Verwerkersovereenkomst

Gemeente Utrecht, verder te noemen Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door....

en
..... verder te noemen Verwerker, hierbij rechtsgeldig vertegenwoordigd door ...

hierna afzonderlijk te noemen “Partij”, of gezamenlijk “Partijen”

Overwegen het volgende:
a) Partijen hebben op 19-03-2021 de raamovereenkomst afgesloten, op grond waarvan Verwerker de volgende dienst(en) levert aan de Verwerkingsverantwoordelijke:
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;

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.

Gemeente Utrecht

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 Als Verwerker een (vermoedelijke) beveiligingsinbreuk, datalek of ander beveiligingsincident ontdekt, neemt hij onmiddellijk maatregelen om nadelige gevolgen van de beveiligingsinbreuk of het datalek zoveel mogelijk te voorkomen en/of te herstellen.

5.2 De Verwerker meldt (vermoedelijke) beveiligingsinbreuken, datalekken of andere beveiligingsincidenten betreffende de persoonsgegevens waarop deze overeenkomst ziet, onmiddellijk doch uiterlijk binnen 24 uur na eerste ontdekking, aan de Verantwoordelijke (via de website van de gemeente Utrecht: Product - Beveiligingslek of datalek melden - Online loket (utrecht.nl). Verwerker geeft daarbij direct aan wat de aard van de inbreuk of lek is, welke maatregelen hij heeft getroffen, zal treffen en voorstelt te treffen om de gevolgen van de inbreuk of lek te verhelpen of zoveel mogelijk te beperken.

5.3 De melding zoals bedoeld in artikel 6.2 vindt plaats via de procedure voor het melden van datalekken zoals omschreven op www.utrecht.nl/privacy.

5.4 Verwerker zal verder op het eerste verzoek van de Verantwoordelijke alle (aanvullende) inlichtingen verschaffen die de Verantwoordelijke noodzakelijk acht om het incident te kunnen

beoordelen. Daarbij verschaft Verwerker in ieder geval de volgende informatie aan de Verantwoordelijke:

a. wat de (vermeende) oorzaak is van de inbreuk;
b. wat het (vooralsnog bekende en/of te verwachten) gevolg is;
c. wat de (voorgestelde) oplossing is;
d. contactgegevens voor de opvolging van de melding;
e. aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
f. een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
g. het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
h. de datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen de inbreuk heeft plaatsgevonden);
i. de datum en het tijdstip waarop de inbreuk bekend is geworden bij Verwerker of bij een door hem ingeschakelde derde of onderaannemer;
j. of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
k. wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.

5.5 De Verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van inbreuken en zal de Verantwoordelijke, op diens verzoek, inzage verschaffen in het plan. Verwerker stelt de Verantwoordelijke op de hoogte van materiele wijzigingen in het plan van aanpak.

5.6 De Verwerker zal het doen van meldingen aan de toezichthouder(s) overlaten aan de Verantwoordelijke, voor zover deze zien op de verwerking waarop deze overeenkomst ziet.

5.7 De Verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen waarin minimaal de informatie zoals bedoeld in artikel 6.4 is opgenomen, en geeft daar op eerste verzoek van de Verantwoordelijke inzage in.

5.8 Verwerker zal aan Verantwoordelijke waar mogelijk medewerking verlenen bij het opstellen van een beschrijving van de geconstateerde beveiligingsinbreuken en datalekken en de vermoedelijke gevolgen daarvan voor de verwerking van persoonsgegevens ten behoeve van de meldplicht van Verantwoordelijke.

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: 8 februari 2021

Gemeente Utrecht
namens deze**:**

plaats: Utrecht

datum: <……>

Bedrijfsnaam
namens deze:

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)	Classificatie gegevens	Doorgifte naar derde landen

2. **Contactgegevens**

Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)	Naam:
Contactpersoon Verwerker (NB: Ook buiten kantooruren)	Naam:
Contactgegevens IBD	Telefoonnummer

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 BIO, NCSC richtlijnen
□ Anders, nl. ……..

Toereikendheid

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

□ Certificering 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 (bijv. Norea)
……

Algoritme

De verwerker zend een lijst van algoritmes die gebruikt worden voor het verwerken van (persoons)gegevens aan de DISO van Stadsbedrijven DISO.STADSBEDRIJVEN@utrecht.nl .

- Omschrijving van het proces / verwerking
  - Wat is de rol van het algoritme of voorspellend model binnen het proces?
  - Geeft het algoritme of voorspellend model informatie of neemt het zelfstandig een besluit?

Niet noodzakelijke gegevens

Alle persoonsgegevens dat niet noodzakelijk zijn voor verwante deelprocessen / handelingen en/of archiefwaardig zijn, worden direct geanonimiseerd.

Toegankelijkheid en cookies

Database encryptie op persoonlijke gegevens
Wachtwoord - alleen instelbaar door gebruiker
Wachtwoord – hashing
Wachtwoord - sterkte afdwingen

Wachtwoord – verloop
Two factor authentication

Alleen gebruik maken van noodzakelijke functionele cookies ten behoeve van een juist gebruik van de applicatie. Overige cookies zijn automatisch uitgeschakeld.

Versleutelde connectiviteit:
A of A+ rating conform de test standaarden : SSL Server Test (Powered by Qualys SSL Labs)
IPv6 on default

Artikelgewijze 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 verwerkingsverantwoordelijke 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: 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

2.2: Dit artikel moet in samenhang met artikel 7.1 worden gelezen.

3.1: 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.

3.2: De verwerker mag alleen de in Bijlage 1, tabel 1 vermelde verwerkingen uitvoeren.

4.1: Een uit artikel 4.1 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.

4.2: 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.

4.3: Als de Europese Commissie een adequaatheidsbesluit heeft genomen t.a.v. de verwerking in een derde land, of door een internationale organisatie, is voor de verwerking in dat desbetreffende derde land, of door deze internationale organisatie, geen toestemming nodig van de verwerkingsverantwoordelijke (art. 45 AVG). Als er geen adequaatheidsbesluit is afgegeven en het derde land toch passende waarborgen biedt en betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken, mag een verwerking van persoonsgegevens daar toch plaatsvinden (artikel 46 AVG). Als hieraan wordt voldaan op grond van de in artikel 46 AVG genoemde instrumenten, is toestemming hiervoor van de verwerkingsverantwoordelijke ook niet vereist.
Wel moet de verwerker de verwerkingsverantwoordelijke in alle gevallen vooraf op de hoogte stellen van een verwerking in een land buiten de EER, dan wel door een internationale organisatie.

4.4: 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. 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.

4.6: 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.
Voor wat betreft eventuele kosten die hiermee gepaard gaan: zie § 2.4.

4.7: 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.

5.1: 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 de 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 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. **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.

5.4: 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, 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.

7.1 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 geeft onder andere een manier aan. Partijen kunnen er voor kiezen om deze exit-strategie te volgen.

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.

BD factsheet over assurance lezen.