Brief aan de leden
T.a.v. het college en de raad

Datum
8 mei 2019

Ons kenmerk
VNGR/U201900370
Lbr. 19/033

Telefoon
070 - 373 8393

Bijlage(n)
1

Onderwerp
Gemeentelijke verwerkersovereenkomst verbindend per 1/1/2020

Samenvatting

Hierbij leggen wij u de standaard gemeentelijke verwerkersovereenkomst (VWO) voor ter besluitvorming. De ALV wordt gevraagd de VWO voor leden verbindend te verklaren. Tijdens de BALV van 30 november 2018 hebben de leden van de VNG ingestemd met het proces standaardverklaring. Met de besluitvorming in de ALV van 5 juni wordt voldaan aan vereiste ledenconsultatie in het proces standaardverklaring.

Gemeenten zijn op basis van de Algemene Verordening Gegevensbescherming (AVG) wettelijk verplicht een VWO af te sluiten met alle opdrachtnemers die namens hen persoonsgegevens verwerken. De VWO bevat een eenduidig pakket aan afspraken over het verwerken van persoonsgegevens tussen gemeenten als opdrachtgever en hun opdrachtnemers (ICT-leveranciers of partijen die diensten leveren).

Met de vaststelling van een eigen VWO kiezen wij als gemeenten voor uniforme afspraken over het verwerken van persoonsgegevens. Deze standaard is ontwikkeld door én voor gemeenten, in overleg met landelijke leveranciers. Uit een consultatie langs gemeenten in Nederland bleek dat veel gemeenten in een impasse zaten en daarmee niet aan de AVG voldoen. De standaard VWO lost dit probleem voor alle gemeenten in een keer op.

Zowel het College van Dienstverleningszaken als het bestuur van de VNG adviseren om de standaard verbindend te verklaren per 1 januari 2020. Tot aan deze datum geldt het principe van *'pas-toe-of-leg-uit'*. In de ledenbrief geven wij een toelichting op de totstandkoming, het beheer en het monitoren van de bijgevoegde standaard VWO.

Vereniging van Nederlandse Gemeenten
Nassaulaan 12 Den Haag | Postbus 30435 | 2500 GK Den Haag
070 - 373 83 93 | info@vng.nl

Aan de leden

Datum
8 mei 2019

Ons kenmerk
VNGR/U201900370
Lbr. 19/033

Telefoon
070 - 373 8393

Bijlage(n)
1

Onderwerp
Gemeentelijke verwerkersovereenkomst verbindend per 1/1/2020

Geacht college en gemeenteraad,

Hierbij leggen wij u de gemeentelijke verwerkersovereenkomst (VWO) voor als VNG-standaard volgens het principe van verplichtende zelfregulering. Het College van Dienstverleningszaken (CvD) en het bestuur van de VNG adviseren positief op dit voorstel dat tot stand gekomen is in samenwerking met gemeenten en leveranciers. In de Buitengewone Algemene Ledenvergadering van 30 november 2018 is het proces van standaardverklaring vastgesteld. Conform dit proces heeft het CvD, op voorspraak van de Taskforce Samen Organiseren en met instemming van de commissie Informatiesamenleving, positief geadviseerd over het opstellen van een standaard VWO voor gemeenten.

Aanleiding

Gemeenten zijn wettelijk verplicht om afspraken over het verwerken van persoonsgegevens te maken met hun opdrachtnemers. Deze afspraken worden vastgelegd in een VWO. De VWO regelt op een uniforme wijze de afspraken rondom de verwerking van persoonsgegevens en bevat slechts die zaken die niet al op een andere wijze zijn geregeld zoals bijvoorbeeld in de wet of in een hoofdovereenkomst. De toezichthouder, de Autoriteit Persoonsgegevens, kan gemeenten boetes opleggen bij het niet hebben van een VWO.

Iedere gemeente maakt gemiddeld met zo'n 50 partijen afspraken over de verwerking van persoonsgegevens. In de praktijk blijkt dat afspraken in ongeveer de helft van de gevallen ontbreken. Een inventarisatie van de Informatiebeveiligingsdienst (IBD) van VNG Realisatie wijst uit dat de hoofdredenen voor het ontbreken van afspraken zijn dat:

- Leveranciers vanwege het ontbreken van een standaard VWO voor gemeenten bij voorkeur hun eigen VWO hanteren.

Vereniging van Nederlandse Gemeenten
Nassaulaan 12 Den Haag | Postbus 30435 | 2500 GK Den Haag
070 - 373 83 93 | info@vng.nl

- Geen overeenstemming kan worden bereikt met leveranciers over zaken die wettelijk gezien thuishoren in andere overeenkomsten (zoals aansprakelijkheid).

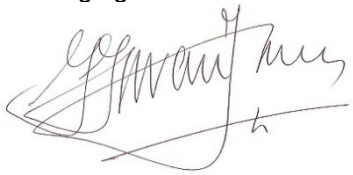
Voordelen van een standaard VWO
Het voordeel voor gemeenten is dat zij tijd en geld (juridisch advies en onderhandelingen) besparen en ontzorgd worden bij het maken van afspraken over het verwerken van persoonsgegevens. De VWO versterkt de positie van gemeenten als betrouwbare en voorspelbare partners voor hun leveranciers. Marktpartijen weten exact waar ze aan toe zijn wanneer ze persoonsgegevens voor of namens gemeenten verwerken. Een bijkomend voordeel van deze aanpak is dat bij geschillen over het gebruik van de VWO de VNG namens 355 gemeenten een standpunt kan bepalen en in gesprek kan gaan met leveranciers.

Proces van totstandkoming en betrokken stakeholders
De VWO is besproken met de Autoriteit Persoonsgegevens, die de ontwikkeling van dergelijke standaarden van harte toejuicht. Het document is tevens getoetst door de landsadvocaat.
De standaard is tot stand gekomen in een nauwe samenwerking tussen gemeenten, leveranciers en de VNG. Meerdere rondes van feedback en commentaar zijn verwerkt in de nu voorliggende standaard. Gemeenten en leveranciers kunnen op basis van het feitelijke gebruik verbetervoorstellen en wijzigingsverzoeken indienen. Een beheergroep bestaande uit inkopers, privacy-specialisten en beveiligingsspecialisten van gemeenten en leveranciers beoordeelt wijzigingsvoorstellen en adviseert het bestuur over mogelijke wijzigingen in de VWO. Zo blijft de standaard actueel en relevant. Het gebruik van de standaard door gemeenten wordt gemonitord door VNG Realisatie.

Verbindendverklaring van de standaard
De Taskforce Samen Organiseren, het CvD en het VNG-bestuur hebben positief geadviseerd over de VWO als standaard voor gemeenten, volgens het principe van verplichtende zelfregulering per 1 januari 2020. In de periode in aanloop naar deze datum geldt het principe van *'pas-toe-of-leg-uit'* in deze periode kunnen gemeenten en leverancier waardevolle ervaring opdoen met het werken met de standaard. Op 28 maart heeft de beheergroep een versie vastgesteld die geschikt is voor verbindendverklaring. Zo ontstaat landelijk een uniforme werkwijze en daarmee een effectieve en efficiënte werkwijze voor alle betrokkenen.

Meer informatie
In de bijlage is de handreiking VWO opgenomen. De meest actuele VWO en meer informatie is beschikbaar via: www.informatiebeveiligingsdienst.nl/vwo - De Informatiebeveiligingsdienst van VNG Realisatie heeft een helpdesk ingericht voor vragen over de VWO, de helpdesk is bereikbaar via privacy@VNG.nl.

Met vriendelijke groet,
Vereniging van Nederlandse Gemeenten



mr J.H.C. van Zanen
Voorzitter

INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie

Handreiking

Standaard Verwerkersovereenkomst Gemeenten

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Handreiking standaard verwerkersovereenkomst gemeenten

Versienummer
2.0

Versiedatum
05-04-2019

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

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

Wijzigingshistorie:

Versie	Datum	Wijziging / Actie
0.1	20-05-2018	Opzet
		Bespreking met leveranciers en gemeenten
0.2	17-06-2018	Commentaar bespreking verwerkt
		Voorgelegd aan alle contactpersonen van gemeenten en leveranciers
0.99	30-07-2018	Commentaar Leveranciers en Gemeenten verwerkt
1.00	01-08-2018	Voorpublicatie IBD website – Ter vaststelling aangeboden aan 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)
2.0	28-03-2019	Versie aangepast conform input Landsadvocaat en besluitvorming Beheergroep VWO

Over de IBD

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

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

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

Doel

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

Het doel van 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) nadere afspraken te maken en vast te leggen over de omgang met persoonsgegevens.

Rangorde

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

Beheer van deze standaard

Deze standaard verwerkersovereenkomst wordt beheerd door VNG-Realisatie/IBD. Verbetervoorstellen kunnen door zowel gemeenten als leveranciers naar privacy@vng.nl worden gemaild. Tweemaal per jaar zal de Beheergroep VWO (bestaande uit vertegenwoordigers van gemeenten en leveranciers), de verbetervoorstellen beoordelen en zonodig 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 documenten:

- GIBIT;
- Vanaf 2020: Baseline Informatiebeveiliging Overheid (BIO)
- Tot 2020: Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG);
- Tot 2020: Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten;
- Tot 2020: 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 en;
- 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

Inhoudsopgave

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 (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 heldere kaders over de verwerking van persoonsgegevens.

Partijen mogen in 2019 nog afwijken van de Standaard Verwerkersovereenkomst. Wel moeten zij dan uitleggen waarom zij dat doen (Pas-Toe-Of-Leg-Uit). Gemeenten moeten een eventuele afwijking van de standaard VWO in hun jaarrapportage vastleggen.

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 bestande 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. 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.

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
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

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.

2.5. 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.

3. Standaard verwerkersovereenkomst gemeenten

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.