

Gemeente Helmond



Standaard verwerkersovereenkomst

Colofon

Naam document

Standaard verwerkersovereenkomst gemeente Helmond

Versienummer

1.3

Versiedatum

12-01-2026

Versiebeheer

Het beheer van dit document berust bij de afdeling IVA/Team Regie, privacy & security.

Bron

Standaard verwerkersovereenkomst gemeenten, Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten, licentie onder: CC BY-NC-SA 4.0 (voor meer informatie: <http://creativecommons.org/licenses/by-nc-sa/4.0>).

Deze publicatie, waarvan de intellectuele eigendomsrechten niet bij de gemeente Helmond berusten, blijven onderworpen aan de beperkingen opgelegd door de IBD en / of de Vereniging van Nederlandse Gemeenten. Iedere kopie van dit document, of een gedeelte daarvan, moet zijn voorzien van deze mededeling.

Rechten en vrijwaring

De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Wijzigingshistorie:

Versie	Datum	Wijziging / Actie
0.1	24-10-2019	Eerste initiële opzet o.b.v. het standaard VWO model VNG/IBD, v2.0
0.2	30-11-2020	Aanpassing aan de nieuwe IBD-versie, 2.3 dd 26-11-2020
0.3	19-01-2021	Aanpassing aan de IBD-versie 2.3-3 i.v.m. privacy shield (EDPB advies n.a.v. Schrems II)
0.4	28-05-2021	Aanpassing aan de IBD-versie 2.4 i.v.m. aanpassing conform besluit Beheergroep VWO
0.5	18-01-2022	Aanpassing aan de IBD-versie 2.4.1 van 15-12-2022
0.6	04-08-2022	Aanpassing aan de IBD-versie 1.0 van 18-07-2022 m.b.t. de Wpg
0.7	24-01-2023	Aanpassing aan de IBD-versie 1.1 van 01-12-2022 m.b.t. aanpassing artikel 4.3
0.8	28-11-2023	Aanpassing aan de IBD-versie 1.2 van november 2023
0.9	01-02-2024	Verwijdering bijlage 3 met GIBIT 2020
1.0	15-03-2024	Aanpassing aan de IBD-versie 1.3 van maart 2024
1.1	15-07-2024	Aanpassing aan de IBD-versie 2.51 van juli 2024
1.2	23-04-2025	Aanpassing aan de IBD-versie 2.52
1.3	12-01-2026	Aanpassing bijlage 3

Toelichting

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 en Wpg nakomen. Daarbij willen Partijen uitgaan van wederzijds vertrouwen.

Het doel van de verwerkersovereenkomst is om het de gemeente Helmond en haar 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 artikel 28.3 en 28.9 AVG, alsmede artikel 6c lid 2 Wpg 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 het Security & Privacy Officers-team (SPO-team), conform de standaard verwerkersovereenkomst van VNG-Realisatie/IBD. Heeft u vragen over het gebruik van deze standaard overeenkomst neem dan contact op met de IVA/CIO via SPO@helmond.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 2020](#); (en klik vervolgens op 'GIBIT-Toolbox')
- [Baseline Informatiebeveiliging Overheid \(BIO\)](#);
- [Inkoopvoorwaarden en informatiebeveiligingseisen](#);
- [Handreiking Service Level Agreements](#);
- [Handreiking Geheimhoudingsverklaringen](#);
- [Handreiking Screening Personeel BIO](#).

In gebruik nemen standaard verwerkersovereenkomst

Bij de dienstverlening en bedrijfsvoering verwerkt de gemeente Helmond 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. Voor het vastleggen van deze afspraken wordt door de gemeente Helmond verplicht gebruik gemaakt van de door de VNG/IBD opgestelde standaard verwerkersovereenkomst.

Gemeenten én leveranciers

Bij het opstellen van de standaard verwerkersovereenkomst gemeenten door VNG/IBD 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.

Verwerkersovereenkomst uitvoering <naam hoofdovereenkomst>

Gemeente Helmond, waarvan <het college van Burgemeester en Wethouders/de Gemeenteraad/de burgemeester> de verwerkingsverantwoordelijke is, 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 en Politiegegevens voor Verwerkingsverantwoordelijke;
- c) Op de verwerking van Persoonsgegevens door Verwerker zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing;
- d) Op de verwerking van Politiegegevens door Verwerker zijn de Wet politiegegevens (Wpg) en het Besluit politiegegevens (Bpg) van toepassing;
- e) Partijen willen in aanvulling op de AVG en de UAVG en de Wpg en het Bpg de volgende afspraken over de verwerking van Persoonsgegevens en Politiegegevens vastleggen in deze verwerkersovereenkomst (hierna: de Verwerkersovereenkomst);

En komen het volgende overeen:

Artikel 1 Definities

- 1.1 Begrippen uit de AVG en de UAVG die in deze Verwerkersovereenkomst worden gebruikt, hebben dezelfde betekenis.
- 1.2 Begrippen uit de Wpg en het Bpg in deze Verwerkersovereenkomst worden gebruikt, hebben dezelfde betekenis.
- 1.3 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die onlosmakelijk 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 en Politiegegevens op grond van de Hoofdovereenkomst heeft beëindigd en de afspraken over het teruggeven en/of wissen van Persoonsgegevens en Politiegegevens zijn nagekomen.
- 2.3 Wanneer Partijen een (nieuwe) Verwerkersovereenkomst overeenkomen, betekent dat dat de oude Verwerkersovereenkomst komt te vervallen.

Artikel 3 Onderwerp van deze Verwerkersovereenkomst

- 3.1 Verwerker verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens en Politiegegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke voor de uitvoering van de Hoofdovereenkomst en uitsluitend overeenkomstig schriftelijke instructies van Verwerkingsverantwoordelijke, tenzij 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 zonder onredelijke vertraging in kennis stellen, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
Voor iedere verdere verwerking van persoonsgegevens die buiten de opdrachtverlening valt zoals

genoemd in tabel 1 van Bijlage 1, moet de verwerker vooraf uitdrukkelijk toestemming vragen aan de verwerkingsverantwoordelijke.

- 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 en Politiegegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG en in artikel 4a Wpg. 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 uitgevoerd door een gecertificeerde auditor over de nakoming van de afspraken binnen deze Verwerkersovereenkomst en Bijlagen, tenzij Verwerker door middel van een geldige certificering, die periodiek door een geaccrediteerde instelling wordt getoetst, heeft aangetoond dat Verwerker de gemaakte afspraken nakomt. De kosten van deze audit 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 buiten de Europese Economische Ruimte (laten) verwerken wanneer is voldaan aan de voorwaarden van artikel 45 of 46 AVG, en Politiegegevens wanneer is voldaan aan de voorwaarden van artikel 17a Wpg. Wanneer er sprake is van een verwerking buiten de EER, dan stelt Verwerker Verwerkingsverantwoordelijke daarvan vooraf op de hoogte.

4.4 Geheimhouding

Personen die werken voor (sub)Verwerker en (sub)Verwerker zelf, moeten Persoonsgegevens en Politiegegevens 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 de artikelen 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 en in artikel 24a t/m 25 en 28 Wpg, 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 en in artikel 4c en 33b Wpg.

Artikel 5 Inbreuk in verband met Persoonsgegevens

- 5.1 Verwerker zal Verwerkingsverantwoordelijke **zonder onredelijke vertraging**, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens en Politiegegevens. Verwerker vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie Persoonsgegevens en Politiegegevens, de categorie betrokkenen en het aantal betrokkenen.
- 5.2 In geval van een Inbreuk neemt Verwerker zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen en houdt de Verwerkingsverantwoordelijke hiervan voortdurend op de hoogte.
- 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. Verwerker ondersteunt de Verwerkingsverantwoordelijke waar nodig bij de melding aan de toezichthoudende autoriteit en/of Betrokkene.

Artikel 6 Aansprakelijkheid

- 6.1 Eventuele in de Hoofdovereenkomst overeengekomen beperkingen van de 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 en Politiegegevens.
- 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 Helmond

De burgemeester van Helmond

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	Categorieën Persoons gegevens en Politiegegevens (waaronder bijzondere persoons gegevens en bijzondere categorieën van Politiegegevens)	Verwerkings-locatie	Doorgifte instrument (indien van toepassing)	Aanvullende maatregelen (indien van toepassing)

1b. Verwerkingsactiviteiten politiegegevens

Verwerker biedt de technische middelen en ondersteuning aan de Verwerkingsverantwoordelijken ten behoeve van de verwerking van politiegegevens voor de volgende doeleinden:

- a. het houden van toezicht op naleving en handhaving van wetgeving door de Boa's binnen het kader van hun wettelijke opsporingstaken;
- b. het opsporen van strafbare feiten door de Boa's binnen het kader van hun wettelijke opsporingstaken;
- c. het verrichten van een concreet opsporingsonderzoek op verzoek van een officier van justitie;
- d. het samenwerken met andere bevoegde opsporingsinstanties binnen het kader van hun wettelijke taken;
- e. het samenstellen en op verzoek beschikbaar stellen van anonieme rapportages op basis van verwerkte gegevens;
- f. het verstrekken van Politiegegevens conform de Verstrekkingenwijzer Wpg voor Boa's, alsmede;
 - i. het informeren van de (direct)toezichthouders, (het samenwerkingsverband van) de werkgever en de desbetreffende Boa indien er sprake is van een klacht gericht tegen het optreden van een Boa;
 - ii. het verstrekken van gegevens ten behoeve van beleidsinformatie, wetenschappelijk onderzoek en statistiek aan daartoe gekwalificeerde onderzoekers of onderzoeksinstituten.

2. Contactgegevens

Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)	Naam: Contactgegevens: Tel: 140492
Contactpersoon Verwerker (NB: Ook buiten kantooruren)	Naam: Contactgegevens:
Contactgegevens IBD	Telefoonnummer 070-204 55 11 e-mailadres: privacy@vng.nl

3. Ingeschakelde subverwerkers

Naam en contactgegevens subverwerker	KvK-nummer	Uitbestede verwerkingen	Toepassing (geautomatiseerd systeem)	Verwerkingslocatie	Doorgifte instrument	Aanvullende maatregelen (indien van toepassing)

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

Toelichting bij 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 het Register van Verwerkingen.
- Verwerkingsdoeleinden, zie hiervoor het Register van Verwerkingen.
- Categorieën van betrokkenen: dit zijn voorbeelden van categorieën van betrokkenen:
 - o Aanvragers/Indieners
 - o Belanghebbenden
 - o Bestuurders/Raadsleden
 - o Ambtenaren gemeente
 - o Websitebezoekers
 - o Personeel leveranciers
 - o Scholieren
 - o Studenten
 - o Ouderen
 - o Gehandicapten
 - o Kinderen
- Categorieën van 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
Politiegegevens	Een persoonsgegeven, dat verwerkt wordt in het kader van de opsporingstaak. Hiervoor geldt de Wet politiegegevens (Wpg) . Een politiegegeven is een specifieke versie van een persoonsgegeven. Voor een boea zijn strafrecht en opsporing bepalende begrippen voor het werken 'onder' de Wpg.

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

- **Verwerkingslocatie**

Het moet duidelijk zijn waar de verwerking plaatsvindt. 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. Adequaateitsbesluit;
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).

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).

Op de volgende pagina wordt een voorbeeld weergegeven.

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	EER		
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 aanvraag)	EER		

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 en waar de gegevens worden verwerkt. Als een subverwerker de gegevens in een derde land verwerkt, moet deze aangeven wat het doorgifte instrument is en welke eventuele noodzakelijke aanvullende maatregelen zijn getroffen.

Bijlage 2: Aantonen passend niveau van beveiliging

Normenstelsel

- ☐ De verwerker werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten:
..... (vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS) en is volgens deze norm wel/niet gecertificeerd.
 - ☐ Datum laatste certificering:
- ☐ De verwerker werkt volgens een algemeen erkende overheidsnorm zoals de BIO, of vergelijkbaar, te weten:
.....
- ☐ De verwerker werkt volgens een andere norm, te weten:
.....

Toereikendheid

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

- ☐ Verwerker verstrekt een actueel en geldig certificaat en verklaring van toepasselijkheid (VVT);
- ☐ Rapportages van periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II);
- ☐ Een assurance rapport (TPM) van een auditor die is aangesloten bij NOREA;
- ☐ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven (in lijn met de aanpak uit hoofdstuk 4.4 uit de BIO, een ICV):
.....

NB: Uit de certificering/periodieke externe controles/audits of uit de eigen controles/beschrijvingen blijkt of kan afgeleid worden dat de beveiliging passend is bij de verwerking(en) genoemd in Bijlage 1.

Aansluiting bij goedgekeurde gedragscode

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

NB: Substantiële wijzigingen in het bovenstaande en achteruitgang van de voorwaarden geven partijen op korte termijn aan elkaar door.

Toelichting bij 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 echter, als 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 verstrekt¹¹ 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 de IBD factsheet over [assurance](#) lezen.

Verder kan de verwerker aangeven of deze is aangesloten bij een goedgekeurde gedragscode.

[\[1\]](#) *Hardcopy, via de mail, of via een link.*

Deze bijlage is facultatief: Alleen als bijlage opnemen als deze van toepassing is!

Bijlage 3: Relevante GIBIT 2020 artikelen

Artikel 13. Aansprakelijkheid

13.1 De partij die toerekenbaar tekortschiet in de nakoming van zijn verplichtingen, of jegens de ander onrechtmatig handelt, is tegenover de andere partij aansprakelijk voor de door deze aldus geleden en/of te lijden schade.

13.2 Voor zover nakoming niet reeds blijvend onmogelijk is, of de verbintenis voortvloeit uit onrechtmatige daad of strekt tot schadevergoeding, vindt lid 1 slechts toepassing met inachtneming van het bepaalde in artikel 20.9 omtrent verzuim.

13.3 De in lid 1 bedoelde aansprakelijkheid voor persoons- en zaakschade en daaruit voortvloeiende schade, is beperkt tot een bedrag van € 1.250.000,- per gebeurtenis. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.

13.4 De aansprakelijkheid voor overige schade is beperkt tot tien maal de Jaarvergoeding per gebeurtenis. De totale aansprakelijkheid per jaar bedraagt evenwel nooit meer dan twintig maal de Jaarvergoeding (ongeacht het aantal gebeurtenissen). Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.

13.5 De in dit artikel opgenomen beperkingen van aansprakelijkheid komen te vervallen:

- i) in geval van aanspraken van derden op schadevergoeding ten gevolge van dood of letsel en/of;
- ii) indien sprake is van opzet of grove schuld aan de zijde van de andere partij of diens Personeel; en/of
- iii) in geval van schending van intellectuele eigendomsrechten als bedoeld in artikel 17;
- iv) ten aanzien van door de toezichthoudende autoriteit opgelegde boetes:
 - 1. voor zover die boetes ook rechtstreeks aan de Leverancier hadden kunnen worden opgelegd, maar niet zijn opgelegd; en
 - 2. onder de voorwaarde dat Opdrachtgever Leverancier:
 - a) onverwijld schriftelijk informeert over een door een toezichthoudende autoriteit gestart onderzoek dat kan leiden tot een boete alsmede over en het bestaan en de inhoud van de opgelegde boete; en
 - b) Leverancier volledig betreft bij het voeren van verweer tegen die boete althans het aan Leverancier toe te rekenen deel van die boete.

13.6 Alle verplichtingen, ook die krachtens de belasting-, zorgverzekerings- en sociale verzekeringswetgeving met betrekking tot Personeel van Leverancier, komen ten laste van Leverancier. Leverancier vrijwaart Opdrachtgever tegen elke aansprakelijkheid die daarmee verband houdt. Op deze vrijwaring zijn de voorgaande beperkingen van aansprakelijkheid niet van toepassing.

Artikel 20. Opschorting, opzegging en ontbinding

Gevolgen van beëindiging

20.14 Leverancier retourneert of verwijdt bij het, op welke grond dan ook, eindigen van de Overeenkomst(en) onverwijld alle hem door Opdrachtgever ter hand gestelde documenten, boeken, bescheiden en andere zaken (waaronder begrepen gegevens- en informatiedragers). Bij vroegtijdige beëindiging geldt het voorgaande wederkerig.

Artikel 21. Controlerecht en medewerking audits bij Opdrachtgever

Controlerecht

21.1 Opdrachtgever is gerechtigd de naleving door Leverancier van de wezenlijke verplichtingen uit hoofde van de Overeenkomst, de GIBIT 2020 en de daarmee samenhangende overeenkomsten (SLA, verwerkersovereenkomst, etc.), alsmede de juistheid van toegezonden facturen, binnen een redelijke termijn door een onafhankelijke ter zake deskundige aan geheimhouding gebonden derde te laten controleren.

- 21.2 Opdrachtgever zal alvorens een controle te doen verrichten eerst Leverancier om de op grond van het vorige lid noodzakelijke informatie vragen.
- 21.3 De controle zal alleen plaatsvinden indien Opdrachtgever - ook na beantwoording van het in het vorige lid bedoelde verzoek om informatie - gerede twijfel heeft over de nakoming van de verplichtingen door Leverancier, of indien Opdrachtgever anderszins een gerechtvaardigd belang bij de controle heeft (o.m. wettelijke plicht, instructie toezichthouder).
- 21.4 Leverancier zal alle redelijkerwijs te verwachten medewerking verlenen aan een dergelijke controle. Leverancier zal in dat kader ten minste inzage verlenen in alle relevante gegevens en achtergrondinformatie die relevant kan zijn in het kader van voornoemde controle. Ook zal Leverancier toegang verlenen tot de locatie waar de diensten worden verleend.
- 21.5 Opdrachtgever staat er voor in dat de in het eerste lid bedoelde derde eventueel door Leverancier gehanteerde voorschriften zal opvolgen. Indien de controle niet (volledig) kan worden uitgevoerd vanwege voornoemde voorschriften, dan komt dit evenwel voor risico van Leverancier.
- 21.6 De kosten voor deze controle worden gedragen door Opdrachtgever (zowel eigen kosten als kosten van de Leverancier), tenzij de derde één of meer tekortkomingen van niet ondergeschikte aard van Leverancier constateert die ten nadele zijn van Opdrachtgever.

Medewerking audits bij Opdrachtgever

- 21.7 Voor zover Opdrachtgever afhankelijk is van Leverancier voor de uitvoering van (wettelijke verplichte) audits, zal Leverancier alle noodzakelijke medewerking verlenen aan de uitvoering van deze audits. De kosten voor deze medewerking worden gedragen door Opdrachtgever.

Artikel 22. Overstap, beperkte voortzetting, overdracht en verlengd gebruik

Exit-plan

22.1 Op eerste verzoek van Opdrachtgever zullen Partijen een exit-plan opstellen waarin wordt vastgelegd wat er dient te gebeuren ter voorbereiding op en uitvoering van de in dit artikel beschreven werkzaamheden. Artikel 5.2 en 5.3 zijn van overeenkomstige toepassing op het exit-plan.

22.2 De in dit artikel bedoelde werkzaamheden – te weten overstap (artikel 22.3 e.v.), beperkte voortzetting (artikel 22.6 e.v.), overdracht (artikel 22.8) en beperkte verlenging (artikel 22.9) – zullen worden verricht overeenkomstig het exit-plan en het bepaalde in de Overeenkomst en de GIBIT 2020, tegen de dan reguliere tarieven van Leverancier.

Overstap naar soortgelijke ICT Prestatie

22.3 Leverancier doet bij het, op welke grond ook beëindigen van de Overeenkomst(en), op eerste verzoek van Opdrachtgever datgene wat redelijkerwijs noodzakelijk is om er voor te zorgen dat een nieuwe leverancier of Opdrachtgever zelf zonder belemmeringen een soortgelijke ICT Prestatie ten behoeve van Opdrachtgever kan verrichten (zulks met uitzondering van de afgifte van de broncode van de Programmatuur).

22.4 Onder de in het vorige lid bedoelde redelijke maatregelen in het kader van de overstap naar een andere leverancier/ander systeem worden in ieder geval verstaan (naar keuze van Opdrachtgever):

- i) het alsnog aan de verplichtingen uit artikel 18 voldoen;
- ii) het vernietigen van de gegevens waarvoor Opdrachtgever verantwoordelijk is (tegen afgifte van bewijs van vernietiging);
- iii) het technisch ontvlechten en ontmantelen van (een deel van) de ICT Presentatie.

22.5 In afwijking van artikel 22.2 worden voornoemde diensten kosteloos verricht indien sprake is van een toerekenbaar tekortschieten door Leverancier. De onder sub 22.4ii) bedoelde werkzaamheden worden op verzoek hoe dan ook kosteloos verricht.

Beperkte voortzetting van ICT Prestatie

22.6 Leverancier verklaart zich reeds nu voor alsdan bereid bij beëindiging van de Overeenkomst(en) – op welke grond dan ook – op eerste verzoek van Opdrachtgever:

- i) een nieuwe ICT Prestatie of beperkte voortzetting van de bestaande ICT Prestatie te leveren waarmee

- Opdrachtgever in staat blijft de met de huidige ICT Prestatie opgeslagen gegevens te raadplegen; en
- ii) een beperkte vorm van Onderhoud te (blijven) verlenen op de in het vorige lid bedoelde ICT Prestatie (namelijk binnen de kaders van de in het vorige lid bedoelde beperkte functionaliteit).
- 22.7 Voor de duur en kosten voor de in het vorige lid bedoelde ICT Prestatie geldt dat:
- i) de duur ten minste een zodanige duur is dat Opdrachtgever aan de wettelijke administratieplichten kan voldoen;
- ii) de kosten voor in redelijke verhouding staan tot de oorspronkelijke kosten voor de gehele ICT Prestatie (naar rato van de verminderde functionaliteit), met dien verstande dat noodzakelijke verlengingen van Derdenprogrammatuur volledig kunnen worden doorbelast.

Overdracht ICT Prestatie

22.8 Opdrachtgever is gerechtigd de ICT Prestatie geheel of gedeeltelijk, inclusief alle daarbij behorende Gebruiksrechten en alle aanspraken in het kader van Onderhoud, onder gelijkblijvende voorwaarden (waaronder begrepen gelijkblijvende omvang Gebruiksrechten) over te dragen aan een gemeenschappelijke regeling of andere entiteit met een publieke functie in het kader van een uitbesteding van een deel van de activiteiten van Opdrachtgever. Leverancier zal alle noodzakelijke medewerking verlenen aan voornoemde overdracht. Leverancier is niet gerechtigd voor de overgang als zodanig kosten in rekening te brengen, wel voor eventueel aanvullend te verrichten werkzaamheden. Derdenprogrammatuur is alleen overdraagbaar voor zover de wet of de toepasselijke licentievoorwaarden daaraan niet in de weg staan (vgl. artikel 19.5).

Verlengd gebruik

22.9 Leverancier verklaart zich voorts bereid om Opdrachtgever desgewenst toe te staan het gebruik van de ICT Prestatie na de beëindigingsdatum voor een redelijke periode te verlengen, indien de werkzaamheden overeenkomstig het Exit-plan niet tijdig zijn afgerond. Hiervoor zal een vergoeding in rekening worden gebracht naar rato van de laatst geldende gebruiksvergoedingen (waarbij noodzakelijke verlengingen van Derdenprogrammatuur volledig kunnen worden doorbelast), tenzij de niet-tijdige afronding van de Exit-werkzaamheden toerekenbaar is aan Leverancier (de verlenging is dan gratis).

Toelichting bij 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!).