INFORMATIE
BEVEILIGINGS
DIENST

VNG Realisatie

# Standaard Verwerkersovereenkomst Gemeenten

## Verwerkersovereenkomst behorende bij "Hoofdovereenkomst ten behoeve van de levering (inclusief het gebruiksrecht), de implementatie, het beheer, het onderhoud en support van een SaaS-ICT-oplossing voor VTH"

De publiekrechtelijke rechtspersoon Omgevingsdienst Drenthe, te dezen rechtsgeldig vertegenwoordigd door xxxxx, hierna te noemen **"de Verwerkingsverantwoordelijke"**;

en

<Bedrijf>, gevestigd te <plaatsnaam>, KVK-nummer <nummer>verder te noemen Verwerker, 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 <titel hoofdovereenkomst>, hierna Hoofdovereenkomst, afgesloten, op grond waarvan Verwerker de volgende dienst(en) levert aan de Verwerkingsverantwoordelijke: <specificatie dienst(en)>;
b) Verwerker verwerkt voor de uitvoering van de Hoofdovereenkomst Persoonsgegevens voor Verwerkingsverantwoordelijke;
c) Op de verwerking van Persoonsgegevens door Verwerker zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing;
d) Partijen willen in aanvulling op de AVG en de UAVG de volgende afspraken over de verwerking van Persoonsgegevens vastleggen in deze verwerkersovereenkomst (hierna: de Verwerkersovereenkomst);

En komen het volgende overeen:

**Artikel 1 Definities**

1.1 Begrippen uit de AVG en de UAVG die in deze Verwerkersovereenkomst worden gebruikt, hebben dezelfde betekenis.
1.2 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die onlosmakelijk deel uitmaken van deze Verwerkersovereenkomst.

**Artikel 2 Ingangsdatum en duur**

2.1 Deze Verwerkersovereenkomst gaat in op het moment dat de Hoofdovereenkomst tot stand is gekomen, tenzij Partijen anders overeenkomen.
2.2 Deze Verwerkersovereenkomst eindigt op het moment dat Verwerker de verwerking van Persoonsgegevens op grond van de Hoofdovereenkomst heeft beëindigd en de afspraken over het teruggeven en/of wissen van Persoonsgegevens zijn nagekomen.
2.3 Wanneer Partijen een (nieuwe) Verwerkersovereenkomst overeenkomen, betekent dat dat de oude Verwerkersovereenkomst komt te vervallen.

**Artikel 3 Onderwerp van deze Verwerkersovereenkomst**

3.1 Verwerker verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke voor de uitvoering van de Hoofdovereenkomst en uitsluitend overeenkomstig schriftelijke instructies van Verwerkingsverantwoordelijke, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke wettelijke bepaling hem tot verwerking verplicht. In dat geval zal Verwerker Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, daarvan zonder onredelijke vertraging in kennis stellen, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
3.2 De door Verwerker uit te voeren verwerkingen staan beschreven in tabel 1 van Bijlage 1.

**Artikel 4 Inhoudelijke afspraken**

4.1 **Beveiligingsmaatregelen**
Verwerker zorgt voor passende technische en organisatorische maatregelen om de Persoonsgegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG. De wijze waarop Verwerker de passende

technische en organisatorische maatregelen aantoont, staat in Bijlage 2.

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

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

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

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

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

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

**Artikel 5 Inbreuk in verband met Persoonsgegevens**

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

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

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

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

**Artikel 6 Aansprakelijkheid**

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

**Artikel 7 Beëindigen verwerkersovereenkomst**

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

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

**Artikel 8 Overige bepalingen**

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

8.2 In afwijking op de standaard verwerkersovereenkomst: verwerking buiten de EER is niet toegestaan. Verwerker mag Persoonsgegevens niet buiten de Europese Economische Ruimte (laten) verwerken. Ook niet wanneer is voldaan aan de voorwaarden van artikel 45 of 46 AVG.

**Ondertekening**

Aldus overeengekomen en in tweevoud ondertekend,

Ingangsdatum: <……>

| | |
|---|---|
| **Omgevingsdienst Drenthe** | **<Naam organisatie>** |
| namens deze**:** <naam, functie> | namens deze: <naam, functie> |
| plaats: <……> | plaats: <……> |
| datum: <……> | datum: <……> |

## Bijlage 1: Overzicht van te verwerken persoonsgegevens, contactgegevens partijen en overzicht ingeschakelde subverwerkers

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

| **Naam verwerking/ Welke dienst en/of product** | **Verwerkings-doeleinden** | **Categorieën van Betrokkenen** | **(Bijzondere) Persoons-gegevens** | **Verwerkings -locatie** | **Doorgifte-instrument (indien van toepassing)** | **Aanvullende maatregelen (indien van toepassing)** |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

**2. Contactgegevens**

| | |
|---|---|
| **Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)** | Naam:<br>Contactgegevens: |
| **Contactpersoon Verwerker (NB: Ook buiten kantooruren)** | Naam:<br>Contactgegevens: |
| **Contactgegevens IBD** | telefoonnummer: 070-204 55 11<br>e-mailadres : privacy@vng.nl |

**3. Ingeschakelde subverwerkers**

| **Naam en contactgegevens subverwerker** | **KvK-nummer** | **Uitbestede verwerkingen** | **Toepassing (geautomatiseerd systeem)** | **Verwerkings-locatie** | **Doorgifte instrument** | **Aanvullende maatregelen (indien van toepassing)** |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |

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

## Bijlage 2: Aantonen passend niveau van beveiliging

Normenstelsel

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

- Datum laatste certificering: …….

□ De verwerker werkt volgens een algemeen erkende overheidsnorm zoals de BIO2, of vergelijkbaar, te weten:
……..,

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

Toereikendheid
De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

□ Verwerker 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 BIO2, een ICV):
……

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

Aansluiting bij goedgekeurde gedragscode

□ Verwerker is aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode, te weten …….

**NB:** Substantiële wijzigingen in het bovenstaande en achteruitgang van de voorwaarden geven partijen op korte termijn aan elkaar door.

# Toelichting bij de Standaard Verwerkersovereenkomst

De Standaard Verwerkersovereenkomst gemeenten is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

Op 23 september 2025 heeft het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) de Baseline Informatiebeveiliging Overheid versie 2 (BIO2) bestuurlijk vastgesteld. De BIO2 vormt het nieuwe kader voor informatiebeveiliging binnen de overheid. Dit vernieuwde model is tot stand gekomen na een evaluatie van de huidige BIO en sluit aan op de ontwikkelingen rondom de NIS2-richtlijn. Hiermee geeft de BIO2 invulling aan de zorgplicht uit de NIS2-richtlijn voor de overheid. De BIO2 is onder leiding van BZK ontwikkeld in samenwerking met gemeenten, provincies, waterschappen en het rijk. De BIO2 is gebaseerd op de laatste versie van de ISO 27001 en de ISO 27002.

## Doel

Gemeenten en leveranciers willen bij de uitvoering van hun taken en diensten komen tot een goede dienstverlening voor inwoners en bedrijven. Als bij de uitvoering van deze taken en diensten persoonsgegevens worden verwerkt dan willen gemeenten en leveranciers de verplichtingen op grond van de AVG nakomen. Daarbij willen Partijen uitgaan van wederzijds vertrouwen.

Het doel van deze standaard verwerkersovereenkomst is het gemeenten en hun leveranciers makkelijker te maken om tot afspraken te komen over de verwerking van persoonsgegevens. Deze standaard wordt gebruikt als aanvulling op een hoofdovereenkomst om op grond van de AVG (artikel 28.3 en 28.9) nadere afspraken te maken en vast te leggen over de omgang met persoonsgegevens.

## Rangorde

De rangorde van de verschillende documenten (o.a. inkoopdocumenten, hoofdovereenkomst, verwerkersovereenkomst) wordt geregeld in de hoofdovereenkomst.

## Beheer van deze standaard

VNG-Realisatie/IBD beheert deze standaard verwerkersovereenkomst. Zowel gemeenten als leveranciers kunnen verbetervoorstellen mailen naar privacy@vng.nl. Maximaal tweemaal per jaar beoordeelt de Beheergroep VWO (bestaande uit vertegenwoordigers van gemeenten en leveranciers), de verbetervoorstellen en zo nodig worden deze verwerkt in een volgende versie.

Hebt u vragen over het gebruik van deze standaard overeenkomst neem dan contact op met de IBD: privacy@vng.nl.

## Doelgroep

Dit document is van belang voor het management van de gemeente, de systeemeigenaren, gemeentelijke inkopers, privacyfunctionarissen en informatiebeveiligers.

### Relatie met overige documenten:

- GIBIT 2023;
- Baseline Informatiebeveiliging Overheid (BIO);
- Inkoopvoorwaarden en informatiebeveiligingseisen;
- Handreiking Service Level Agreements;
- Handreiking Geheimhoudingsverklaringen;
- Handreiking Screening Personeel BIO.

# Inhoudsopgave

Verwerkersovereenkomst uitvoering <naam hoofdovereenkomst> ..... **Fout! Bladwijzer niet gedefinieerd.**
Bijlage 1: Overzicht van te verwerken persoonsgegevens, contactgegevens partijen en overzicht ingeschakelde subverwerkers ..... 5
Bijlage 2: Aantonen passend niveau van beveiliging ..... 6

**1. Inleiding ..... 10**

**2. Algemeen ..... 11**

2.1 Is er wel een verwerkersovereenkomst nodig? ..... 11
2.2 Gedeelde verantwoordelijkheid en vertrouwen ..... 11
2.3 Over welke onderwerpen moeten afspraken gemaakt worden? ..... 11
2.5 Artikelsgewijze toelichting ..... 12
2.6 Toelichting bijlagen ..... 15

**3. Colofon ..... 21**

# 1. Inleiding

Bij de dienstverlening en bedrijfsvoering verwerken gemeenten persoonsgegevens. In voorkomende gevallen worden de verwerkingen uitgevoerd door derde partijen zoals andere overheidsorganisaties, semi-overheidsorganisaties en particuliere bedrijven. Bij de verwerking van persoonsgegevens is het van belang en zelfs wettelijk verplicht dat partijen hierover afspraken maken.

De IBD stelt vast dat gemeenten en leveranciers veel tijd en energie stoppen in het maken van afspraken hierover, maar dat het in veel gevallen niet lukt om tot overeenstemming te komen. De IBD ondersteunt - sinds de oprichting in 2013 - gemeenten en heeft daarom de volgende acties ondernomen:

- Het samen met gemeenten opstellen van een model verwerkersovereenkomst;
- Het ondersteunen van gebruikersverenigingen van gemeenten in de onderhandelingen met enkele grote leveranciers;
- Het opstellen van een factsheet over het opstellen van verwerkersovereenkomsten;
- Het opstellen van een factsheet over verwerkingsverantwoordelijken en verwerkers.

Deze acties hebben enig effect gehad, maar nog steeds ontbraken in veel gevallen sluitende afspraken. Opdrachtgevers en opdrachtnemers, verantwoordelijken en verwerkers achtten dit een hoogst onwenselijke situatie omdat het 1. strijdig is met de wet, 2. ongewenst is bij beveiligingsincidenten (datalekken) en 3. een verkeerd signaal geeft richting inwoners van de betrokken gemeente: de gemeente zou géén prioriteit geven aan een zorgvuldige verwerking van onze persoonsgegevens door derden.

## Compromis als oplossing voor een complex probleem

Gemeenten en leveranciers gaven aan dat er dringend behoefte is om te komen tot een oplossing van situaties waarin er geen sluitende afspraken zijn over de verwerking van persoonsgegevens namens Nederlandse gemeenten. Een oplossing voor een complex probleem als dit is per definitie een compromis. Dit compromis is gevonden in de standaardisering van de gemeentelijke verwerkersovereenkomst (standaard VWO) waar zowel gemeenten als leveranciers zich aan committeren. Gemeenten en leveranciers doen ten opzichte van elkaar op gecontroleerde wijze water bij de wijn om uit de huidige impasse te geraken. Op het niveau van een individuele overeenkomst kan het zijn dat partijen deze standaard ervaren als verbetering of verslechtering. Op het niveau van het collectief maken gemeenten en hun leveranciers een enorme stap voorwaarts: in alle gevallen waarin dat nodig is zijn er nu heldere kaders over de verwerking van persoonsgegevens.

Gemeenten hebben zichzelf op de ALV van de VNG d.d. 5 juni 2019 de verplichting opgelegd om de Standaard VWO te gebruiken. Gemeenten moeten daarom in hun jaarrapportage vastleggen in het geval zij de Standaard VWO niet gebruiken, of daarvan afwijken.

### Gemeenten èn leveranciers

Bij het opstellen van deze standaard VWO is uitvoerig overleg geweest met een representatieve groep gemeenten en leveranciers. De uiteindelijke inhoud is vastgesteld door de Beheergroep VWO bestaande uit vertegenwoordigers van 14 gemeenten (CISO's, FG's en inkopers). Het IBD-model verwerkersovereenkomst diende als basis voor deze standaard. Uit dit model zijn onderdelen verwijderd die zijn geregeld in de Algemene Verordening Gegevensbescherming (definities, inbreuken), het Burgerlijk Wetboek (ingebrekestelling, beëindiging overeenkomst), of de hoofdovereenkomst (meerwerk en vergoeding daarvan, aansprakelijkheid). Daarnaast is gewerkt om het document toegankelijker te maken voor de doelgroepen die de afspraken uitvoeren of daarop toezien. Het document bevat juridische taal waar nodig en een toegankelijke omschrijving waar dat kan.

**NB**: Overal in de Handreiking waar 'gemeenten' staat, moet worden gelezen 'gemeentelijke organisaties'.

# 2. Algemeen

## 2.1 Is er wel een verwerkersovereenkomst nodig?

Voordat partijen afspraken maken over de verwerking van persoonsgegevens is het noodzakelijk om te weten wat de rol is van de betrokken partijen. Is er ten aanzien van de verwerking van persoonsgegevens wel sprake van een relatie verwerkingsverantwoordelijke - verwerker? Zo ja, dan maken partijen afspraken over de verwerking van persoonsgegevens. Om te bepalen wat de precieze rol is van de betrokken partijen en daarmee of het dan ook nodig is om een verwerkersovereenkomst af te sluiten, verwijzen wij u naar de Factsheet en beslismodel "Is mijn leverancier wel of geen verwerker".

## 2.2 Gedeelde verantwoordelijkheid en vertrouwen

Verwerkingsverantwoordelijken en verwerkers hebben op grond van de AVG gezamenlijk en individueel een verantwoordelijkheid ten aanzien van de verwerking van persoonsgegevens. Zodoende moet het echt de intentie van partijen zijn om de persoonsgegevens van betrokkenen zorgvuldig te verwerken en te beveiligen. Partijen maken in aanvulling op de hoofdovereenkomst dan ook nadere afspraken over de verwerking van persoonsgegevens. Dat kan een verwerkersovereenkomst zijn.

## 2.3 Over welke onderwerpen moeten afspraken gemaakt worden?

Het is verplicht om afspraken te maken over de omgang met persoonsgegevens tussen verantwoordelijke en verwerker. Het is echter niet verplicht om een verwerkersovereenkomst af te sluiten. Afspraken over hoe partijen omgaan met persoonsgegevens mogen bijvoorbeeld ook best in de hoofdovereenkomst worden vastgelegd. Er zijn enkele onderwerpen waarover verplicht afspraken gemaakt moeten worden. Deze onderwerpen staan ook in de standaard verwerkersovereenkomst:

| **Onderwerp** | **Waar geregeld in verwerkersovereenkomst** |
|---|---|
| Onderwerp | Artikel 3 |
| Duur | Artikel 2 |
| Aard en doel | Bijlage 1, tabel 1 |
| Soort persoonsgegevens | Bijlage 1, tabel 1 |
| Categorieën van betrokkenen | Bijlage 1, tabel 1 |
| Rechten en verplichtingen van de verwerkingsverantwoordelijke | Hele overeenkomst |
| Verwerking alleen op basis van schriftelijke instructies | Art. 3.1 |
| Doorgifte naar derde landen | Art. 4.3 |
| Vertrouwelijkheid | Art. 4.4 |
| Passende technische en organisatorische maatregelen | Art. 4.1 |
| Inschakeling subverwerkers | Art. 4.5 |

| | |
|---|---|
| Verwerker verleent bijstand bij verzoeken van betrokkene | Art. 4.6 |
| Verwerker verleent bijstand bij nakoming art. 32 t/m 36 | Art. 4.1 / 5 / 4.7 |
| Verwerker wist persoonsgegevens of geeft deze na afloop verwerking terug | Art. 2.1 en 7.1 |

**NB:** Over andere onderwerpen zoals de uitvoering van audits, aansprakelijkheid en de exit-strategie maken partijen afspraken in de hoofdovereenkomst. Als hierover geen afspraken zijn gemaakt in de hoofdovereenkomst, adviseren wij partijen om dat alsnog te doen in een addendum bij de hoofdovereenkomst. In die gevallen dat er helemaal geen hoofdovereenkomst is, kunnen partijen er voor kiezen om deze afspraken te maken in een addendum bij de Standaard VWO. En dus niet in de Standaard VWO zelf. Het vorenstaande geldt ook als bestaande afspraken niet meer passend zijn; in dat geval maken partijen in een addendum bij de hoofdovereenkomst, of in een addendum bij de Standaard VWO, nieuwe afspraken en niet in de Standaard VWO zelf.

Over de inhoud van de eventueel nader te maken afspraken verwijzen wij naar de GIBIT 2023[1]:

Aansprakelijkheid : artikel 16
Exit-strategie : artikel 24.14 en artikel 26
Audit : artikel 25[2]

## 2.4 Meerwerk

Het komt voor dat de verwerker bij de uitvoering van de overeenkomst t.a.v. verwerking van persoonsgegevens kosten moet maken. De vraag of dit wel of geen meerwerk en derhalve wel of niet in aanmerking komt voor vergoeding door de opdrachtgever, moet in de hoofdovereenkomst worden geregeld of in een addendum bij de hoofdovereenkomst. In die gevallen dat er helemaal geen hoofdovereenkomst is, kunnen partijen er voor kiezen om deze afspraken te maken in een addendum bij de Standaard VWO. Ook hiervoor geldt: niet regelen in de Standaard VWO zelf. Zie hiervoor artikel 11.3 van de GIBIT 2023.

## 2.5 Artikelsgewijze toelichting

### Aanhef:

Stelregel is dat als de gemeente privaatrechtelijk handelt (bijvoorbeeld overeenkomsten sluit, gronden verkoopt), de gemeente als rechtspersoon optreedt. In het privaatrecht kunnen alleen natuurlijke personen en rechtspersonen aan het rechtsverkeer deelnemen. Voor de AVG is echter het bestuursorgaan de verwerkingsverantwoordelijke. Dit kan de burgemeester, het college of de gemeenteraad zijn. Bij het sluiten van de verwerkersovereenkomst moet wel duidelijk zijn welk gemeentelijk bestuursorgaan verwerkingsverantwoordelijke is.

### Overwegingen:

De verwerkersovereenkomst maakt onderdeel uit van een hoofdovereenkomst. Vul hier de naam van hoofdovereenkomst in.

[1] Voor vragen over de GIBIT 2023 kunt u contact opnemen met info@gibit.nl
[2] Zie hiervoor Bijlage 3.

## Artikelen:

1.1: De definities van art. 4 AVG hebben in deze verwerkersovereenkomst dezelfde betekenis.

2.1: Het uitgangspunt is dat de verwerkersovereenkomst ingaat op het moment dat de hoofdovereenkomst tot stand is gekomen. Partijen kunnen daar echter van afwijken. Zij moeten dat dan wel expliciet aangeven

2.2: Dit artikel moet in samenhang met artikel 7.1 worden gelezen.

2.3 Wanneer Partijen ervoor kiezen om de nieuwe versie van de Standaard VWO af te sluiten, betekent dat dat de vorige overeengekomen verwerkersovereenkomst niet meer geldig is.

3.1: Voor iedere verdere verwerking van persoonsgegevens die buiten de opdrachtverlening valt zoals genoemd in tabel 1 van Bijlage 1, moet de verwerker vooraf uitdrukkelijk toestemming vragen aan de verwerkingsverantwoordelijke. Dit geldt ook voor de verwerking van persoonsgegevens als op enige wijze kunstmatige intelligentie wordt toegepast, waaronder testen en trainen.
Verwerker zal de verwerkingsverantwoordelijke zonder onredelijke vertraging informeren, indien een schriftelijke instructie van de verwerkingsverantwoordelijke naar het oordeel van de verwerker in strijd is met de AVG of de UAVG.

3.2: De verwerker mag alleen de in Bijlage 1, tabel 1 vermelde verwerkingen uitvoeren.

4.1: Een uit artikel 4.1 volgend passend beveiligingsniveau kan betekenen dat de verwerker zelf het initiatief neemt om aanvullende maatregelen te nemen. Daarnaast kan ook de verwerkingsverantwoordelijke aan de verwerker opdragen om het beveiligingsniveau te verbeteren. Als objectief is vastgesteld dat de verwerker geen passend beveiligingsniveau heeft en de verwerkingsverantwoordelijke daarom uitdrukkelijk schriftelijk verzoekt, zullen partijen in onderling overleg bepalen welke aanvullende beveiligingsmaatregelen de verwerker zal treffen.

4.2: De verwerker is op grond van de AVG verplicht om mee te werken aan de uitvoering van een audit. Partijen maken vooraf afspraken over de frequentie van de uit te voeren audits. Als de verwerker op basis van een certificering kan aantonen dat het beveiligingsniveau voldoende is, kan een audit achterwege blijven. Hiervoor dienen de scope en de verklaring van toepasselijkheid van de certificering wel de verwerking volledig dekken. Partijen treden daarover in overleg. Mocht uit het auditverslag blijken dat de verwerker bepaalde werkzaamheden moet verrichten om het beveiligingsniveau aan te passen, dan zal de verwerker deze werkzaamheden binnen een redelijke termijn uitvoeren. T.a.v. de kosten van de audit wordt aangesloten bij art. 25.6 van de GIBIT 2023.
Bij twijfel over de uitkomsten van de audit gaat de verwerkingsverantwoordelijke daarover in gesprek met de verwerker. Eventueel kan de verwerkingsverantwoordelijke zich wenden tot de auditor.
Als DigiD wordt gebruikt bij de verwerking, moet de verwerker jaarlijks een TPM overleggen aan de verwerkingsverantwoordelijke.
NB: De kosten van de certificering zelf zijn voor rekening van de verwerker.

4.3: De verwerker moet de verwerkingsverantwoordelijke altijd vooraf op de hoogte brengen van een doorgifte aan een derde land of een internationale organisatie. Als de Europese Commissie een adequaatheidsbesluit heeft genomen t.a.v. de doorgifte aan een derde land, of een internationale organisatie, is hiervoor geen toestemming nodig van de verwerkingsverantwoordelijke (art. 45 AVG).
Als er geen adequaatheidsbesluit is afgegeven voor een doorgifte aan een derde land of een internationale organisatie, dan mag de verwerking van persoonsgegevens daar toch plaatsvinden, als er wordt voldaan aan de in artikel 46 AVG genoemde instrumenten. De verwerker maakt dan een analyse van de passende waarborgen en de voor de betrokkenen afdwingbare rechten en doeltreffende rechtsmiddelen die het derde land of internationale organisatie heeft getroffen en de eventueel noodzakelijke aanvullende maatregelen. De verwerker legt deze analyse ter beoordeling voor aan de verwerkingsverantwoordelijke.

Het vorenstaande geldt ook als een subverwerker persoonsgegevens doorgeeft aan een derde land of een internationale organisatie.

4.4: De verwerker zorgt dat de personen die onder zijn verantwoordelijkheid werkzaam zijn en toegang hebben tot de persoonsgegevens op een of andere schriftelijke manier zijn gehouden aan de geheimhoudingsplicht.

4.5: Verwerker mag een andere verwerker inschakelen: een subverwerker. Een subverwerker is een andere zelfstandige partij die in opdracht van de 1e verwerker (een deel) van de persoonsgegevens verwerkt. Deze subverwerker opereert zelfstandig, maar moet de persoonsgegevens wel verwerken volgens de schriftelijke instructies van de verwerkingsverantwoordelijke, net als de 1e verwerker. De subverwerker heeft t.a.v. de gegevensbescherming dezelfde verplichtingen die de 1e verwerker heeft. Als de subverwerker zijn verplichtingen niet nakomt, blijft de 1e verwerker t.a.v. de gegevensbescherming volledig aansprakelijk voor het niet nakomen van de verplichtingen door de subverwerker. In het geval het niet (direct) mogelijk is om dezelfde afspraken te maken met een subverwerker (bv. In geval van multinationals als Microsoft/Google), dan moet de subverwerker in ieder geval voldoen aan de verplichtingen van de AVG. Ook na de ingangsdatum van de verwerkersovereenkomst moet de verwerker de verwerkingsverantwoordelijke informeren over de inschakeling van nieuwe subverwerkers. Verwerkingsverantwoordelijke heeft overeenkomstig artikel 28.2 AVG het recht om bezwaar te maken tegen een subverwerker. Als een verwerkingsverantwoordelijke daadwerkelijk bezwaar heeft tegen een subverwerker, gaan partijen hierover in overleg.
NB: Als de verwerker een persoon inhuurt voor bepaalde werkzaamheden, hoeft dat niet automatisch te betekenen dat er sprake is van een subverwerker.

4.6: Als een betrokkene een beroep doet op zijn rechten, dan helpt de verwerker de verwerkingsverantwoordelijke om hier binnen de wettelijke termijn op te kunnen beslissen. Mocht een betrokkene bij de uitoefening van zijn rechten zich rechtstreeks richten tot de verwerker, dan neemt laatstgenoemde hierover direct contact op met de verwerkingsverantwoordelijke.
Voor wat betreft eventuele kosten die hiermee gepaard gaan: zie § 2.4.

4.7: Partijen zullen in onderling overleg afspraken maken over de uitvoering, de termijn van uitvoering van de DPIA en de kosten die daarmee zijn gemoeid. Als partijen hier vooraf concrete afspraken over maken, nemen ze deze op in de hoofdovereenkomst, dan wel een addendum bij de hoofdovereenkomst. Als er helemaal geen hoofdovereenkomst is, kunnen partijen het opnemen in het addendum bij de Standaard VWO. En dus niet in de Standaard VWO zelf.

5.1: Het is belangrijk dat de verwerker de verwerkingsverantwoordelijke zo snel mogelijk op de hoogte brengt van een (vermoedelijke) inbreuk. Het gaat er daarbij om dat de verwerker de verwerkingsverantwoordelijke direct informeert zodra er voldoende redenen zijn om aan te nemen dat er sprake is van een inbreuk. Als er sprake is van verdachte activiteiten, hoeft er geen sprake te zijn van een inbreuk. Verwerker moet daar wel een adequaat onderzoek naar doen. Partijen vertrouwen er daarbij op dat de verwerker professioneel genoeg is om een inschatting te maken van het incident dat moet worden gemeld. Mocht verwerker desondanks niet een goede inschatting kunnen maken van het incident, dan kan deze een second opinion vragen bij de IBD. Daarbij blijft de verantwoordelijkheid om het incident wel of niet te melden aan de verwerkingsverantwoordelijke altijd bij de verwerker. Zolang een onderzoek naar een vermoedelijke inbreuk loopt, kan de verwerker niet worden geacht "kennis" te hebben genomen van een inbreuk. De meldingstermijn van 24 uur begint op dat moment dan ook niet te lopen. Zodra de verwerker wel kennis heeft van de inbreuk, moet hij die binnen 24 uur melden bij de verwerkingsverantwoordelijke. De termijn van 24 uur is een maximale termijn.
De termijn van 72 uur die de verwerkingsverantwoordelijke heeft om de inbreuk te melden bij de toezichthoudende autoriteit begint te lopen, zodra de verwerkingsverantwoordelijke kennis heeft genomen van de inbreuk. Zie hiervoor opinie 250 van de EDPB:

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 (en dan vooral onderaan pagina 15). Dus als de inbreuk heeft plaatsgevonden bij de verwerker en deze meldt het aan de verwerkingsverantwoordelijke, heeft laatstgenoemde pas op dat moment kennis genomen van de inbreuk en begint de meldingstermijn van 72 uur te lopen.
Ten behoeve van de uiteindelijke melding aan de toezichthoudende autoriteit verstrekt de verwerker alle hem beschikbare informatie aan de Verwerkingsverantwoordelijke zoals vermeld op het formulier van Meldloket van de Autoriteit Persoonsgegevens (hierna: AP).
**Let op:** De verwerker doet nooit zelf een melding bij de AP.
Verwerkingsverantwoordelijke moet zorgen voor een 24/7 bereikbaarheid om zo een melding via het afgesproken kanaal in ontvangst te kunnen nemen. Als een verwerker is aangesloten bij de IBD, kan verwerker ervoor kiezen om een inbreuk ook te melden via IBD. De IBD is een CERT en is erop ingericht om in geval van een inbreuk direct alle betrokken gemeenten te informeren.

5.3 Een verwerkingsverantwoordelijke heeft alleen toegang heeft tot het logboek van de verwerker voor zover dat betrekking heeft op de verwerkingen die worden gedaan in opdracht van de verwerkingsverantwoordelijke.

5.4: De beslissing om de inbreuk te melden bij de toezichthoudende autoriteit en/of de betrokkene ligt bij de verwerkingsverantwoordelijke en niet bij de verwerker.

6.1: Afspraken over aansprakelijkheid t.a.v. de verwerking van persoonsgegevens horen thuis in de hoofdovereenkomst. Als hierover geen afspraken zijn gemaakt, adviseren wij partijen om dat alsnog te doen in een addendum bij de hoofdovereenkomst. In die gevallen dat er helemaal geen hoofdovereenkomst is, kunnen partijen ervoor kiezen om deze afspraken te maken in een addendum bij de Standaard VWO. En dus niet in de Standaard VWO zelf. Zie ook § 2.3.
Let op: Als er (in de hoofdovereenkomst, een addendum bij de hoofdovereenkomst of een addendum bij de Standaard VWO) t.a.v. de verwerking van persoonsgegevens geen aparte afspraken zijn gemaakt over aansprakelijkheid, dan geldt de aansprakelijkheidsregeling in de toepasselijke inkoopvoorwaarden, te weten de GIBIT 2023, of de van de van het VNG Model Inkoopvoorwaarden diensten en leveringen afgeleide gemeentelijke inkoopvoorwaarden, of een eventuele afwijkende aansprakelijkheidsregeling in de hoofdovereenkomst. Als in de hoofdovereenkomst of in de inkoopvoorwaarden een beperking van de aansprakelijkheid is opgenomen, adviseren wij partijen om te verifieren of deze beperking ook van toepassing is op de aansprakelijkheid t.a.v. de verwerking van persoonsgegevens en of deze beperking passend is.

7.1 Afspraken over de exit-strategie t.a.v. de verwerking van persoonsgegevens horen thuis in de hoofdovereenkomst. Als hierover geen afspraken zijn gemaakt adviseren wij partijen om dat alsnog te doen, hetzij in de hoofdovereenkomst, of in een addendum bij de hoofdovereenkomst. In die gevallen dat er helemaal geen hoofdovereenkomst is, kunnen partijen er voor kiezen om deze afspraken te maken in een addendum bij de Standaard VWO. En dus niet in de Standaard VWO zelf. Zie ook § 2.3.
Er zijn verschillende manieren waarop partijen de exit-strategie vorm kunnen geven. Artikel 26 van de GIBIT 2023 is onder andere een voorbeeld van een exit-strategie die aan de minimumvoorwaarden voldoet.

## 2.6 Toelichting bijlagen

**Bijlage 1:**

De verwerker vult bijlage 1 in. Als deze daarbij hulp nodig heeft, kan de verwerker de hulp inroepen van de verwerkingsverantwoordelijke.

Tabel 1: In het eerste deel wordt ingevuld:

- Welke verwerking: zie hiervoor: https://www.informatiebeveiligingsdienst.nl/product/vooringevuld-verwerkingsregister-gemeenten/ Zie onder Kolom ‘H’.

- Verwerkingsdoeleinden, zie hiervoor: https://www.informatiebeveiligingsdienst.nl/product/vooringevuld-verwerkingsregister-gemeenten/ Zie onder Kolom 'L'.
- Categorieën van betrokkenen: dit zijn voorbeelden van categorieën van betrokkenen:
  - Aanvragers/Indieners
  - Belanghebbenden
  - Bestuurders/Raadsleden
  - Ambtenaren gemeente
  - Websitebezoekers
  - Personeel leveranciers
  - Scholieren
  - Studenten
  - Ouderen
  - Gehandicapten
  - Kinderen
  - Categorieën persoonsgegevens: dit zijn voorbeelden van categorieën persoonsgegevens:

| | |
|---|---|
| Arbeidsgegevens | Functie, werktijden |
| Beeldmateriaal | Videomateriaal, audiomateriaal |
| Contactgegevens | e-mailadres, telefoonnummer, adres |
| Identiteitsgegevens | Identificatienr., paspoortnr., BTW nummer ZZP-er |
| Inloggegevens | Gebruikersnaam, wachtwoord |
| Internetgegevens | IP-adres, online surfgedrag, cookies |
| Locatiegegevens | Lengtegraad, breedtegraad |
| Persoonlijke gegevens | Naam, geboortedatum, geboorteplaats, geslacht, gezinssamenstelling |

**Bijzondere en gevoelige persoonsgegevens**

| |
|---|
| Biometrische gegevens met het oog op de unieke identificatie van een persoon |
| BSN |
| Financiële gegevens |
| Genetische gegevens |
| Gezondheidsgegevens |
| Lidmaatschap van een vakbond |
| Politieke opvattingen |
| Ras of etnische afkomst |
| Religieuze of levensbeschouwelijke overtuigingen |
| Seksueel gedrag of seksuele gerichtheid |
| Strafrechtelijke persoonsgegevens |

**Verwerkingslocatie**
Het moet duidelijk zijn waar de verwerking plaatsvindt. Als persoonsgegevens worden doorgegeven naar (of toegankelijk zijn in) een land buiten de EER moet dat hier ook worden aangegeven.

**Doorgifte-instrument**
Als er sprake is van een verwerking buiten de EER moet aangegeven worden welk doorgifte-instrument wordt gebruikt. De mogelijke doorgifte-instrumenten zijn:

1. Adequaatheidsbesluit;
2. Specifieke uitzonderingen (art. 49);
3. Standaard bepalingen (standard contractual clauses SCCs);
4. Bindende bedrijfsvoorschriften (binding corporate rules, BCRs);
5. Gedragsregels (codes of conduct; certification mechanisms);
6. Ad hoc modelcontractbepalingen (ad hoc contractual clauses).

**Aanvullende maatregelen**

- Indien gebruik wordt gemaakt van doorgifte-instrumenten 3 t/m 6 worden, conform de aanbevelingen van de EDPB (Recommendations 01/2020), aanvullende technische, organisatorische en contractuele maatregelen getroffen om een aan de AVG gelijkwaardig beschermingsniveau te waarborgen.
- De aanvullende maatregelen worden vastgesteld op basis van een risicoafweging, rekening houdend met de aard van de persoonsgegevens, de verwerkingsactiviteiten en het derde land. Hiermee wordt beoogd een beschermingsniveau te realiseren dat materieel gelijkwaardig is aan het beschermingsniveau binnen de EER.

- Technische maatregelen (voorbeelden)
  - Encryptie van persoonsgegevens tijdens opslag en overdracht
  - Beheer van encryptiesleutels binnen de EER
  - Toegangsbeperkingen op basis van need-to-know en/of least privilege
  - Logging en monitoring van toegang tot persoonsgegevens
  - Logische scheiding van gegevens
  - Pseudonimisering of anonimisering waar mogelijk
- Organisatorische maatregelen (voorbeelden)
  - Beleidsregels die toegang vanuit derde landen beperken
  - Training en bewustwording van medewerkers
  - Procedures voor beoordeling en afhandeling van verzoeken van buitenlandse autoriteiten
  - Incident- en datalekprocedures gericht op internationale doorgifte
- Contractuele maatregelen (voorbeelden)
  - Verwerking uitsluitend op schriftelijke instructie van de verwerkingsverantwoordelijke
  - Informatieplicht bij verzoeken van buitenlandse autoriteiten, voor zover wettelijk toegestaan
  - Verplichting tot juridische toetsing en betwisting van dergelijke verzoeken
  - Beperking van verdere doorgifte aan (sub)verwerkers
  - Audit- en controlebevoegdheden voor de verwerkingsverantwoordelijke

Hieronder een voorbeeld :

| **Naam verwerking/Welke dienst en/of product** | **Verwerkings-doeleinden** | **Categorieën van betrokkenen** | **(Bijzondere) persoonsgegevens** | **Verwerkings-locatie** | **Doorgifte instrument (indien van toepassing)** | **Aanvullende maatregelen (indien van toepassing)** |
|---|---|---|---|---|---|---|
| Xxxxxxsite CMS | • Identificatie binnen de applicatie<br>• Content kunnen plaatsen op website<br><br>Optioneel:<br>• Registreren nieuwsbrief abonnees (module Nieuwsbrief)<br>• Reactiemogelijk op vacature (module Vacature) | • Aanvragers/Indieners<br>• Belanghebbenden<br>• Websitebezoekers<br>• Medewerkers organisatie | • Persoonlijke gegevens: Naam, geboortedatum, geslacht<br>• Contactgegevens: e-mailadres, telefoonnummer, adres<br>• Inloggegevens: Gebruikersnaam, wachtwoord<br>• Internetgegevens: IP-adres, online surfgedrag, cookies<br>• Arbeidsgegevens: Functie, werktijden | EER | Niet van toepassing | Niet van toepassing |
| Xxxform (formulieren-generator) | "Benodigd om bepaalde diensten te kunnen afnemen. Bijvoorbeeld het doorgeven van een verhuizing" | • Aanvragers/Indieners<br>• Belanghebbenden<br>• Websitebezoekers<br>Medewerkers organisatie | • Persoonlijke gegevens: Naam, geboortedatum, geslacht<br>• Contactgegevens: e-mailadres, telefoonnummer, adres<br>• Inloggegevens: Gebruikersnaam, wachtwoord<br>• Internetgegevens: IP-adres, online surfgedrag, cookies | EER | Niet van toepassing | Niet van toepassing |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | Optioneel:<br>• BSN (bij gebruik DigiD)<br>• Overige formuliergegevens afhankelijk van de uitvraag. | | | |

Tabel 2: hier wordt ingevuld:

- Wie zijn (ook buiten kantooruren!) de contactpersonen van de verwerkingsverantwoordelijke, de verwerker en de IBD. Zorg voor een gemeentelijk e-mailadres dat niet wijzigt als de gemeentelijke contactpersoon niet meer in dienst is. Dus bijvoorbeeld: privacy@naamgemeente.nl.
- In het geval er meerdere gemeenten bij het incident zijn betrokken, informeren partijen ook de IBD. De IBD is telefonisch 24 uur per dag bereikbaar. De mail van de IBD wordt niet 24 uur per dag gelezen.

Tabel 3:

- Indien er sprake is van een of meerdere subverwerkers, dan vult de verwerker de tabel voor iedere subverwerker met de volgende gegevens:
  - **de naam en de contactgegevens subverwerker**: Vermeld de volledige handelsnaam van de subverwerker en relevante contactgegevens;
  - het **Kvk-nummer**
  - **Uitbestede verwerkingen:** Hier wordt aangegeven welke categorieën van verwerkingen de subverwerker uitvoert. De verwerker selecteert uitsluitend de categorieën die feitelijk van toepassing zijn. Onderstaande categorieën zijn juridisch herleidbaar tot artikel 4, lid 2 AVG. Categorieën uitbestede verwerkingen:
    - Opslaan en hosten van persoonsgegevens: Hieronder valt het vastleggen en opslaan van persoonsgegevens, ongeacht de vorm (digitaal of fysiek). Dit betreft onder meer opslag op servers, databases, archieven of andere opslagmedia.
    - Beschikbaar stellen van persoonsgegevens ten behoeve van uitvoering van diensten: Hieronder valt het raadplegen en gebruiken van persoonsgegevens zodat de dienstverlening aan de verwerkingsverantwoordelijke kan worden uitgevoerd, bijvoorbeeld inzage, verwerking of weergave van gegevens.
    - Technisch, organisatorisch of operationeel beheer met mogelijke toegang tot persoonsgegevens: Hieronder valt beheer waarbij toegang tot persoonsgegevens mogelijk is, zoals onderhoud, ondersteuning, kwaliteitscontrole, beveiliging of incidentafhandeling. Dit kan zowel geautomatiseerd als handmatig plaatsvinden.
    - Vastleggen, wijzigen of actualiseren van persoonsgegevens: Hieronder valt het bijwerken, corrigeren of aanvullen van persoonsgegevens op instructie van de verwerkingsverantwoordelijke.
    - Ordenen, structureren of combineren van persoonsgegevens: Hieronder valt het structureren, rubriceren, koppelen of anderszins organiseren van persoonsgegevens ten behoeve van de overeengekomen dienstverlening.
    - Back-ups, herstel en continuïteitsvoorzieningen: Hieronder vallen het maken van back-ups, het bewaren daarvan, en het herstellen van persoonsgegevens bij incidenten of calamiteiten.
    - Verstrekken of ter beschikking stellen van persoonsgegevens: Hieronder valt het doorgeven of beschikbaar stellen van persoonsgegevens aan de verwerkingsverantwoordelijke of, indien toegestaan, aan andere partijen op instructie van de verwerkingsverantwoordelijke.
    - Afschermen, beveiligen en beperken van toegang tot persoonsgegevens: Hieronder vallen beveiligingsmaatregelen zoals toegangsbeperkingen, autorisaties, logging en monitoring.
    - Verwijderen en vernietigen van persoonsgegevens: Hieronder valt het wissen of vernietigen van persoonsgegevens na beëindiging van de dienstverlening of op instructie van de verwerkingsverantwoordelijke.
  - **Toepassing (geautomatiseerd systeem)**
    Vermeld het systeem, de applicatie of de omgeving waarin de uitbestede verwerkingen plaatsvinden. Dit kan zowel een geautomatiseerd systeem als een fysieke of hybride omgeving zijn.

- **Verwerkingslocatie**
  Vermeld het land of de landen waar de verwerking feitelijk plaatsvindt. Indien persoonsgegevens worden doorgegeven aan of toegankelijk zijn vanuit landen buiten de EER, moet dit expliciet worden vermeld.
- **Doorgifte instrument**
  Zie toelichting bij Bijlage 1 tabel 1
- Aanvullende maatregelen
  Zie toelichting bij Bijlage 1 tabel 1

Voorbeeld

**4. Ingeschakelde subverwerkers**

| Naam en contactgegevens subverwerker | KvK-nummer | Uitbestede verwerkingen | Toepassing (geautomatiseerd systeem) | Verwerkings-locatie | Doorgifte instrument | Aanvullende maatregelen (indien van toepassing) |
|---|---|---|---|---|---|---|
| HostingXXX | KvK XXX | • Opslaan en hosten van persoonsgegevens<br>• Beschikbaar stellen van persoonsgegevens ten behoeve van uitvoering van diensten<br>• Technisch beheer met mogelijke toegang tot persoonsgegevens<br>• Back-ups, herstel en continuïteitsvoorzieningen<br>• Verwijderen en vernietigen van persoonsgegevens | Xxxxxxsite CMS | Duitsland - Europese Economische Ruimte (EER) | N.v.t. of gekozen instrument | Encryptie, toegangsbeperking, logging, etc. |
| | | | | | | |

**Bijlage 2:**

Bijlage 2 is een praktische uitwerking van artikel 32 AVG. Dus verwerker moet hier aangeven welke passende technische en organisatorische maatregelen hij heeft genomen die een op het risico afgestemd beveiligingsniveau waarborgen. Dus de verwerker geeft aan welk normenstelsel hij voldoet, hoe de toereikendheid van de informatiebeveiliging is gewaarborgd. In dat kader kan verwerker aangeven of hij is aangesloten bij een door de AP goedgekeurde gedragscode.

Normenstelsel: Hier wordt een keuze gemaakt voor het normenstelsel dat van toepassing is op de verwerking waarover de overeenkomst wordt afgesloten. Dit is bij voorkeur de BIO2 maar, indien verwerker kan aantonen dat hij voldoet aan een andere vergelijkbare norm, kan die hier ook worden ingevuld om de punten 1 en 2 van deze bijlage met elkaar in één lijn te brengen.

Toereikendheid: Omdat het onder de AVG belangrijk is om te kunnen aantonen dat de verwerking voldoet aan de afgesproken eisen over een niveau van beveiliging dat past bij de verwerking, wordt hier aangegeven hoe een verwerker dit kan aantonen. Hierbij zijn diverse mogelijkheden aan te kruisen. Waar relevant verstrekt[3] Verwerker bewijsstukken (zoals een geldig certificaat, verklaring van toepasselijkheid en andere bewijsstukken) waaruit blijkt dat wordt voldaan aan opgegeven normen, certificeringen, etc. Tenzij het zonder meer verstrekken de informatieveiligheid van Verwerker ernstig verlaagt.
Het is aan de verwerkingsverantwoordelijke om te beoordelen of deze verantwoording voldoende is voor de betreffende verwerking en ook aan verwerker om actief te controleren of aan deze paragraaf van de bijlage gevolg wordt gegeven. Voor meer informatie over hoe je kunt bepalen of een certificaat valide is, kunt u de IBD factsheet over assurance lezen.

Verder kan de verwerker aangeven of deze is aangesloten bij een goedgekeurde gedragscode.

[3] Hardcopy, via de mail, of via een link.

**Bijlage 3:**
Bijlage 3 is géén onderdeel van de Standaard VWO.

Partijen hebben niet altijd afspraken gemaakt over de aansprakelijkheid, de exit-strategie en/of de uitvoering van audits. Soms willen zij hierover alsnog afspraken maken. In de GIBIT 2023 zijn de aansprakelijkheid, de exit-strategie en de uitvoering van audits wel geregeld. In Bijlage 3 staan de artikelen uit de GIBIT 2023 over deze onderwerpen. Partijen kunnen er voor kiezen om deze artikelen over te nemen in een bijlage bij de hoofdovereenkomst of een bijlage bij de Standaard VWO (en dus niet in de Standaard VWO zelf!).

NB: Deze artikelsgewijze toelichting maakt onderdeel uit van de Standaard Verwerkersovereenkomst.

# 3. Colofon

## Naam document
Standaard verwerkersovereenkomst gemeenten

## Versienummer
2.53

## Versiedatum
15-12 2025

## Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten (IBD)

Tenzij anders vermeld, is dit werk verstrekt onder een Creative Commons Naamsvermelding-Niet Commercieel-Gelijk Delen 4.0 Internationaal licentie. Dit houdt in dat het materiaal gebruikt en gedeeld mag worden onder de volgende voorwaarden: Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:
1. De IBD wordt als bron vermeld.
2. Het document en de inhoud mogen commercieel niet geëxploiteerd worden.
3. Publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door de IBD en / of de Vereniging van Nederlandse Gemeenten.
4. Iedere kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Wanneer dit werk wordt gebruikt, hanteer dan de volgende methode van naamsvermelding: “Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten”, licentie onder: CC BY-NC-SA 4.0.

Bezoek http://creativecommons.org/licenses/by-nc-sa/4.0 voor meer informatie over de licentie.

## Rechten en vrijwaring
De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

## Met dank aan

De gemeenten, leveranciers en derden die hebben bijgedragen aan de totstandkoming van dit document. In het bijzonder de toetsgroep, de klankbordgroep en Beheergroep VWO die hebben bijgedragen aan het verwerken van de feedback.

## Wijzigingshistorie:

| Versie | Datum | Wijziging / Actie |
|---|---|---|
| 0.1 | 20-05-2018 | Opzet |
| | | Bespreking met leveranciers en gemeenten. |
| 0.2 | 17-06-2018 | Commentaar bespreking verwerkt. |
| | | Voorgelegd aan alle contactpersonen van gemeenten en leveranciers. |
| 0.99 | 30-07-2018 | Commentaar Leveranciers en Gemeenten verwerkt. |
| 1.00 | 01-08-2018 | Voorpublicatie IBD website – Ter vaststelling aangeboden aan het College van Dienstverlening. |
| 1.09 | 07-11-2018 | Versie aangepast na consultatie gemeenten en leveranciers.<br>Deze versie wordt voorgelegd aan toetsgroep. |
| 1.10 | 15-11-2018 | Versie aangepast op basis van beslissing toetsgroep d.d. 12-11-2018 |
| 1.11 | 30-11-2018 | Versie aangepast op basis van consultatie Beheergroep VWO (toetsgroep gemeenten en klankbordgroep leveranciers). |
| 2.0 | 28-03-2019 | Versie aangepast conform input Landsadvocaat en besluitvorming Beheergroep VWO. |
| 2.1 | 11-11-2019 | Versie 2.0 aangepast n.a.v. bijeenkomst Beheergroep VWO d.d. 10-10-2019. |
| 2.2 | 08-04-2020 | Versie 2.1 aangepast conform besluit Beheergroep VWO. |
| 2.3 | 19-11-2020 | Versie 2.2 aangepast conform besluit beheergroep VWO |
| 2.3-3 | 19-01-2021 | Versie 2.3-3 aangepast o.b.v. EDPB advies n.a.v. Schrems II |
| 2.4 | 12-04-2021 | Versie 2.3-3 aangepast conform besluit Beheergroep VWO |
| 2.41 | 15-12-2021 | Versie 2.4 aangepast conform besluit Beheergroep VWO |
| 2.42 | 15-08-2023 | Versie 2.42 aangepast conform besluit Beheergroep VWO |
| 2.5 | 15-02-2024 | Versie 2.42 aangepast conform besluit Beheergroep VWO |
| 2.51 | 18-06-2024 | Versie 2.5 aangepast conform besluit Beheergroep VWO |
| 2.52 | 06-01-2025 | Versie 2.51 aangepast conform besluit Beheergroep VWO |
| 2.53 | 15-12-2025 | Versie 2.52 aangepast conform besluit Beheergroep VWO |

## Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD. De IBD is ondergebracht bij VNG Realisatie.