Convenant

inzake
de verwerking van Persoonsgegevens

De ondergetekenden

De publiekrechtelijke rechtspersoon gemeente Heemskerk zetelende te Heemskerk aan het Maerten van Heemskerckplein 1, ten deze rechtsgeldig vertegenwoordigd Ralph de Vries, handelend ter uitvoering van het besluit van het college van Burgemeester en Wethouders van Gemeente Heemskerk hierna te noemen: '**gemeente**',

en

BDO Audit & Assurance B.V. gevestigd en kantoorhoudend aan de dr. Holtroplaan 23; 5652XR te Eindhoven, ten deze rechtsgeldig vertegenwoordigd door Jeroen Brak, hierna te noemen: '**contractspartij**',

hierna gezamenlijk te noemen 'partijen',

overwegende dat:

- Partijen zijn op 5 juli 2021 de Hoofdovereenkomst Accountantsdiensten aangegaan vanwege het verrichten van de volgende opdracht: Accountantsdienstverlening. Partijen Verwerken daarbij Persoonsgegevens die vermeld staan in Bijlage 1 van dit Convenant;
- Partijen zijn – vanwege het uitvoeren van deze opdracht en met betrekking tot de Persoonsgegevens die partijen hierbij Verwerken – aan te merken als zelfstandig Verwerkingsverantwoordelijken. In dit Convenant liggen wederzijdse rechten en verplichtingen vast voor de Verwerking van Persoonsgegevens.

komen het volgende overeen:

Artikel 1: Definities
In dit Convenant wordt verstaan onder:

a. AVG: Algemene verordening gegevensbescherming, alsmede de uitvoeringswet van deze verordening.
b. Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.
c. Convenant: dit Convenant inzake de Verwerking van Persoonsgegevens.
d. Datalek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot - of waarbij redelijkerwijs niet uit te sluiten valt dat die kan leiden tot - de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins Verwerkte Persoonsgegevens.
e. Derden: Anderen dan partijen.
f. Hoofdovereenkomst: de overeenkomst waaruit de opdracht en/of samenwerking voortvloeit van partijen.
g. Meldplicht: de verplichting tot het melden van Datalekken aan de Autoriteit Persoonsgegevens en (in sommige gevallen) aan Betrokkene(n).
h. Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
i. Verwerken: elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

j. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens Verwerkt.
k. Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt.

Artikel 2: Geheimhoudingsplicht

1. Personen in dienst van, dan wel werkzaam ten behoeve van de contractspartij, evenals de contractspartij zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht. De medewerkers van de contractspartij tekenen hiertoe een geheimhoudingsverklaring.
2. Indien de contractspartij op grond van een wettelijke verplichting gegevens dient te verstrekken, verifieert de contractspartij de grondslag van het verzoek en de identiteit van de verzoeker. De contractspartij informeert de gemeente onmiddellijk, voorafgaand aan de verstrekking ter zake, tenzij wettelijke bepalingen dit verbieden.

Artikel 3: Rechten van Betrokkenen

Als een betrokkene een beroep doet op zijn rechten zoals genoemd in artikel 12 t/m 22 AVG, helpt Contractspartij de gemeente om daarop binnen de wettelijke termijnen een beslissing te nemen.

Artikel 4: Technische en organisatorische beveiligingsmaatregelen

Partijen zorgen voor passende technische en organisatorische maatregelen om de Persoonsgegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG en vermeld in Bijlage 2.

Artikel 5: Melding Datalekken en beveiligingsincidenten

1. Partijen informeren elkaar zo spoedig mogelijk – doch uiterlijk binnen 24 uur na de eerste ontdekking – over alle inbreuken op de beveiliging die betrekking hebben op werkzaamheden zoals in de hoofdovereenkomst vastgelegd en die op grond van de AVG en/of wet- en regelgeving moeten worden gemeld aan de Autoriteit Persoonsgegevens. Partijen gebruiken de contactgegevens in Bijlage 1.
2. Partijen bepalen in het voorkomende geval dat er een Datalek heeft plaatsgevonden gezamenlijk welke partij blijkend uit handelen de meest logische is om het Datalek te melden bij de Autoriteit Persoonsgegevens. Melding bij de Autoriteit Persoonsgegevens wordt uitsluitend gedaan als uit aard en omvang van het Datalek blijkt dat de Meldplicht van toepassing is.
3. Lid 2 is tevens van toepassing op de Meldplicht aan Betrokkene(n).

Artikel 6: Aansprakelijkheid

1. Indien de contractspartij tekortschiet in de nakoming van een verplichting uit dit Convenant kan de gemeente hem in gebreke stellen. De contractspartij is echter onmiddellijk in gebreke als de nakoming van deze verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan de contractspartij een redelijke termijn wordt gegund om alsnog haar verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is de contractspartij in verzuim. De in de Hoofdovereenkomst en daarbij behorende algemene voorwaarden overeengekomen beperking van aansprakelijkheid is van kracht op de verplichtingen zoals opgenomen in dit Convenant, met dien verstande dat een of meerdere schadevorderingen uit hoofde van dit Convenant en/of de Hoofdovereenkomst nimmer tot overschrijding van de beperking kan leiden.

Artikel 7: Duur en beëindiging van het Convenant

1. Dit Convenant treedt in werking op de datum waarop de Hoofdovereenkomst van kracht is en eindigt op moment dat partijen de Hoofdovereenkomst beëindigen. Het is niet mogelijk om dit Convenant tussentijds op te zeggen.
2. Zodra de Hoofdovereenkomst is beëindigd, zal de contractspartij naar keuze van de gemeente:
   a. alle of een door de gemeente bepaald gedeelte van haar in het kader van dit Convenant ter beschikking gestelde Persoonsgegevens aan de gemeente ter beschikking stellen; of
   b. de Persoonsgegevens die hij van de gemeente heeft ontvangen op alle locaties vernietigen, in welke vorm dan ook en toont dit aan, tenzij partijen iets anders overeenkomen.

   De gemeente kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen een nader overeen te komen redelijke termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.
3. De contractspartij waarborgt te allen tijde het in het vorig lid beschreven recht op overdraagbaarheid van gegevens conform artikel 20 van de AVG, zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.
4. Partijen treden met elkaar in overleg over wijzigingen in dit Convenant als een wijziging in regelgeving of een wijziging in de uitleg van regelgeving daartoe aanleiding geven.

Artikel 8: Toepasselijk recht

Op dit Convenant en op alle geschillen die daaruit voortvloeien of daarmee samenhangen, is Nederlands recht van toepassing.

Aldus overeengekomen in tweevoud op 5 juli 2021

Gemeente Heemskerk	BDO Audit & Assurance B.V.
Ralph de Vries, Griffier	Jeroen Brak, Partner

Bijlage 1 Overzicht van te verwerken persoonsgegevens

1. Naam verwerking, doeleinden, categorieën van betrokkenen, (bijzondere) persoonsgegevens en eventuele doorgifte naar derde landen

Naam verwerking	**Verwerkings-doeleinden**	**Categorieën van Betrokkenen**	**(Bijzondere) Persoonsgegevens**	**Doorgifte naar derde landen**
<< in te vullen door beide partijen>>				

2. Contactgegevens

Contactpersoon Gemeente Heemskerk	H.H. Hogendoorn CISO/PO E-mail: privacy@heemskerk.nl Tel.: 0251 256 802 (schakelt door naar mobiel)
Contactpersoon BDO Audit & Assurance	Naam: afdeling QRM & Legal (informatiebeveiliging en privacy) Emailadres: privacy@bdo.nl Telnr.: 040-2698111

Bijlage 2 Aantonen passend niveau van beveiliging

BDO ICT voldoet voor de beveiliging van haar organisatie en infrastructuur aan de internationaal erkende standaard voor informatiebeveiliging: de norm ISO 27001. De norm is van toepassing op de ICT-processen: informatie, informatiesystemen, netwerken, en op het IT-personeel dat de bedrijfsprocessen ondersteunt.

Door het regelmatig uitvoeren van informatiebeveiligingscontroles en van in- en externe audits blijft het informatiebeveiligingsniveau van BDO hoog. BDO heeft alle beheersmaatregelen geselecteerd vanuit risicoanalyses en uit de baselines/beleid. Alle maatregelen uit de norm ISO 27001 zijn geïmplementeerd en de audits zijn uitgevoerd door BDO IT audit en BSI.

Het afschrift het ISO 27001 certificaat en bijbehorende verklaring van toepasselijkheid kunnen worden opgevraagd bij de afdeling QRM & Legal via eerdergenoemd emailadres.

De basis voor deze certificering ligt in het informatiebeveiligings- en privacybeleid van BDO. Dit beleid zorgt ervoor dat de organisatie van BDO blijft voldoen aan de norm ISO 27001. Verantwoordelijk hiervoor is de afdeling Quality & Riskmanagement. Een team van Information Security & Privacy Officers is verantwoordelijk voor het rapporteren over beveiligingsincidenten en relevante ontwikkelingen op het gebied van informatiebeveiliging en privacy aan het multidisciplinair samengestelde Forum Informatiebeveiliging binnen BDO.

Binnen het informatiebeveiligingsbeleid van BDO zijn verschillende beheersmaatregelen actief die zijn onderverdeeld in onderstaande categorieën:
- Beveiliging van de fysieke ICT-omgeving;
- Ontwikkeling en onderhoud van informatiesystemen;
- Beheer van bedrijfsmiddelen;
- Medewerkers;
- Beveiligde applicaties en toepassingen;
- Leveranciersrelaties;
- Beheer van informatiebeveiligingsincidenten.