

Verwerkersovereenkomst uitvoering <naam hoofdovereenkomst>

Het college van burgemeester en wethouders van <naam gemeente>, verder te noemen Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door de <heer of mevrouw> <persoonsnaam>, <functie>

en

<Bedrijf>, gevestigd te <plaatsnaam>, 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;

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 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 en geldt tot het moment dat Verwerker in overeenstemming met artikel 7.1 van deze Verwerkersovereenkomst de persoonsgegevens heeft teruggegeven en/of gewist.

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. Afwijking hiervan kan alleen als wettelijke verplichtingen of bindende uitspraken van de toezichthoudende autoriteit of een bevoegde rechter anders bepalen.
- 3.2 De door Verwerker uit te voeren verwerkingen staan uitputtend beschreven in tabel 1 van Bijlage 1 en/of de Hoofdovereenkomst.

Artikel 4

4.1 Beveiligingsmaatregelen

Verwerker zorgt voor passende technische en organisatorische maatregelen om de Persoonsgegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG en vermeld in Bijlage 2. Een passend beveiligingsniveau kan betekenen dat Verwerker aanvullende maatregelen moet nemen. Als objectief is vastgesteld dat Verwerker geen passend beveiligingsniveau heeft en Verwerkingsverantwoordelijke daarom uitdrukkelijk schriftelijk verzoekt, zullen Partijen in onderling overleg bepalen welke aanvullende beveiligingsmaatregelen Verwerker zal treffen.

4.2 Audits

Verwerker verleent alle benodigde medewerking aan audits, tenzij Verwerker door middel van certificering heeft aangetoond dat het beveiligingsniveau voldoende is. De kosten van deze controle 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 alleen conform de AVG buiten de Europese Economische Ruimte verwerken als hij daarvoor uitdrukkelijk schriftelijk toestemming heeft gekregen van Verwerkingsverantwoordelijke.

4.4 Geheimhouding

Personen die werken voor Verwerker, en Verwerker zelf, moeten de Persoonsgegevens waarmee zij werken geheimhouden, behalve als er een wettelijke uitzondering is. De personen die werken voor Verwerker 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 de verwerkersovereenkomst bekende subverwerkers vermeldt Verwerker in tabel 3 van Bijlage 1. Verwerker houdt na de start van de werkzaamheden Verwerkingsverantwoordelijke op de hoogte van de inschakeling van nieuwe Subverwerkers. Bij de inschakeling van Subverwerkers blijven artikel 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

Op verzoek van Verwerkingsverantwoordelijke werkt Verwerker altijd mee aan een gegevensbeschermingseffectbeoordeling (DPIA).

Artikel 5 Inbreuk in verband met Persoonsgegevens

- 5.1 Verwerker zal Verwerkingsverantwoordelijke zo snel mogelijk, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens. Verwerker vermeldt hierbij de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens en de categorie betrokkenen.
- 5.2 In geval van een Inbreuk neemt Verwerker zo snel mogelijk alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen.
- 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 Autoriteit Persoonsgegevens en/of Betrokkene.

Artikel 6

6.1 Aansprakelijkheid

Het aansprakelijkheidsartikel uit de Hoofdovereenkomst is van overeenkomstige toepassing voor schade, uit welke hoofde dan ook, ten aanzien van de verwerking van Persoonsgegevens. Als Partijen niets hebben geregeld over aansprakelijkheid in de Hoofdovereenkomst, zullen zij zich conformeren aan artikel 82 AVG.

6.2 Bestuurlijke boete

De aansprakelijkheid voor boetes opgelegd door de Autoriteit Persoonsgegevens regelen Partijen in de Hoofdovereenkomst. Als partijen hierover niets geregeld hebben in de Hoofdovereenkomst en de Autoriteit Persoonsgegevens een boete oplegt aan één partij, terwijl meer partijen toerekenbaar tekort zijn geschoten, zullen partijen naar rato van verwijtbaarheid de boete dragen.

Artikel 7 Beëindigen verwerkersovereenkomst

- 7.1 Partijen maken in de Hoofdovereenkomst afspraken over de beëindiging van de Hoofdovereenkomst en de daaruit voortvloeiende teruggave en wissing van Persoonsgegevens. De geheimhouding geldt ook nog na beëindiging van deze Verwerkersovereenkomst.

Artikel 8 Overige bepalingen

- 8.1 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.

Ondertekening

Aldus overeengekomen en in tweevoud ondertekend,

Ingangsdatum: <.....>

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

plaats: <.....>

datum: <.....>

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

plaats: <.....>

datum: <.....>

Bijlage 1 Overzicht van te verwerken persoonsgegevens**1. Naam verwerking, doeleinden, categorieën van betrokkenen, (bijzondere) persoonsgegevens en eventuele doorgifte naar derde landen**

Naam verwerking	Verwerkings-doeleinden	Categorieën van Betrokkenen	(Bijzondere) Persoonsgegevens	Doorgifte naar derde landen

2. Contactgegevens

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

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

3. Ingeschakelde subverwerkers

Naam en contactgegevens subverwerker	KvK-nummer	Uitbestede verwerkingen

Bijlage 2 Aantonen passend niveau van beveiliging

- ☐ Normenstelsel
 - ☐ De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk:
.....
.....
(vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS).
 - ☐ De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm zoals de BIG (of de BIR, BIO) of vergelijkbaar, namelijk:
.....
 - ☐ Anders, nl.
- ☐ De toereikendheid van de informatiebeveiliging blijkt uit de volgende certificering en verklaring van toepasselijkheid:
 - ☐ Periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II);
 - ☐ Een Assurance rapport van een auditor die is aangesloten bij NOREA;
 - ☐ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven:
.....

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.

Standaard Verwerkersovereenkomst Gemeenten

Handreiking



Versienummer

1.11

Versiedatum

30-11-2018

Versiebeheer

Het beheer van dit document berust bij VNG Realisatie.

Copyright

© 2018 Informatiebeveiligingsdienst (IBD). 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.

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 en de klankbordgroep 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
		Vorgelegd 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 College van Dienstverlening
1.09	07-11-2018	Versie aangepast na consultatie gemeenten en leveranciers. 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)

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 beheert de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) 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 gebruik maken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Doel

Gemeenten en leveranciers willen bij de uitvoering van hun taken, dan wel 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 de verwerkersovereenkomst is om het gemeenten en hun leveranciers makkelijker te maken om tot afspraken te komen over de verwerking van persoonsgegevens. Dit product bevat de gemeentelijke standaard voor een verwerkersovereenkomst. Deze standaard wordt gebruikt als aanvulling op een hoofdovereenkomst om op grond van de AVG (artikel 28.3 en 28.9) en/of de BRP (artikel 7 Besluit basisregistratie personen) nadere afspraken te maken en vast te leggen over de omgang met persoonsgegevens.

Beheer van deze standaard

Deze standaard verwerkersovereenkomst wordt beheerd door VNG-Realisatie.

Verbetervoorstellen kunnen door zowel gemeenten als leveranciers naar privacy@vng.nl worden gemaild. Iedere drie maanden zal de Beheergroep VWO (bestaande uit vertegenwoordigers van gemeenten en leveranciers), de verbetervoorstellen beoordelen en zo nodig verwerken in een volgende versie.

Hebt u vragen over het gebruik van deze standaard overeenkomst neem dan ook contact op met de IBD via 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 producten

- GIBIT;
- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG);
 - Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten;
 - Tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten;
- Voorbeeld Informatiebeveiligingsbeleid van de gemeente, H2.4.1;
- Inkoopvoorwaarden en informatiebeveiligingseisen;
- Toegang van externe partijen en inhuur;
- Handreiking Service Level Agreements;
- Geheimhoudingsverklaringen;
- Handleiding screening personeel;
- Contractmanagement;
- Responsible Disclosure.

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Maatregel 6.2.1.5 Afsluiten bewerkersovereenkomst

Maatregel 6.2.1.6 Vastleggen beveiligingsmaatregelen in contracten

Maatregel 6.2.1.7 Rapporteren over naleving van afspraken

Vereniging van Nederlandse Gemeenten

Nassaulaan 12
2514 JS Den Haag

November 2018

Inhoud

1.	Inleiding.....	11
2.	Toelichting.....	13
2.1	Is er wel een verwerkersovereenkomst nodig?	13
2.2	Gezamenlijke verantwoordelijkheid en vertrouwen	13
2.3	Over welke onderwerpen moeten afspraken gemaakt worden?	13
2.4	Artikelsgewijze toelichting.....	14

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 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 maar dat het in veel gevallen niet lukt om tot een sluitende overeenstemming te komen. De IBD ondersteunt sinds de oprichting in 2103 gemeenten en ontvangt veel vragen en opmerkingen over afspraken met leveranciers en andere derde partijen. Deze vragen hebben geleid tot acties van de IBD:

- 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 verantwoordelijken en verwerkers.

Deze acties hebben enig effect gehad, maar nog steeds ontbreken in veel gevallen sluitende afspraken. Opdrachtgevers en opdrachtnemers, verantwoordelijken en verwerkers achten 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 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 (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 status quo 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 heldere kaders over de verwerking van persoonsgegevens.

Gemeenten én 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 een toetsgroep met vertegenwoordigers van 13 gemeenten (CISO's, FG's en inkopers). Het IBD-model van verwerkersovereenkomst diende als basis voor de 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.

2. Toelichting

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 Verwerkingsverantwoordelijke of verwerker.

2.2 Gezamenlijke 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 maar dat is niet noodzakelijk.

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 er wordt omgegaan 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

Onderwerp	Waar geregeld in verwerkersovereenkomst
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 geeft persoonsgegevens terug na afloop verwerking	Art. 2.1 en 7.1

2.4 Artikelsgewijze toelichting

Aanhef

De verwerkersovereenkomst wordt gesloten door de verwerkingsverantwoordelijke. Dat is over het algemeen het college van B&W, maar dat kan ook de burgemeester, de gemeenteraad, of de gemeentelijke rekenkamer zijn. Vul in welk bestuursorgaan verwerkingsverantwoordelijk is.

Overwegingen:

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

Artikelen:

- 1.1: De definities van art. 4 AVG hebben in deze verwerkersovereenkomst dezelfde betekenis.
- 2.1: De verwerkersovereenkomst gaat in op het moment dat de hoofdovereenkomst ingaat of, als bij de ondertekening een ingangsdatum is ingevuld op de ingevulde datum. De einddatum is op het moment dat de teruggave en/of wissing van de persoonsgegevens heeft plaatsgevonden. Nadere afspraken daarover worden in de hoofdovereenkomst gemaakt (zie artikel 7.1).
- 3.1: -
- 3.2: In Bijlage 1, tabel 1 moeten partijen de uit te voeren verwerkingen ('Naam verwerking') vermelden. Verwerker mag alleen de hier ingevulde verwerkingen daadwerkelijk uitvoeren.
- 4.1: De verwerkingsverantwoordelijke en de verwerker dienen passende en aantoonbare technische en organisatorische maatregelen te nemen om er zo voor te zorgen dat de in tabel 1 van Bijlage 1 vermelde persoonsgegevens goed zijn beveiligd. De verwerker dient aan te tonen hoe de systemen zijn beveiligd. De verwerker vult hiertoe Bijlage 2 in. Een 'passend beveiligingsniveau' kan betekenen dat de verwerker zelf het initiatief moet nemen om de beveiliging te verbeteren. Daarnaast kan ook de verwerkingsverantwoordelijke aan de verwerker opdragen om het beveiligingsniveau te verbeteren. Partijen treden hiertoe in overleg.

- 4.2: De verwerker is verplicht om mee te werken aan de uitvoering van een audit. Als de verwerker op basis van een certificering, of een recent auditrapport 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. 21.5 van de GIBIT. 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.
- 4.3: De verwerking van persoonsgegevens mag alleen binnen de EER plaatsvinden. Daarvan mag worden afgeweken als de verwerkingsverantwoordelijke op grond van artikel 45 en 46 AVG uitdrukkelijk toestemming geeft.
- 4.4: Iedereen die voor de verwerker werkt, moet de persoonsgegevens waar hij/zij kennis van kan nemen geheimhouden. 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. Als de verwerker een persoon inhurt voor bepaalde werkzaamheden, hoeft dat niet automatisch te betekenen dat er sprake is van een subverwerker. 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.
- 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.

- 4.7: Partijen zullen in onderling overleg de gevolgen, de uitvoering, de termijn van uitvoering van de DPIA en de kosten die daarmee zijn gemoeid bepalen. Wil je hier toch vooraf concrete afspraken over maken, neem ze dan op in de hoofdovereenkomst.
- 5.1: Het is belangrijk dat de verwerker de gemeente zo snel mogelijk op de hoogte brengt van een (vermoedelijke) inbreuk. Het gaat er daarbij om dat verwerker de verwerkingsverantwoordelijke direct informeert zodra er iets vreemds gebeurt met een geautomatiseerd systeem dat persoonsgegevens verwerkt. Partijen vertrouwen er daarbij op dat de verwerker professioneel genoeg is om een inschatting te maken van het incident. 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 dit onderzoek 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 dit 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 Autoriteit Persoonsgegevens begint te lopen, zodra de verwerkingsverantwoordelijke kennis heeft genomen van de inbreuk. 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.
- Ten behoeve van de uiteindelijke melding aan de Autoriteit Persoonsgegevens verstrekt de verwerker alle hem beschikbare informatie aan de Verwerkingsverantwoordelijke zoals vermeld op het formulier van Meldloket van de Autoriteit Persoonsgegevens.
- 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 de Informatiebeveiligingsdienst (IBD). De IBD zal in zo'n geval meteen de betrokken gemeenten informeren.
- 5.2: -
- 5.3: --
- 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. Mochten de afspraken in de hoofdovereenkomst onvoldoende zijn, adviseren we u dringend een addendum op de hoofdovereenkomst overeen te komen. Als dit allebei niet gebeurt, is gewoon art. 82 AVG van toepassing waarin niets is geregeld over de beperking van de aansprakelijkheid. Veel leveranciers, zeker de kleinere, zullen niet akkoord gaan met zo'n onbeperkte aansprakelijkheid. Dit kan tot gevolg hebben dat er geen Verwerkersovereenkomst wordt afgesloten, waardoor er geen enkele afspraak is over hoe verwerkers met persoonsgegevens om moeten gaan.

6.2: Verwerkers dienen er rekening mee te houden dat indien de oorzaak van een inbreuk te wijten is aan de verwerker, de toezichhoudende autoriteit direct een boete kan opleggen aan de verwerker. Net zoals de betrokkene zich in zo'n geval rechtstreeks kan richten tot de verwerker voor schadevergoeding. Als partijen geen afspraken hieromtrent in de hoofdovereenkomst hebben gemaakt geldt artikel 6.2 tweede zin.

7.1: --

8.1: -

Bijlagen

Bijlage 1:

Tabel 1: Hier wordt ingevuld:

- Welke verwerking
- Verwerkingsdoeleinden
- Categorieën van betrokkenen: is er sprake van kwetsbare groepen zoals kinderen, mensen met een beperking, e.d.
- Bijzondere persoonsgegevens: worden er bijzondere persoonsgegevens verwerkt zoals gezondheidsgegevens, gegevens m.b.t. ras of etnische afkomst, politieke opvattingen, etc.
- Is er sprake van doorgifte naar derde landen: zo ja dan moet de verwerkingsverantwoordelijke daarvoor eerst toestemming geven. Indien deze toestemming er is, moet de verwerker dat vermelden in de tabel.
- Hoog risico: als er sprake is van een hoog risico voor betrokkene, vullen partijen dat hier in.

Tabel 2: Hier wordt ingevuld:

- Wie zijn (ook buiten kantooruren!) de contactpersonen van de verwerkingsverantwoordelijke, de verwerker en de IBD.

Tabel 3: Hier wordt ingevuld:

- Indien er sprake is van subverwerkers, dan vult verwerker dat hier in. Verwerker zorgt dat vanaf de start van de verwerkersovereenkomst inzichtelijk is welke subverwerkers zijn ingeschakeld.

Bijlage 2:

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 BIG of straks de BIO 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. Het is aan de verwerkingsverantwoordelijke om te beoordelen of deze verantwoording voldoende is voor de betreffende verwerking en leverancier en ook om actief te controleren of aan deze paragraaf van de bijlage gevolg wordt gegeven.

Voor meer informatie over hoe u kunt bepalen of een certificaat valide is, kunt u de IBD factsheet over [Assurance](#) lezen. Als er bij de verwerking sprake is van een DigiD-aansluiting bekijk dan voor het invullen van bijlage 2 de Norea-guidance DIGID ([Handreiking DidiD-assesments 2.0](#))