VERWERKERSOVEREENKOMST DRECHTSTEDEN

IBD model versie 2.0

Voorblad Verwerkersovereenkomst Drechtsteden

De Verwerkersovereenkomst Drechtsteden is de standaard verwerkersovereenkomst zoals deze binnen de Drechtsteden wordt gebruikt; en is overeenkomstig met het landelijke model van de VNG/IBD. Deze verwerkersovereenkomst wordt gebruikt als **aanvulling** op een hoofdovereenkomst om op grond van de AVG nadere afspraken te maken én vast te leggen over de omgang met persoonsgegevens.

In dit voorblad worden puntsgewijs een aantal zaken behandeld:

1. Wat is een Verwerkersovereenkomst?
2. Het proces van het afsluiten van een verwerkersovereenkomst
3. Aandachtspunten voor het gebruik van deze verwerkersovereenkomst
4. Registratie van de verwerkersovereenkomst

Tevens is aan het einde van het document de uitgebreide toelichting van de VNG op de verwerkersovereenkomst te vinden. Zowel de toelichting als dit voorblad dienen **niet** opgenomen te worden in de uiteindelijk te tekenen overeenkomst.

1. Wat is een Verwerkersovereenkomst?

Aldus artikel 3, lid 3, AVG moet er wanneer een verwerking van persoonsgegevens wordt verricht door een derde partij, namens een Verwerkingsverantwoordelijke, hier een overeenkomst of andere rechtshandeling voor afgesloten worden met de Verwerker. In deze overeenkomst dienen onder andere afspraken te worden gemaakt omtrent het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke.

Verwerker – Verwerkingsverantwoordelijke?
Verwerkingsverantwoordelijke: De partij die, alleen of samen met anderen, het doel van de verwerking en de middelen voor de verwerking vaststelt.
Verwerker: Een derde partij, die ten behoeve van de verwerkingsverantwoordelijke, persoonsgegevens verwerkt, zonder dat deze aan diens rechtstreekse gezag is onderworpen.

Dit betekent dus dat een afdeling van dezelfde organisatie geen verwerker is, die vallen immers onder diens rechtstreekse gezag. De praktijk wijst uit dat er nogal wat discussie kan ontstaan over wie aan te merken valt als verwerker en verwerkingsverantwoordelijke. De Informatiebeveiligingsdienst (IBD) heeft hier een factsheet[1] voor ontwikkeld. Mocht dit nog geen volledige duidelijkheid verschaffen, kan er bij het JKC advies ingewonnen worden.

Ook wanneer een externe partij zelf (mede)verwerkingsverantwoordelijke is, en geen verwerker, is het aan te raden afspraken te maken over de omgang met, en beveiliging van, persoonsgegevens. Ook hierover kan er bij het JKC advies ingewonnen worden

2. Het proces

Binnen de Drechtsteden wordt de Verwerkersovereenkomst Drechtsteden gebruikt. In principe wordt deze verwerkersovereenkomst voorgelegd aan, en afgesloten met, Verwerkers. Echter kan het in voorkomende gevallen ook zijn dat de Verwerker een eigen verwerkersovereenkomst voorlegt. Dit geniet absoluut niet de voorkeur, maar is (nog) wel een mogelijkheid. Dit zit zo: zoals eerder gesteld is de Verwerkersovereenkomst Drechtsteden overeenkomstig met het landelijke model van de IBD/VNG. Op dit moment geldt voor deze landelijke (standaard) overeenkomst dat dit de verplichte standaard is met een pas toe of leg uit variant. Vanaf 1-1-2020 wordt dit naar alle waarschijnlijkheid een volledige verplichting, daar de gemeenten deze verplichting aan zichzelf hebben opgelegd (middels de VNG).

De eerste voorwaarde voor het kunnen afsluiten van een verwerkersovereenkomst is dat de Basis Risico Analyse Drechtsteden (BRA) uitgevoerd moet zijn. De BRA is een korte risicoanalyse om de risico's van een proces te bepalen, en daarmee het vereiste beveiligingsniveau. Hoe hoger de score uit de BRA, hoe hoger het af te spreken informatiebeveiligingsniveau waaraan de verwerker moet voldoen. Ook kun je de daarmee de basisrisco's op het gebied van privacy bepalen. Deze risicoanalyse vul je als proceseigenaar in, samen met een of meerdere materiedeskundigen, en onder begeleiding van ofwel het PIO-D lid, ofwel de Privacy Coördinator van je organisatie. De ingevulde BRA dien je op te sturen naar een van de CISO's (Chief Information Security Officer).

[1] https://www.informatiebeveiligingsdienst.nl/product/factsheet-en-beslismodel-verwerkingsverantwoordelijke-of-verwerker/

De BRA is te vinden op Mozaïek en op de SID-pagina Privacy & AVG. De resultaten van deze BRA bepalen de informatiebeveiligingseisen die aan de Verwerker opgelegd worden. De CISO's geven op basis van de ingevulde BRA advies hoe deze door te vertalen is naar de op te leggen eisen. Tevens kan er uit de BRA komen dat er een zogeheten PIA, Privacy Impact Assessment, uitgevoerd moet worden. Neem in dergelijke gevallen contact op met je Privacy Coördinator.

Nu de BRA is ingevuld, en de informatiebeveiligingseisen duidelijk zijn, is het zaak om deze te verwerken in de verwerkersovereenkomst. Dit kan ofwel in de Verwerkersovereenkomst Drechtsteden, ofwel in de door de Verwerker aangeleverde verwerkersovereenkomst. Nog even ter herhaling: het geniet absoluut de voorkeur om de Verwerkersovereenkomst Drechtsteden te gebruiken!

In het geval dat de Verwerkersovereenkomst Drechtsteden gebruikt wordt, kan deze na het verwerken van de informatiebeveiligingseisen voorgelegd worden aan de Verwerker. Als deze verder geen aanpassingen nodig acht, kan er getekend worden. In het geval deze wel aanpassingen wilt, kan je deze laten toetsen door het JKC. Waar nodig zal het gesprek met de Verwerker verder aangegaan moeten worden om tot een gezamenlijk akkoord te komen. Wanneer dit bereikt is, zal er getekend kunnen worden.

In het geval dat een door de Verwerker opgestelde verwerkersovereenkomst wordt gebruikt, doorloop je in principe hetzelfde pad: Laat de overeenkomst toetsen door het JKC en vul de informatiebeveiligingseisen aan op basis van de ingevulde BRA. Hierbij nogmaals de opmerking dat dit niet de voorkeur geniet, en in de toekomst mogelijkerwijs ook niet meer zal mogen (zie eerste alinea van punt 2).

Let tevens op dat de juiste persoon de verwerkersovereenkomst ondertekent! Ook dit kan voorgelegd worden aan het JKC.

3. Aandachtspunten Verwerkersovereenkomst Drechtsteden

Deze standaard verwerkersovereenkomst is het compromis tussen verschillende partijen, waaronder gemeenten en marktpartijen, om te komen tot een beter afsluitbare overeenkomst. Om het afsluiten verder te bevorderen en discussie te voorkomen zijn er enkele onderwerpen verplaats naar de hoofdovereenkomst. Draag er dus zorg voor dat deze onderwerpen worden opgenomen in de Hoofdovereenkomst! De onderwerpen zijn:

A. Wanneer eindigt de overeenkomst?
B. Wat gebeurt er met de gegevens wanneer de overeenkomst wordt beëindigd?
C. De aansprakelijkheidsregeling tussen beide partijen

Hierbij de kanttekening dat de deze standaard met name gericht is op **nieuwe** verwerkingen waar nog geen hoofdovereenkomst onder ligt. Moet er een verwerkersovereenkomst worden afgesloten voor een **bestaande** verwerking waar al een hoofdovereenkomst onder ligt, **neem bovenstaande punten dan alsnog op in de verwerkersovereenkomst**.

N.B.: Reeds bestaande (afgesloten) verwerkersovereenkomsten hoeven niet naar dit nieuwe model aangepast te worden.

4. Registratie van de verwerkersovereenkomst

Alle afgesloten verwerkersovereenkomsten dienen opgeslagen en geregistreerd te worden. Neem hiervoor contact op met de Privacy Coördinator van jouw organisatie.

Win voor al het bovenstaande advies in bij het JKC. Dit kan door te bellen naar 078 770 8036, of stel je vraag via het **contactformulier.**

Verwerkersovereenkomst uitvoering <naam hoofdovereenkomst>

Gemeente <naam gemeente>, verder te noemen Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door de <heer of mevrouw> <persoonsnaam>, <functie>

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);

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.
2.2 Deze Verwerkersovereenkomst eindigt op het moment dat Verwerker de verwerking van Persoonsgegevens op grond van de Hoofdovereenkomst heeft beëindigd.

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. Afwijking hiervan kan alleen als wettelijke verplichtingen of bindende uitspraken van de toezichthoudende autoriteit of een bevoegde rechter anders bepalen, of 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 in kennis stellen, tenzij deze kennisgeving om gewichtige redenen van algemeen belang is verboden.
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 over de nakoming van de afspraken binnen deze Verwerkersovereenkomst en Bijlagen, tenzij Verwerker door middel van certificering heeft aangetoond dat Verwerker de gemaakte afspraken nakomt. 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 buiten de Europese Economische Ruimte verwerken als hij daarvoor uitdrukkelijk schriftelijk toestemming heeft gekregen van Verwerkingsverantwoordelijke.

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 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 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 zo snel mogelijk, 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 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 toezichthoudende autoriteit en/of Betrokkene.

Artikel 6 Aansprakelijkheid

6.1 Eventuele in de Hoofdovereenkomst overeengekomen beperkingen van 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.

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, soort persoonsgegevens en eventuele doorgifte naar derde landen.

Naam verwerking	Verwerkings-doeleinden	Categorieën van Betrokkenen	Soort Persoonsgegevens (waaronder 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	Toepassing

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.

Toelichting

1.1. 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.

1.2. 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.

1.3. 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
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

1.4. Artikelsgewijze toelichting

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 de verwerkingsverantwoordelijk is.

Overwegingen:

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.

2.2: De einddatum is op het moment dat de verwerker de verwerking van de persoonsgegevens op grond van de hoofdovereenkomst heeft beëindigd. Nadere afspraken daarover worden in de hoofdovereenkomst gemaakt (zie artikel 7.1).

3.1: Indien een schriftelijke instructie van de verwerkingsverantwoordelijke naar het oordeel van de verwerker in strijd is met de AVG of de UAVG, zal de verwerker de verwerkingsverantwoordelijke hierover onmiddellijk informeren.

3.2: In Bijlage 1, tabel 1 moeten partijen de uit te voeren verwerkingen (‘Naam verwerking’) vermelden. De 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 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 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. Partijen maken vooraf afspraken over frequentie en overleggen van kopieën. Als DigiD wordt gebruikt bij de verwerking, moet de verwerker jaarlijks een TPM overleggen aan de verwerkingsverantwoordelijke. 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. Als de verwerker toestemming krijgt van de verwerkingsverantwoordelijke om de persoonsgegevens buiten de EER te verwerken moet er in ieder geval een adequaatheidsbesluit zijn van de Europese Commissie, dan wel moet er sprake zijn van passende maatregelen en moeten betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken, zoals bedoeld in artikel 46 AVG.

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 inhuurt 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. Als partijen hier vooraf concrete afspraken over maken, nemen ze deze op in de hoofdovereenkomst.

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 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 toezichthoudende autoriteit 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 toezichthoudende autoriteit 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.

5.4: 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 partijen daarin afspraken hebben gemaakt over beperking van de aansprakelijkheid dan gelden die ook voor de standaard VWO.

1.5. Toelichting bijlagen

Bijlage 1:

Tabel 1: In het eerste deel wordt ingevuld:

- Welke verwerking
- Verwerkingsdoeleinden
- 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

  - Soort persoonsgegevens: dit zijn voorbeelden van persoonsgegevens:
  - Contactgegevens beperkt (naam, e-mailadres, telefoonnummer)
  - Contactgegevens uitgebreid(NAW gegevens, geboortedatum, titulatuur e.d,)
  - BSN
  - Identificatienummer
  - Geslacht
  - Nationaliteit
  - Strafrechtelijke gegevens
  - Kopie identiteitsbewijs
  - Betalingsgegevens
  - Schulden
  - Salarisgegevens
  - Arbeidsrelatiegegevens
  - Beeldmateriaal
  - Locatiegegevens
  - IP-adres
  - Inloggegevens
  - Bijzondere persoonsgegevens:
  - Ras of etnische afkomst
  - Politieke opvattingen
  - Religieuze of levensbeschouwelijke overtuigingen
  - Lidmaatschap van een vakbond
  - Genetische gegeven
  - Biometrische gegevens
  - Gezondheidsgegevens
  - Seksueel gedrag of seksuele gerichtheid,
  - 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.

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 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.