betreffende de bescherming van persoonsgegevens, voor zover noodzakelijk ter uitvoering van zijn verplichtingen uit de Hoofdovereenkomst en deze Verwerkersovereenkomst. De Verwerker verwerkt persoonsgegevens slechts in opdracht en volgens instructies van de Verantwoordelijke en zal alle redelijke instructies van de Verantwoordelijke dienaangaande 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.
- 4.6 Verwerker stelt de persoonsgegevens uitsluitend beschikbaar aan die personen in dienst van, dan wel werkzaam ten behoeve van Verwerker, die noodzakelijkerwijs van de persoonsgegevens kennis dienen te nemen.
- 4.7 Verwerker draagt er zorg voor dat personen in dienst van, dan wel werkzaam ten behoeve van Verwerker zich houden aan de in deze Verwerkersovereenkomst en de daarbij behorende bijlagen vastgelegde verplichtingen.
- 4.8 De Verwerker stelt altijd op eerste verzoek van de contactpersoon van Verantwoordelijke alle van de Verantwoordelijke afkomstige persoonsgegevens met betrekking tot de Hoofdovereenkomst ter hand.
- 4.9 De Verwerker vernietigt op schriftelijk verzoek van Verantwoordelijke alle van de Verantwoordelijke met betrekking tot de Raamovereenkomst verkregen persoonsgegevens, in welke vorm dan ook, op een nader te bepalen wijze **<invullen bij gunning> [omschrijf dit zo concreet mogelijk]**. Deze vernietiging moet binnen een nader overeen te komen termijn uitgevoerd worden en hiervan maakt Verwerker een verslag, waarin wordt aangetoond wordt dat de persoonsgegevens daadwerkelijk vernietigd zijn.¹
- 4.10 De Verwerker stelt de Verantwoordelijke altijd in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder de rechten van degene op wie een persoonsgegeven betrekking heeft, zoals maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet.
- 4.11 De Verwerker werkt op verzoek van Verantwoordelijke mee aan een gegevensbeschermingseffectbeoordeling (DPIA).

5. Inschakeling derden en plaats van verwerking

- 5.1 Verwerker mag de uitvoering van de werkzaamheden slechts geheel of ten dele uitbesteden aan derden na voorafgaande, duidelijk gespecificeerde, schriftelijke toestemming van de Verantwoordelijke.
- 5.2 Verantwoordelijke kan aan de schriftelijke toestemming voorwaarden verbinden op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze Verwerkersovereenkomst.

¹ *Indien sprake is van gevoelige persoonsgegevens, kunnen we om een auditrapport verzoeken. Dit is ter inschatting van de DISO.*

- 5.3 Verwerker garandeert dat deze derden minimaal dezelfde plichten op zich nemen als tussen de Verantwoordelijke en de Verwerker zijn overeengekomen en zal de Verantwoordelijke op diens verzoek inzage verschaffen in de overeenkomsten met deze derden waarin deze plichten zijn opgenomen.
- 5.4 Verwerker blijft in deze gevallen altijd aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze Verwerkersovereenkomst.
- 5.5 Verwerker houdt een register bij van de door hem ingeschakelde derden en onderaannemers waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de derden of onderaannemers zijn opgenomen, alsmede eventuele door de Verantwoordelijke gestelde aanvullende voorwaarden. Dit register is als **bijlage 3** aan deze Verwerkersovereenkomst toegevoegd en wordt steeds door Verwerker actueel gehouden.
- 5.6 Verwerker mag de persoonsgegevens uitsluitend verwerken in de Europese Unie. Doorgifte naar landen buiten de Europese Unie is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van de Verantwoordelijke en met inachtneming van de toepasselijke wet- en regelgeving.

6. Beveiligingsincidenten en datalekken

- 6.1 Als Verwerker een (vermoedelijke) beveiligingsinbreuk, datalek of ander beveiligingsincident ontdekt, neemt hij onmiddellijk maatregelen om nadelige gevolgen van de beveiligingsinbreuk of het datalek zoveel mogelijk te voorkomen en/of te herstellen.
- 6.2 De Verwerker meldt (vermoedelijke) beveiligingsinbreuken, datalekken of andere beveiligingsincidenten betreffende de persoonsgegevens waarop deze overeenkomst ziet, onmiddellijk doch uiterlijk binnen 24 uur na eerste ontdekking, aan de Verantwoordelijke. Verwerker geeft daarbij direct aan wat de aard van de inbreuk of lek is, welke maatregelen hij heeft getroffen, zal treffen en voorstelt te treffen om de gevolgen van de inbreuk of lek te verhelpen of zoveel mogelijk te beperken. <OPTIE: Als Verwerker niet voldoet aan deze verplichting, verbeurt hij een direct opeisbare boete aan Verantwoordelijke ter hoogte van <...>²
- 6.3 De melding zoals bedoeld in artikel 6.2 vindt plaats via de procedure voor het melden van datalekken zoals omschreven op www.utrecht.nl/privacy.
- 6.4 Verwerker zal verder op het eerste verzoek van de Verantwoordelijke alle (aanvullende) inlichtingen verschaffen die de Verantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft Verwerker in ieder geval de volgende informatie aan de Verantwoordelijke:
- wat de (vermeende) oorzaak is van de inbreuk;
 - wat het (vooralsnog bekende en/of te verwachten) gevolg is;

² *Het al dan niet opnemen van een boete kan onderdeel zijn van onderhandelingen. Of een boetebeding aan te bevelen is, hangt van het risico dat samenhangt met beveiligingsincidenten in dit specifieke geval. Relevante omstandigheden hierbij zijn bijvoorbeeld of bijzondere persoonsgegevens worden verwerkt.*

- c. wat de (voorgestelde) oplossing is;
 - d. contactgegevens voor de opvolging van de melding;
 - e. 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);
 - f. een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
 - g. het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
 - h. de datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen de inbreuk heeft plaatsgevonden);
 - i. de datum en het tijdstip waarop de inbreuk bekend is geworden bij Verwerker of bij een door hem ingeschakelde derde of onderaannemer;
 - j. of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
 - k. wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.
- 6.5 De Verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van inbreuken en zal de Verantwoordelijke, op diens verzoek, inzage verschaffen in het plan. Verwerker stelt de Verantwoordelijke op de hoogte van materiele wijzigingen in het plan van aanpak.
- 6.6 De Verwerker zal het doen van meldingen aan de toezichthouder(s) overlaten aan de Verantwoordelijke, voor zover deze zien op de verwerking waarop deze overeenkomst ziet.
- 6.7 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 artikel 6.4 is opgenomen, en geeft daar op eerste verzoek van de Verantwoordelijke inzage in.
- 6.8 Verwerker zal aan Verantwoordelijke waar mogelijk medewerking verlenen bij het opstellen van een beschrijving van de geconstateerde beveiligingsinbreuken en datalekken en de vermoedelijke gevolgen daarvan voor de verwerking van persoonsgegevens ten behoeve van de meldplicht van Verantwoordelijke.

7. Geheimhoudingsplicht

- 7.1 Verwerker, personen in dienst van, dan wel werkzaam ten behoeve van de Verwerker zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, voor zover de wet niet anders bepaalt. De medewerkers van de Verwerker tekenen hiertoe een geheimhoudingsverklaring.
- 7.2 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 Verantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren voor zover dit wettelijk is toegestaan.

8. Verantwoording en controle

- 8.1 Verantwoording over het voldoen aan het geldende normenkader vindt plaats op de in **bijlage 1** omschreven wijze.
- 8.2 De Verantwoordelijke mag daarnaast altijd de verwerking van persoonsgegevens en nakoming van deze overeenkomst (laten) controleren. De Verwerker is verplicht de Verantwoordelijke of controlerende instantie in opdracht van Verantwoordelijke toe te laten en is verplicht medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden. De Verantwoordelijke, of de door de Verantwoordelijke ingeschakelde derde, dient alle informatie betreffende deze controles vertrouwelijk behandelen.
- 8.3 De Verantwoordelijke zal de in artikel 8.2 genoemde controle slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan de Verwerker.
- 8.4 De Verwerker verbindt zich om binnen een door de Verantwoordelijke te bepalen termijn de Verantwoordelijke, of de door de Verantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie ter uitvoering van de controle. Hierdoor kan deze zich een oordeel vormen over de naleving door de Verwerker van deze Verwerkersovereenkomst. De Verantwoordelijke of de door hem ingeschakelde derde dient alle informatie betreffende deze controles vertrouwelijk te behandelen.
- 8.5 Uit de in artikel 8.2 genoemde controle kan blijken dat Verwerker in strijd met deze overeenkomst handelt of in strijd met de AVG persoonsgegevens namens Verantwoordelijke verwerkt. Als dat het geval is, voert Verwerker de door Verantwoordelijke of door deze ingeschakelde derde aangegeven aanbevelingen om deze gebreken te verhelpen uit, binnen de daartoe door de Verantwoordelijke te bepalen redelijke termijn.
- 8.6 De redelijke kosten van de controle worden gedragen door de partij die de kosten maakt, tenzij uit de controle blijkt dat de Verwerker enig punt uit deze Verwerkersovereenkomst niet heeft nageleefd. In dat geval worden de kosten van de controle gedragen door de Verwerker.

9. Wijziging overeenkomst

- 9.1 Wijziging van deze overeenkomst kan slechts schriftelijk plaatsvinden middels een door beide partijen geaccordeerd voorstel.
- 9.2 Verantwoordelijke en 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. Aansprakelijkheid en boetes

- 10.1 Verwerker is aansprakelijk op grond van het bepaalde in artikel 82 AVG voor schade of nadeel die voortvloeit uit het door Verwerker niet nakomen van deze Verwerkersovereenkomst. Hieronder valt in ieder geval het niet voldoen aan de specifiek aan Verwerker opgelegde verplichtingen in de AVG, alsmede niet conform rechtmatige instructies van Verantwoordelijke handelen.³

³ *[OPTIE: Deze aansprakelijkheid geldt tot een maximumbedrag van €[]]*

10.2 Verwerker vrijwaart Verantwoordelijke voor schade of nadeel voor zover ontstaan door werkzaamheden van de Verwerker, voortvloeiend uit de verwerking waarop deze overeenkomst ziet.

10.3 Indien Verwerker de in artikel 6 van deze Verwerkersovereenkomst neergelegde verplichtingen niet of niet tijdig nakomt en de toezichthouder de Verantwoordelijke hierdoor een bestuurlijke boete oplegt, zal Verantwoordelijke een contractuele boete ter hoogte van hetzelfde bedrag opleggen aan Verwerker. Deze boete is niet vatbaar voor verrekening en opschorting en laat de rechten van Verantwoordelijke op nakoming en schadevergoeding onverlet.

11. Beëindiging

11.1 Op het moment dat de samenwerking eindigt, zal de Verwerker naar keuze van de Verantwoordelijke:⁴

(i) <invullen bij gunning> <alle of een door Verantwoordelijke bepaald gedeelte van haar in het kader van deze Verwerkersovereenkomst ter beschikking gestelde persoonsgegevens aan de Verantwoordelijke ter beschikking stellen>, en/of

(ii) <invullen bij gunning> <de persoonsgegevens die hij van de Verantwoordelijke heeft ontvangen op alle locaties vernietigen, in welke vorm dan ook en toont dit aan met een verklaring, tenzij partijen iets anders overeenkomen.>

11.2 De Verantwoordelijke kan nadere eisen stellen aan de wijze van beschikbaarstelling of vernietiging van de gegevens, waaronder eisen aan het bestandsformaat. Aan deze eisen moet, binnen een nader overeen te komen redelijke termijn, tegemoet gekomen worden en hiervan wordt een verslag gemaakt.

11.3 De Verwerker waarborgt bij teruglevering van gegevens aan Verantwoordelijke altijd het behoud van functionaliteit of (delen van) de gegevens.

11.4 De Verantwoordelijke mag, onverminderd hetgeen daartoe bepaald is in de Verwerkersovereenkomst en de daarmee samenhangende raamovereenkomst, en onverminderd hetgeen overigens in de wet is bepaald, de uitvoering van deze Verwerkersovereenkomst door middel van een aangetekend schrijven opschorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang geheel of gedeeltelijk te ontbinden, als Verantwoordelijke constateert dat:

a) Verwerker (voorlopige) surseance van betaling aanvraagt, of

b) Verwerker zijn faillissement aanvraagt of in staat van faillissement wordt verklaard, of

In verband met de verzekeraarbaarheid van Verwerker kan het nodig zijn de aansprakelijkheid te maximeren. Alleen als dit het geval is, kan maximering onderwerp zijn van onderhandeling. Uitgangspunt is dan dat de aansprakelijkheid wordt gemaximeerd tot het maximale bedrag dat de AP de Verantwoordelijke aan boete kan opleggen, namelijk €20.000.000,-. De aanneemsom of het maximaal verzekerde bedrag van Verwerker zijn geen goede indicatie voor de maximering van de aansprakelijkheid. Overleg eventueel met je DISO of jurist.

⁴ *Wat te doen met persoonsgegevens bij beëindiging is altijd maatwerk. Dit zijn dus slechts voorbeelden. Als de gemeente zelf bij beëindiging geen gegevens meer heeft, levert de wederpartij altijd de gegevens terug.*

- c) de onderneming van Verwerker wordt ontbonden, of
 - d) Verwerker zijn onderneming staakt, of
 - e) er sprake is van een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming van Verwerker die maakt dat het in alle redelijkheid niet van de Verantwoordelijke kan worden verwacht dat zij de Verwerkersovereenkomst in stand houdt, of
 - f) op een aanmerkelijk deel van het vermogen van Verwerker beslag wordt gelegd (anders dan door verantwoordelijke), of
 - g) andere partij(en) 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.
- 11.5 Verwerker informeert Verantwoordelijke direct als een faillissement dan wel surseance van betaling bij Verwerker dreigt, zodat de Verantwoordelijke tijdig de persoonsgegevens terug kan eisen.
- 11.6 Verantwoordelijke mag deze Verwerkersovereenkomst en de raamovereenkomst per direct ontbinden indien 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.
- 11.7 Indien de Verwerkersovereenkomst voortijdig wordt beëindigd zijn de artikelen 11 leden 1 tot en met 3 van overeenkomstige toepassing.
- 11.8 Verwerker bewaart de persoonsgegevens niet langer dan [geef bewaartermijn per persoonsgegeven aan].⁵ Hierna worden de gegevens vernietigd door [aangeven hoe vernietigd wordt]. Gegevens worden nooit langer bewaard dan strikt noodzakelijk voor de verwerkingsdoeleinden.

12. Toepasselijk recht en geschilbeslechting

- 12.1 Op deze overeenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is het Nederlands recht van toepassing.
- 12.2 Partijen zullen, indien sprake is van een geschil, trachten dit geschil bij te leggen door middel van (bestuurlijk) overleg, vóórdat zij zich wenden tot de rechter, spoedeisende gevallen daargelaten. Geschillen zullen in eerste aanleg met uitsluiting worden voorgelegd aan de rechtbank te Utrecht.

Aldus overeengekomen en in tweevoud opgesteld en ondertekend,

⁵ *Per persoonsgegeven afspreken welke bewaartermijn hiervoor geldt, als deze termijn niet voor alle persoonsgegevens gelijk is. De bewaartermijn mag nooit langer zijn dan nodig is voor de verwerkingsdoeleinden. De bewaartermijn moet daadwerkelijk worden nageleefd, dus de techniek of de werkwijze moet hierop aantoonbaar worden ingericht. Als de gemeente zelf de gegevens niet (meer) heeft, spreek dan eventueel af of de Verwerker voor vernietiging de gegevens moet (terug)leveren.*

Plaats:

Datum:

<Verantwoordelijke>,

<naam tekeningsbevoegde>

Handtekening:

Plaats:

Datum:

<Verwerker>,

<naam tekeningsbevoegde>

Handtekening:

Bijlage 1: Normenkader en verantwoordingswijze, ter uitwerking van artikel 4 lid 1 en artikel 8 lid 1

1. Vastgesteld Risicoprofiel

Partijen stellen het Risicoprofiel van de aan Verwerker toevertrouwde verwerking vast op [laag/midden/hoog].⁶

2. Geldende normenstelsel⁷

Op basis van het hiervoor genoemde vastgestelde risicoprofiel vindt de informatiebeveiliging plaats conform het hieronder geselecteerde normenkader:

Risicoprofiel verwerking	Van toepassing verklaard normenkader
Laag	Baseline informatiebeveiliging Gemeentes (BIG) of passende technische en organisatorische maatregelen, zoals bijvoorbeeld blijkend uit een uitgevoerde DPIA, te weten: - <invullen bij gunning> [OPTIE: neem hier de specifieke maatregelen op]
Midden	Baseline informatiebeveiliging Gemeentes (BIG) of gelijkwaardig + Eventuele specifieke maatregelen voortvloeiend uit een uitgevoerde DPIA
Hoog	Baseline informatiebeveiliging Gemeentes (BIG) of gelijkwaardig + Eigen risico analyse van de verwerker van de verwerking met aanvullende maatregelen indien deze nodig zijn op basis van de risicoanalyse. + Eventuele specifieke maatregelen voortvloeiend uit een uitgevoerde DPIA

In alle gevallen zal de laatste officieel gepubliceerde versie van het van toepassing zijnde normenkader leidend zijn. In geval van update of vervanging van het geldende normenkader zal de Verwerker

⁶ *Bepaal voorafgaand aan het sluiten van de overeenkomst het risicoprofiel van de verwerking, Zie het Leidraad Verwerkersovereenkomst voor meer informatie. Partijen stellen dit risicoprofiel bij elke wijziging van de verwerking opnieuw vast*

⁷ *Van dit normenkader mogen partijen gezamenlijk gemotiveerd afwijken.*

telkens binnen een periode van één jaar zijn verwerking en alle daarvoor relevante processen en systemen op het nieuwe normenstelsel aanpassen en hierover verantwoording afleggen.

3. Verantwoording van het normenstelsel

Verantwoording over het voldoen aan het geldende normenkader vindt plaats op de hieronder geselecteerde wijze:

Risicoprofiel verwerking	Wijze van verantwoording
Laag	Jaarlijkse zelfevaluatie van het BIG normenkader of de overeengekomen specifieke maatregelen
Midden	Geldig ISO 27001 certificaat of gelijkwaardige certificering, of jaarlijkse TPM van een onafhankelijk RE Auditor over het van toepassing verklaarde normenkader ⁸
Hoog	Jaarlijkse TPM van een onafhankelijke RE Auditor over het van toepassing verklaarde normenkader ⁹

⁸ De scope van de certificering en/of de TPM dient in ieder geval de betreffende verwerking en onderliggende en processen systemen en de BIG-normen af te dekken. Certificering op andere processen dan relevant voor deze verwerking is onvoldoende. [Het vaststellen van het TPM-toetsingskader wordt in afstemming met de opdrachtnemer gedaan.](#)

⁹ Binnen de scope van deze TPM dient uitdrukkelijk ook de risico analyse op basis waarvan aanvullende maatregelen zijn bepaald en volledigheid daarvan te vallen.

Bijlage 2: Werkzaamheden en categorieën van betrokkenen (ter uitwerking van artikel 3 lid 1)

<invullen bij gunning>

Onderdeel	Omschrijving
Beschrijving werkzaamheden van Verwerker of in te schakelen derde(n)	VOORBEELDEN: • Hosting bestaande uit activiteiten zoals... – Back-ups maken en restoren – Applicatiebeheer bestaande uit activiteiten zoals <...> – Technisch beheer bestaande uit activiteiten zoals <...> – Database beheer bestaande uit activiteiten zoals <...> • Helpdesk bestaande uit activiteiten zoals <...> • Communicatievoorziening (zoals berichtenverkeer) • Archiefbeheer • Vernietiging van gegevensdragers • Printing, scanning, kopiëren (lease van Multifunctionals) • Inhoudelijke werkzaamheden die namens de gemeente worden uitgevoerd zoals: – Uitgifte parkeervergunningen – Voeren salarisadministratie
Beschrijving verwerkingsactiviteiten	<Bijvoorbeeld opslaan, raadplegen, verwijderen, combineren, etc>
Verwerkingsdoel(en)	<Bijvoorbeeld: uitvoering geven aan wet WMO>
Categorieën van betrokkenen (wiens gegevens worden verwerkt)	<Bijvoorbeeld: Cliënten, medewerkers, alle inwoners, aanvragers van vergunningen, etc.>
Betreft het een kwetsbare groep?	<Bijvoorbeeld: Ja, minderjarigen / mensen met een verstandelijke beperking etc.. >

De volgende categorieën persoonsgegevens worden verwerkt (aankruisen wat van toepassing is):
 <invullen bij gunning>

Categorie persoonsgegevens	Risico- klasse ¹⁰	Verwerkt? (zo ja, kruisje zetten)
Telefoonnummers	Laag	
E-mailadressen of andere adressen voor elektronische communicatie	Laag	
Toegangs- of identificatiegegevens (Gebruikersnamen, cliëntnummers, wachtwoorden en andere inloggegevens)	Laag/Midden	
Naam-, adres- en woonplaatsgegevens	Laag/Midden	
Geslacht, geboortedatum en/of leeftijd	Midden	
Financiële gegevens (Bankrekeningnummer of creditcardnummer, salaris- en betalingsgegevens)	Midden	
Burgerservicenummer of sofinummer	Midden	
Paspoortkopieën of kopieën van andere legitimatiebewijzen	Hoog	
Bijzondere persoonsgegevens (bijv. ras, etniciteit, gezondheid, strafrechtelijke gegevens, politieke overtuiging, seksuele geaardheid)	Hoog	
(Andere) persoonsgegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. (bijv. informatie over kindermishandeling, huiselijk geweld, opvoedproblemen, schulden, drank- of drugsproblemen)	Hoog	
Medische gegevens en gegevens over (jeugd)hulpverlening of andere zeer kwetsbare groepen.	Hoog	
Overig, namelijk	...	

¹⁰ De risicoklasse van een verwerking wordt bepaald door een combinatie van allerlei omstandigheden. Zie de Leidraad Verwerkersovereenkomst voor meer informatie.

BIJLAGE 3: Register van derden/onderaannemers zoals bedoeld in artikel 5.6

<invullen bij gunning>

PARTIJ 1	<naam>
Vestigingsplaats	< >
Inschrijvingsnummer handelsregister	< >
Beschrijving werkzaamheden	< >
Voorwaarden van Verantwoordelijke aan toestemming	< >
PARTIJ 2	<naam>
Vestigingsplaats	< >
Inschrijvingsnummer handelsregister	< >
Beschrijving werkzaamheden	< >
Voorwaarden van Verantwoordelijke aan toestemming	< >