

Modelovereenkomst Gegevensuitwisseling tussen Zelfstandige Verwerkingsverantwoordelijken op grond van uitvoering Hoofdovereenkomst

Toelichting bij modelovereenkomst gegevensuitwisseling tussen zelfstandige verwerkingsverantwoordelijken:

Titel: Hier zijn verschillende mogelijkheden. Meestal is er sprake van een gezamenlijke uitvoering van een wettelijke taak. Die samenwerking kan worden vormgegeven in een hoofdovereenkomst, een convenant, of in prestatie-, of samenwerkingsafspraken. Voor het gemak wordt hier hoofdovereenkomst gebruikt. Partijen kunnen hier een eigen keuze in maken.

Aanhef: Het kan zijn dat er meer dan twee partijen zijn. Voeg dan de naam van de partij en de vertegenwoordiger toe.

Overwegingen: het uitgangspunt is dat er een Hoofdovereenkomst aan deze overeenkomst ten grondslag ligt. In het geval er geen hoofdovereenkomst is, verwijst dan naar het document dat aan deze overeenkomst ten grondslag ligt.

- 1.1: De definities van art. 4 AVG hebben in deze overeenkomst dezelfde betekenis.
- 2.1: Het uitgangspunt is dat de overeenkomst ingaat op het moment dat de hoofdovereenkomst tot stand is gekomen. Partijen kunnen daar echter van afwijken. De ingangsdatum staat bij de ondertekening vermeld. Die datum is leidend. De ingangsdatum ligt in ieder geval voor het moment dat de verwerking, als bedoeld in artikel 3.2, wordt gestart.
- 6.1: Afspraken over beëindiging van deze overeenkomst horen 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 deze overeenkomst. Partijen kunnen ook kiezen om te verwijzen naar de GIBIT 2020, of delen daarvan overnemen.
- 7.1 Als er geen hoofdovereenkomst is, kunnen partijen verwijzen naar een ander onderliggend document, zoals een offerte. Over de rangorde van documenten maken partijen nadere afspraken.

Ondertekening: als er meer dan twee partijen zijn, vul dit onderdeel dan aan met deze partijen.

2.6 Toelichting bijlagen

Bijlage 1:

Tabel 1: In het eerste deel wordt ingevuld:

- Welke verwerking: zie hiervoor: <https://www.informatiebeveiligingsdienst.nl/product/vooringevuld-verwerkingsregister-gemeenten/> Kolom 'H'.
- Verwerkingsdoeleinden, zie hiervoor: <https://www.informatiebeveiligingsdienst.nl/product/vooringevuld-verwerkingsregister-gemeenten/> 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 persoonsgegevens:

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

Doorgifte derde landen

Als persoonsgegevens worden doorgegeven naar (of toegankelijk zijn in) een land buiten de EER moet dat hier worden aangegeven.

Doorgifte-instrument

Als er sprake is van een verwerking buiten de EER moet aangegeven worden welk doorgifte-instrument wordt gebruikt. De 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).

Volgens de aanbevelingen van de EDPB n.a.v. de Schrems II uitspraak van het Hof van Justitie van de EU ([Recommendations 01/2020, d.d. 10 november 2020](#)) moeten aanvullende maatregelen genomen worden als gebruik wordt gemaakt van doorgifte-instrument 3 – 6. Zo wordt nl. een aan de AVG gelijkwaardig beschermingsniveau bewerkstelligd (zie Bijlage 2 van de EDPB aanbevelingen).

Hieronder een voorbeeld :

Naam verwerking/Welke dienst en/of product	Verwerkings-doeleinden	Categorieën van betrokkenen	(Bijzondere) persoonsgegevens	Doorgifte naar derde landen	Doorgifte instrument	Aanvullende maatregelen (indien)

						van toepassing)
Xxxxxxsite CMS	" - identificatie binnen de applicatie - content kunnen plaatsen - registreren nieuwsbrief abonnees - reactiemogelijkheid op content (bv vacature)"	Gebruiker van de dienstverlening (medewerkers en inwoners)	NAW / Gebruikersnaam en wachtwoord / emailadres / telefoonnummer / pasfoto / politieke partij	Nee		
Xxxform	"Benodigd om bepaalde diensten te kunnen afnemen. Bijvoorbeeld het doorgeven van een verhuizing"	Gebruiker van de dienstverlening (bezoeker website)	NAW / BSN / Overige formuliergegevens (afhankelijk van uitvraag)	Nee		

Tabel 2: hier wordt ingevuld:

- Wie zijn (ook buiten kantooruren!) de contactpersonen van de verwerkingsverantwoordelijken.

Bijlage 2:

Bijlage 2 is een praktische uitwerking van artikel 32 AVG. Dus partijen geven hier aan welke passende technische en organisatorische maatregelen zij hebben 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. En 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 BIO maar, indien een partij 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 partij dit kan aantonen. Hierbij zijn diverse mogelijkheden aan te kruisen. Het is aan desbetreffende partij om te beoordelen of deze verantwoording voldoende is voor de betreffende verwerking en ook aan deze partij 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 een partij aangeven of deze is aangesloten bij een goedgekeurde gedragscode.

Modelovereenkomst Gegevensuitwisseling tussen Zelfstandige Verwerkingsverantwoordelijken op grond van uitvoering Hoofdovereenkomst>

Gemeente <naam gemeente>, waarvan de Gemeenteraad als opdrachtgever, de verwerkingsverantwoordelijke is, verder te noemen Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door de <heer of mevrouw> <persoonsnaam>, <functie>

en

Opdrachtnemer <Naam organisatie>, gevestigd te <plaatsnaam>, KVK-nummer <nummer> 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 <titel hoofdovereenkomst>, hierna naam Hoofdovereenkomst/, afgesloten,
- b) Partijen zullen ter uitvoering van de hiervoor vermelde <taken/afspraken> Persoonsgegevens verwerken;
- c) Op de verwerking van Persoonsgegevens door Partijen zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing;
- d) Partijen zijn ieder Verwerkingsverantwoordelijke als bedoeld in artikel 4, aanhef en onder 7, AVG voor de verwerkingen die zij uitvoeren;
- e) 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.
- f) Partijen willen in aanvulling op de AVG en de UAVG de volgende afspraken vastleggen over de verwerking van Persoonsgegevens;

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 het uitvoeren van onderzoek in het kader van jaarcontrole.
- 3.2 Iedere Partij vult de door haar uit te voeren leveringen aan de andere Partij in tabel 1 van Bijlage 1 in.

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.

Conform de AVG heeft de opdrachtnemer geen toegang tot "verboden" persoonsgegevens, tenzij

wettelijk anders bepaald. Opdrachtgever zal in het kader van rechtmatigheidsonderzoeken de persoonsgegevens van kwetsbare groepen en bij verboden persoonsgegevens medewerking aan opdrachtnemer geven door versleuteling van de persoonsgegevens toe te passen, waardoor deze niet herleidbaar is tot personen.

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 wissing van Persoonsgegevens.
Voor het bewaren van verzamelde persoonsgegevens houden partijen de bewaartermijn aan van: <wettelijke bewaartermijn?> Aldert: doorgaans 7 jaren.
Bij verwijdering van de verzamelde persoonsgegevens biedt de opdrachtnemer deze altijd kosteloos aan de opdrachtgever. Daarna kunnen de persoonsgegevens volledig worden verwijderd uit de bestanden van de opdrachtnemer.
Bij het beëindigen van de overeenkomst levert de opdrachtgever de verzamelde persoonsgegevens binnen 1 maand volledig kosteloos terug aan de opdrachtgever, tenzij de opdrachtnemer gebonden is aan een wettelijke bewaartermijn.
- 6.2 De geheimhouding geldt ook nog na beëindiging van deze Overeenkomst.

Artikel 7 Overige bepalingen

- 7.1 Op deze Overeenkomst s 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 en bevoegde rechter aanwijzen (forumkeuze).
- 7.2 Deze Overeenkomst maakt onlosmakelijk deel uit van de Hoofdovereenkomst.

Ondertekening

Aldus overeengekomen en ondertekend,

Ingangsdatum: <.....>

Gemeente <naam gemeente>
namens deze: <naam, functie>

<Naam organisatie>
namens deze: <naam, functie>

plaats: < >

plaats: < >

datum: < >

datum: < >

VOORBEELD

Bijlage 1: Overzicht van te verwerken persoonsgegevens

1. Iedere Partij vult de cyclus van de levering van Persoonsgegevens in.

Levering/verstrekking van persoonsgegevens, doeleinden categorieën van betrokkenen, soort persoonsgegevens en eventuele doorgifte naar derde landen.

Verstrekking/ levering	Verwerkings- doeleinden	Grondslag	Categori- eën van Betrokke- nen	Categorieën Persoons- gegevens (waaronder bijzondere persoons- gegevens)	Doorgifte naar derde landen	Doorgifte- instrument	Aanvullende maatregelen (indien van toepassing)
Toelichting: aangeven dat het om de leveringen van A->B en van B->A gaat							

2. Contactgegevens <Opdrachtgever>

Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)	Naam: <per gemeente invullen> Contactgegevens:
--	---

Contactgegevens <Opdrachtnemer>

Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)	Naam: Contactgegevens:
--	---------------------------

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

Bijlage 2: Aantonen passend niveau van beveiliging

NB: Iedere Partij vult Bijlage 2 in voor de verwerkingen waar de partij verantwoordelijk is.

- ☐ De verwerkingsverantwoordelijke 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.
- ☐ De verwerkingsverantwoordelijke werkt volgens een algemeen erkende overheidsnorm zoals de BIO, of vergelijkbaar, te weten:,
- ☐ De verwerkingsverantwoordelijke werkt volgens een andere norm, te weten:

Toereikendheid

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

- ☐ Certificering 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

- ☐ Verwerkingsverantwoordelijke is aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode, te weten