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 door [invullen naam door Heemskerk], handelend ter uitvoering van het besluit van het college van Burgemeester en Wethouders van Gemeente Heemskerk hierna te noemen: '**gemeente**',

en

[invullen opdrachtnemer], gevestigd en kantoorhoudend te [Postcode, plaats en straat + nummer], ten deze rechtsgeldig vertegenwoordigd door [In te vullen door contractspartij], hierna te noemen: '**contractspartij**',

hierna gezamenlijk te noemen 'partijen',

overwegende dat:

- Partijen zijn op [datum] de Hoofdovereenkomst met [Naam en kenmerk overeenkomst] aangegaan vanwege het verrichten van de volgende opdracht: ["onderliggende opdracht"]. 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 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.

2. De contractspartij is aansprakelijk op grond van het bepaalde in artikel 82 van de AVG, voor schade of nadeel voortvloeiende uit het niet nakomen van dit Convenant, daaronder begrepen wanneer bij de Verwerking niet wordt voldaan aan de specifiek tot verwerkingsgerichte verplichtingen van de AVG, of buiten de rechtmatige instructies van de gemeente is gehandeld.
3. De contractspartij vrijwaart de gemeente voor schade of nadeel voor zover ontstaan door werkzaamheid van de contractspartij.
4. Indien de contractspartij de in artikel 5.1 neergelegde verplichting niet of niet-tijdig nakomt en de toezichthouder de gemeente daarvoor een bestuurlijke boete oplegt, is de contractspartij
   aansprakelijk en legt de gemeente een contractuele boete ter hoogte van hetzelfde bedrag op aan de contractspartij. Deze boete is niet vatbaar voor verrekening en opschorting en laat de rechten van de gemeente op nakoming en schadevergoeding onverlet.

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 [datum]

Gemeente Heemskerk	[invullen opdrachtnemer]
[Naam + functie]	[Naam + functie]

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 [Contractspartij]	Naam: [In te vullen door contractspartij] Emailadres: [In te vullen door contractspartij] Telnr.: [In te vullen door contractspartij]

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 Baseline Informatiebeveiliging Overheid (BIO) of vergelijkbaar, namelijk: [In te vullen door contractspartij]
  - Anders, nl.: [In te vullen door contractspartij]

- 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: [In te vullen door contractspartij]

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.