<TEAMNAAM>

ons kenmerk <kenmerk>
behandelaar **<behandelaar>**
tel nummer <telefoonnummer>
e-mail <e-mailadres>

onderwerp Overeenkomst gegevensuitwisseling zelfstandige verwerkingsverantwoordelijken

OVEREENKOMST GEGEVENSUITWISSELING TUSSEN ZELFSTANDIGE VERWERKINGSVERANTWOORDELIJKEN

Gemeente Venlo, waarvan <het college van Burgemeester en Wethouders/de burgemeester/de gemeenteraad> de verwerkingsverantwoordelijke is, verder te noemen Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door <de heer of mevrouw> <voorletters, persoonsnaam>, hoofd <teamnaam>

en

<Bedrijf>, gevestigd te <plaatsnaam>, KVK-nummer <nummer>, verder te noemen Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam>, <functie>,

hierna afzonderlijk te noemen “Partij”, of gezamenlijk “Partijen”

Overwegen het volgende:

a) Partijen hebben op <datum> de <naam Hoofdovereenkomst>, hierna Hoofdovereenkomst afgesloten;
b) Op de verwerking van Persoonsgegevens door Partijen zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing;
c) Partijen zijn ieder Verwerkingsverantwoordelijke als bedoeld in artikel 4, aanhef en onder 7, AVG voor de verwerkingen die zij uitvoeren;
d) Partijen stellen vast dat zij beide ieder voor zich verwerkingsverantwoordelijke zijn voor hun eigen deel van de verwerking, als bedoeld in artikel 3.2 van deze overeenkomst;
e) Partijen willen in aanvulling op de AVG en de UAVG de volgende afspraken vastleggen over de verwerking van Persoonsgegevens in deze overeenkomst (overeenkomst gegevensuitwisseling).

En komen het volgende overeen:

Artikel 1 Definities

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

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

Artikel 2 Ingangsdatum en duur

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

2.2 Deze Overeenkomst eindigt op het moment dat Partijen de verwerking van Persoonsgegevens hebben beëindigd.

Artikel 3 Onderwerp van deze Overeenkomst

3.1 Partijen verwerken de door of via Partijen ter beschikking gestelde Persoonsgegevens uitsluitend voor de uitvoering van de hierboven genoemde <Hoofdovereenkomst> en daarmee voor <doel>.

3.2 Iedere Partij vult de door haar uit te voeren leveringen aan de andere Partij in tabel 1 van Bijlage 1.

Artikel 4 Inhoudelijke afspraken

4.1 **Beveiligingsmaatregelen**

Partijen zorgen ervoor dat passende technische en organisatorische maatregelen worden genomen om de Persoonsgegevens goed te beveiligen ten aanzien van de levering van Persoonsgegevens, overeenkomstig artikel 32 AVG. Deze maatregelen garanderen een passend beveiligingsniveau bij de verwerkingen genoemd in Bijlage 1.

4.2 **Geheimhouding**

Personen die werken voor Partijen moeten Persoonsgegevens waarmee zij werken geheimhouden. De personen die werken voor Partijen en eventueel ingeschakelde derden hebben daarom een geheimhoudingsverklaring getekend, of zich op een andere manier schriftelijk gebonden aan de geheimhouding.

4.3 **Verwerkers**

Partijen houden – indien van toepassing – bij welke verwerkers zijn ingeschakeld bij de uitwisseling van de Persoonsgegevens.

4.4 **Rechten van betrokkenen**

Als Betrokkene een beroep doet op zijn rechten, zoals genoemd in artikel 12 t/m 22 AVG, kan deze zich richten tot de Partij die Verwerkingsverantwoordelijke is voor de desbetreffende verwerking (zie Bijlage 1). Mocht een Betrokkene zich tot de verkeerde Verwerkingsverantwoordelijke richten, dan zorgt de Partij die het verzoek ontvangt, dat dit verzoek naar de juiste Partij wordt verzonden. Partijen zullen elkaar zo nodig redelijkerwijs ondersteunen bij het tijdig afhandelen van de hierboven genoemde verzoeken.

4.5 **Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging**

Op verzoek van een Partij werkt de andere Partij 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 tijdens de uitwisseling

5.1 Partijen zullen elkaar dan over en weer zo snel mogelijk, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens. Partijen vermelden 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 nemen Partijen zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen.
5.3 Partijen maken na een geconstateerde Inbreuk afspraken over welke Partij de melding doet bij de toezichthoudende autoriteit en/of de Betrokkene(n).

Artikel 6 Beëindigen Overeenkomst
6.1 Partijen maken – indien noodzakelijk – in de Hoofdovereenkomst afspraken over de teruggave en wissen van Persoonsgegevens.
6.2 De geheimhouding geldt ook nog na beëindiging van deze Overeenkomst.

Artikel 7 Overige bepalingen
7.1 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 de bevoegde rechter. Partijen kunnen onderling ook zelf vooraf een bevoegde rechter aanwijzen (forumkeuze).
7.2 Deze Overeenkomst maakt onlosmakelijk deel uit van de Hoofdovereenkomst.

Ondertekening
Aldus overeengekomen en in tweevoud ondertekend,

Ingangsdatum: <ingangsdatum>

Gemeente Venlo <het college van Burgemeester en Wethouders/de burgemeester/de gemeenteraad>	**<Gemeente X> of <Bedrijf>**
namens deze: <voorletters, naam> hoofd <teamnaam>(of anders)	namens deze: <voorletters, naam> <functie>
Plaats: Venlo	Plaats: <plaats>
Datum:……..	Datum:……..

OVERZICHT BIJLAGEN
Bijlage 1: Overzicht van te verwerken persoonsgegevens
Bijlage 2: Aantonen passend niveau van beveiliging

Bijlage 1: Overzicht van te verwerken persoonsgegevens

1. Gegevensverstrekking gemeente Venlo aan <gemeente X of bedrijf>

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

Naam verwerking	Verwerkings-doeleinden	Categorieën van Betrokkenen	Categorieën Persoons-gegevens (waaronder bijzondere persoons-gegevens)	Doorgifte naar derde landen	Doorgifte-instrument	Aanvullende maatregelen (indien van toepassing)
..	..	..	..	..	..	..
..	..	..	..	..	..	..

2. Gegevensverstrekking <bedrijf X> aan gemeente Venlo

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

Naam verwerking	Verwerkings-doeleinden	Categorieën van Betrokkenen	Categorieën Persoons-gegevens (waaronder bijzondere persoons-gegevens)	Doorgifte naar derde landen	Doorgifte-instrument	Aanvullende maatregelen (indien van toepassing)
..	..	..	..	..	..	..
..	..	..	..	..	..	..

3. Contactgegevens

Contactpersoon gemeente Venlo (NB: Ook buiten kantooruren)	*Naam:* Privacy Officer / Functionaris Gegevensbescherming *Contactgegevens:* datalek@venlo.nl
Contactpersoon <gemeente X of bedrijf> (NB: Ook buiten kantooruren)	*Naam:* <naam> *Contactgegevens:* <contactgegevens>
Contactgegevens IBD	*Telefoonnummer:* 070 - 204 55 11 *Emailadres*: privacy@vng.nl

Bijlage 2: Aantonen passend niveau van beveiliging

Gemeente Venlo:

Normenstelsel

□ De Partij werkt volgens een algemeen erkende norm voor informatiebeveiliging, namelijk:……..
(vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS) en is volgens deze norm wel/niet gecertificeerd.

✓ De Partij werkt volgens een algemeen erkende overheidsnorm zoals de BIO, of vergelijkbaar, namelijk: BIO

□ De Partij werkt volgens een andere norm, te weten:
……

Toereikendheid

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

□ Partij verstrekt een actueel en geldig certificaat en verklaring van toepasselijkheid (VVT);
□ Rapportages van periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II);
✓ een Assurance rapport (TPM) van een auditor die is aangesloten bij NOREA;
✓ eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven (in lijn met de aanpak uit hoofdstuk 4.4 uit de BIO, een ICV):
ENSIA audit

NB: Uit de certificering/periodieke externe controles/audits of uit de eigen controles/beschrijvingen blijkt of kan afgeleid worden dat de beveiliging passend is bij de verwerking(en) genoemd in Bijlage 1.

Aansluiting bij goedgekeurde gedragscode

□ Partij is aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode, te weten:
……

<Bedrijf X>:

Normenstelsel

□ De Partij werkt volgens een algemeen erkende norm voor informatiebeveiliging, namelijk:……..
(vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS) en is volgens deze norm wel/niet gecertificeerd.

□ De Partij werkt volgens een algemeen erkende overheidsnorm zoals de BIO, of vergelijkbaar, namelijk:
……

□ De Partij werkt volgens een andere norm, te weten:
……

Toereikendheid

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

□ Partij verstrekt een actueel en geldig certificaat en verklaring van toepasselijkheid (VVT);
□ Rapportages van periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II);
□ een Assurance rapport (TPM) van een auditor die is aangesloten bij NOREA;
□ eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven (in lijn met de aanpak uit hoofdstuk 4.4 uit de BIO, een ICV):

……

NB: Uit de certificering/periodieke externe controles/audits of uit de eigen controles/beschrijvingen blijkt of kan afgeleid worden dat de beveiliging passend is bij de verwerking(en) genoemd in Bijlage 1.

Aansluiting bij goedgekeurde gedragscode

□ Partij is aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode, te weten:
……