0. Vooraf

Deze toelichting maakt onderdeel uit van de standaardverwerkersovereenkomst van de VNG die de gemeente Arnhem hanteert. De toelichting is inhoudelijk gelijk aan de toelichting in het format van de VNG, alleen de layout verschilt.

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 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 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 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 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 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. 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, eerste lid
Doorgifte naar derde landen	Art. 4, derde lid
Vertrouwelijkheid	Art. 4, vierde lid
Passende technische en organisatorische maatregelen	Art. 4, eerste lid

Inschakeling subverwerkers	Art. 4, vijfde lid
Verwerker verleent bijstand bij verzoeken van betrokkene	Art. 4, zesde lid
Verwerker verleent bijstand bij nakoming	art. 32 t/m 36 Art. 4, eerste lid / 5 / 4, zevende lid
Verwerker wist persoonsgegevens of geeft deze na afloop verwerking terug	Art. 2, eerste lid en 7, eerste lid

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, 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. 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 nader te maken afspraken verwijzen wij naar de GIBIT 2020 :
Aansprakelijkheid : artikel 13
Exit-strategie : artikel 20.14 en artikel 22
Audit : artikel 21

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 9.3 van de GIBIT 2020.

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.

<u>Artikelen</u>:
1, eerste lid: De definities van art. 4 AVG hebben in deze verwerkersovereenkomst dezelfde betekenis.
2, eerste lid: 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, tweede lid: Dit lid moet in samenhang met artikel 7, eerste lid worden gelezen.

3, eerste lid: 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, tweede lid: De verwerker mag alleen de in Bijlage 1, tabel 1 vermelde verwerkingen uitvoeren.

4, eerste lid: Een uit dit lid 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, tweede lid: 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. 21.5 van de GIBIT 2020. 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, derde lid: 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, vierde lid: 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, vijfde lid: 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, zesde lid: 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, zevende lid: 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, eerste lid: 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, derde lid: 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, vierde lid: 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, eerste lid: Afspraken over aansprakelijkheid t.a.v. de verwerking van persoonsgegevens, audits en de exit-strategie 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 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.

7, eerste lid: Afspraken over de exit-strategie, audits en de 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, 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 22 van de GIBIT 2020 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 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;-certificationmechanisms);
6. Ad hoc modelcontractbepalingen (ad hoc contractual clauses).

Toelichting bij standaard verwerkersovereenkomst gemeente Arnhem

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 - reactiemogelijk 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 verwerkingsverantwoordelijke, de verwerker en 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: 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:

Bijlage 2 is een praktische uitwerking van artikel 32 AVG. Dus verwerker geeft hier aan 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. 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 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 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.

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 2020 zijn de aansprakelijkheid, de exit-strategie en de uitvoering van audits wel geregeld. In Bijlage 3 staan de artikelen uit de GIBIT 2020 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!).