Gemeente Amsterdam

Verwerkersovereenkomst in het kader van …….. tussen

Gemeente Amsterdam

en

<naam opdrachtnemer/Verwerker>

Bijlage bij Hoofdovereenkomst ……..

d.d. <datum>

Versie 23 jan. 2018 voor het IVMO

Verwerkersovereenkomst

Verwerkersovereenkomst van de gemeente Amsterdam bij **<naam Hoofdovereenkomst>** conform de Algemene Verordening Gegevensbescherming (AVG)

De gemeente Amsterdam, gevestigd te Amstel 1 te Amsterdam, verder te noemen Verwerkingsverantwoordelijke, ten deze rechtsgeldig vertegenwoordigd door de heer/mevrouw **<naam bevoegde ondertekenaar>, <functie ondertekenaar> van de <rve en afdelingsnaam/ stadsdeel>,**

en

<Bedrijf, afdeling>, gevestigd te <plaatsnaam>, verder te noemen Verwerker, ten deze rechtsgeldig vertegenwoordigd door de **<de heer of mevrouw>, <persoonsnaam> , <functie>,**

Hierna gezamenlijk te noemen: Partijen.

Overwegende dat:

- Verwerkingsverantwoordelijke met Verwerker op **< XX >** een overeenkomst met nummer **< XX** > met betrekking tot **< XX >** heeft gesloten, hierna: de Hoofdovereenkomst;
- Verwerker in het kader van de uitvoering van de Hoofdovereenkomst persoonsgegevens in de zin van artikel 4, onder 1 , van de Algemene Verordening Gegevensbescherming (AVG) (EU 2016/679) verwerkt;
- het college van Burgemeester en Wethouders van de gemeente Amsterdam en/of de Burgemeester Verwerkingsverantwoordelijke is of zijn voor de verwerking van persoonsgegevens;
- de **<naam organisatorische eenheid**> van de gemeente Amsterdam namens Verwerkingsverantwoordelijke belast is met het beheer van de binnen de **< naam van de organisatorische eenheid>** verwerkte persoonsgegevens;
- Partijen ter voldoening aan de AVG (in aanvulling op de Hoofdovereenkomst beschreven afspraken) in deze Verwerkersovereenkomst afspraken over het verwerken van de persoonsgegevens door Verwerker wensen vast te leggen;
- Partijen overeenkomen om bij het verwerken van deze persoonsgegevens de hierna volgende bepalingen in acht te nemen:

KOMEN OVEREEN:

Artikel 1. Definities

1.1 Autoriteit persoonsgegevens: de Autoriteit als bedoeld in artikel 51 van de AVG.

1.2 Betrokkene: degene op wie een persoonsgegeven betrekking heeft.

1.3 Verwerker: degene die ten behoeve van Verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

1.4 Bijlagen: aanhangsels bij deze overeenkomst, die onlosmakelijk deel uitmaken van deze overeenkomst.

1.5 Datalek: Een inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4, onder 12, van de AVG. Een inbreuk in verband met persoonsgegevens is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van, of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens

1.6 Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de Betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch de personen die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd zijn om persoonsgegevens te verwerken.

1.7 Hoofdovereenkomst: de overeenkomst, waarin afspraken over de door Verwerker als opdrachtnemer te verrichten dienstverlening zijn gemaakt.

1.8 Normen en standaarden: de door Verwerkingsverantwoordelijke vastgestelde normen en standaarden ter zake van methoden, technieken, procedures, projecten, productiekenmerken en documentatievoorschriften welke bij de uitvoering van de werkzaamheden door Verwerker zullen worden gevolgd als vastgelegd in de Hoofdovereenkomst of in een bijlage bij deze Verwerkersovereenkomst.

1.9 Ontvanger: degene aan wie de persoonsgegevens worden verstrekt.

1.10 TPM: third party mededeling: een verklaring die afgegeven wordt door een onafhankelijke auditpartij over de kwaliteit van de ICT dienstverlening en beheersing van de organisatie.

1.11 Verwerkingsverantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

1.12 Verstrekken van persoonsgegevens: het bekend maken of ter beschikking stellen van persoonsgegevens.

1.13 Verwerken/verwerking van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Artikel 2. Onderwerp en duur van deze overeenkomst

2.1 Deze Verwerkersovereenkomst is een onlosmakelijk onderdeel van de Hoofdovereenkomst. Ingevolge de Hoofdovereenkomst verricht Verwerker de navolgende dienstverlening **< XX >**.

2.2 Deze Verwerkersovereenkomst heeft als doel dat Partijen voldoen aan de verplichtingen die voortvloeien uit de AVG, waaronder de verplichting van Verwerkingsverantwoordelijke om zorg te dragen dat Verwerker voldoende garanties biedt met betrekking tot het toepassen van passende technische- en organisatorische maatregelen opdat de verwerking aan de vereisten van de AVG voldoet en de bescherming van betrokkenen is gewaarborgd.

2.3 Deze Verwerkersovereenkomst gaat in op het moment van ondertekening. Pas nadat Verwerker naar het oordeel van Verwerkingsverantwoordelijke genoegzaam heeft aangetoond, dat hij heeft voldaan aan de verplichtingen als omschreven in de artikelen 3.12 tot en met 3.14 van deze Verwerkersovereenkomst (vernietigen/ overdragen van persoonsgegevens aan Verwerkingsverantwoordelijke), eindigt deze Verwerkersovereenkomst.

2.4 Verplichtingen die naar hun aard bestemd zijn om ook na de beëindiging van deze Verwerkersovereenkomst voort te duren, blijven gelden. Tot deze verplichtingen behoren onder meer de bepalingen betreffende geheimhouding, aansprakelijkheid, boete en toepasselijk recht.

2.5 De navolgende Bijlagen maken onlosmakelijk deel uit van deze Verwerkersovereenkomst:

Bijlage I	Omschrijving van te verwerken persoonsgegevens (dataset) en de werkzaamheden van de verwerker.
Bijlage II	De door Verwerker te implementeren technische beveiligingsnormen en standaarden van Verwerkingsverantwoordelijke en de te nemen organisatorische maatregelen.
Bijlage III	Inlichtingen om (mogelijke) Datalekken te beoordelen.
Bijlage IV	Lijst van subverwerkers (indien van toepassing).

Artikel 3. Verplichtingen Verwerker

3.1 Verwerker is verplicht te voldoen aan de verplichtingen zoals deze neergelegd in de AVG. Meer specifiek verbindt verwerker zich om alle persoonsgegevens die hij in het kader van de te verzorgen dienstverlening voor Verwerkingsverantwoordelijke verwerkt, zoals nader omschreven in Bijlage I, behoorlijk en zorgvuldig te verwerken. Het is Verwerker niet toegestaan om andere dan de in Bijlage I omschreven handelingen met persoonsgegevens uit te voeren. Verwerker is tevens verplicht om het register van verwerkingsactiviteiten als bedoeld in artikel 30, tweede lid, van de AVG bij te houden.

3.2 Verwerker verbindt zich om alle organisatorische maatregelen te nemen die Verwerkingsverantwoordelijke van een professioneel Verwerker van persoonsgegevens mag verwachten, waaronder de maatregelen zoals omschreven in Bijlage II.

3.3 Verwerker verwerkt de persoonsgegevens slechts in opdracht en ten behoeve van Verwerkingsverantwoordelijke. De verwerking geschiedt in overeenstemming met de instructies en aanwijzingen van Verwerkingsverantwoordelijke en in overeenstemming met de toepasselijke wet- en regelgeving.

3.4 Verwerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens die aan Verwerker zijn verstrekt of hem ter beschikking gekomen, komt niet bij Verwerker te rusten.

3.6 Verwerker is verplicht volledige medewerking te verlenen aan een door de Verwerkingsverantwoordelijke uit te voeren gegevensbeschermingseffectbeoordeling.

Datalekken

3.7 Verwerker stelt Verwerkingsverantwoordelijke onmiddellijk -uiterlijk binnen 24 uur - na het ontdekken van een (mogelijk) Datalek op de hoogte door het sturen van een e-mail aan meldpuntdatalekken@amsterdam.nl.

In de e-mail vermeldt Verwerker: naam van organisatie en contactpersoon, telefoonnummer, dag en tijdstip waarop een (mogelijk) Datalek is geconstateerd, het organisatieonderdeel (inclusief contactpersoon) van de gemeente voor wie de persoonsgegevens verwerkt worden, de aard van de inbreuk en de betrokken persoonsgegevens, de mogelijke gevolgen en de maatregelen die (kunnen) worden genomen.

3.8 Verwerker zal het doen van meldingen aan de toezichthouder overlaten aan de verwerkingsverantwoordelijke. Het is Verwerker niet toegestaan om namens Verwerkingsverantwoordelijke een melding bij de Autoriteit persoonsgegevens te doen van een Datalek.

3.9 Verwerker stelt Verwerkingsverantwoordelijke in staat om aan de wettelijke verplichtingen inzake de melding van een Datalek bij de Autoriteit persoonsgegevens te voldoen. Meer specifiek rusten op Verwerker ingeval van een mogelijk Datalek de navolgende verplichtingen:

a. Verwerker legt alle benodigde gegevens voor de beoordeling van het (mogelijke) Datalek aan Verwerkingsverantwoordelijke over. Daarbij verschaft verwerker in ieder geval de informatie aan de Verwerkingsverantwoordelijke zoals omschreven in bijlage III.

b. Verwerker houdt Verwerkingsverantwoordelijke op de hoogte van de voortgang van het intern onderzoek en de ontwikkelingen rondom het (mogelijke) Datalek;

c. Verwerker verleent de volledige medewerking indien Verwerkingsverantwoordelijke zelf onderzoek naar het (mogelijke) Datalek uitvoert;

d. Verwerker stelt Verwerkingsverantwoordelijke op de hoogte van de maatregelen die hij treft om de gevolgen van het (mogelijke) Datalek te beperken en om een herhaling te voorkomen;

e. Verwerker verleent alle medewerking zodat Verwerkingsverantwoordelijke in staat is om, waar van toepassing, Betrokkene(n) in kennis te stellen;

f. Verwerker volgt de instructies van Verwerkingsverantwoordelijke op;

g. Verwerker voldoet aan de bindende aanwijzing van Autoriteit persoonsgegevens, ook indien deze aan Verwerkingsverantwoordelijke wordt gegeven.

3.10 Verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van (mogelijke) Datalekken en zal Verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in het plan. Verwerker stelt de Verwerkingsverantwoordelijke op de hoogte van de materiele wijzigingen in het plan van aanpak.

3.11 Verwerker houdt een gedetailleerd logboek bij van mogelijke Datalekken, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen waarin minimaal de informatie als bedoeld in bijlage III is opgenomen, en geeft daar op eerste verzoek van Verwerkingsverantwoordelijke inzage in.

Gegevens ter beschikking stellen van Verwerkingsverantwoordelijke

3.12 Verwerker stelt op schriftelijk verzoek van Verwerkingsverantwoordelijke aan hem onmiddellijk alle persoonsgegevens ter hand die in het kader van deze Verwerkersovereenkomst worden verwerkt. Hieronder worden mede begrepen kopieën en bewerkingen van persoonsgegevens. Een dergelijk verzoek kan door Verwerkingsverantwoordelijke worden gedaan gedurende de looptijd van de Verwerkersovereenkomst en op het moment dat de Hoofdovereenkomst wordt beëindigd. De Verwerkingsverantwoordelijke kan zo nodig eisen stellen aan de wijze van beschikbaarstelling van de persoonsgegevens, waaronder begrepen de eisen aan het bestandsformaat.

3.13 Verwerker zal te allen tijde bij de hiervoor beschreven overdracht van persoonsgegevens waarborgen dat er geen sprake is van verlies van functionaliteit of (delen van de persoonsgegevens). De overdracht vindt verder op een zodanige wijze plaats dat de continuïteit van de dienstverlening maximaal gewaarborgd blijft, althans niet door handelen of nalaten van Verwerker wordt belemmerd. Verwerker is gehouden de na overdracht achtergebleven kopieën te vernietigen.

3.14 Van de overdracht en de gevraagde vernietiging wordt door Verwerker een verslag gemaakt. Verwerkingsverantwoordelijke kan van de vernietiging een bewijs verlangen. De kosten van overdracht en vernietiging komen voor rekening van Verwerker.

3.15 Het is Verwerker niet toegestaan persoonsgegevens aan anderen dan Verwerkingsverantwoordelijke te verstrekken, tenzij dit geschiedt op schriftelijk verzoek van Verwerkingsverantwoordelijke of met diens schriftelijke toestemming. Verwerker is in dat geval verplicht schriftelijk te bevestigen dat een verstrekking heeft plaatsgevonden, waarbij hij de verstrekte persoonsgegevens, de Betrokkene(n), de Ontvanger(s) en het moment van verstrekking dient te beschrijven.

Artikel 4. Rechten van Betrokkenen

4.1 Verwerker stelt Verwerkingsverantwoordelijke te allen tijden in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG en meer in het bijzonder de rechten van Betrokkenen.

4.2 Verwerker zal daartoe op verzoek van Verwerkingsverantwoordelijke zo spoedig mogelijk, doch uiterlijk binnen zeven werkdagen nadat het verzoek is gedaan aan Verwerkingsverantwoordelijke schriftelijk alle informatie verstrekken die Verwerkingsverantwoordelijke nodig heeft om te kunnen voldoen aan de in artikelen 12 tot en met 14 van de AVG vervatte mededelingsplicht.

4.3 Verwerker zal tevens op verzoek van Verwerkingsverantwoordelijke persoonsgegevens rectificeren, wissen of overgaan tot een beperking van de verwerking daarvan. Verwerker zal aan dit verzoek voldoen binnen vijf werkdagen nadat het verzoek door Verwerkingsverantwoordelijke is gedaan.

Artikel 5. Geheimhoudingsplicht

5.1 Personen in dienst van, dan wel werkzaam ten behoeve van Verwerker, evenals Verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis hebben kunnen nemen, tenzij een wettelijk voorschrift tot verstrekking verplicht. De medewerkers van Verwerker en van eventuele sub-Verwerkers die door Verwerker worden ingeschakeld - die uit de aard van hun functie over de persoonsgegevens kunnen beschikken - tekenen hiertoe een geheimhoudingsverklaring.

Artikel 6. Beveiligingsmaatregelen

6.1 Verwerker neemt alle passende technische en organisatorische beveiligingsmaatregelen om de persoonsgegevens die voor Verwerkingsverantwoordelijke worden verwerkt te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onzorgvuldig, ondeskundig of ongeoorloofd gebruik. Voor "passende technische en organisatorische maatregen" en "een passend beveiligingsniveau" handelt Verwerker minimaal conform het richtsnoer "beveiliging van de persoonsgegevens" van de Autoriteit persoonsgegevens en de Baseline Informatievoorziening Gemeenten. Verwerker is voorts gehouden tot naleving van de beveiligingsnormen en standaarden van Verwerkingsverantwoordelijke, zoals beschreven in Bijlage II. Verwerker neemt steeds alle maatregelen die Verwerkingsverantwoordelijke van een professioneel handelend Verwerker van persoonsgegevens mag verwachten en zal de benodigde maatregelen treffen naar aanleiding van de plan-do-check-act-cyclus.

6.2 Verwerker rapporteert jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van het bepaalde in deze overeenkomst. Deze rapportage betreft ook, indien van toepassing, de werkzaamheden van door hem ingeschakelde derden. Verwerker zal na een verzoek daartoe door Verwerkingsverantwoordelijke minimaal eens per jaar kosteloos een TPM c.q. een verklaring van een onafhankelijke externe deskundige aan Verwerkingsverantwoordelijke verstrekken over de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen.

Let op bij 6.2!

Als de aard van de verwerking dit toelaat; kan er voor worden gekozen om deze bepaling aan te passen.

Dit kan nadat hierover afstemming met de Security Officer en Privacy Officer heeft plaatsgevonden.

Bij uitbesteding van hosting en beheer is een TPM altijd verplicht.

6.3 Jaarlijks dient Verwerker door middel van een pen- en hacktest, uitgevoerd door een daarin gespecialiseerde onafhankelijke auditor, aan te tonen dat de applicatie en de infrastructuur waarmee persoonsgegevens worden bewerkt voldoen aan de Open Web Application Security Project (OWASP) criteria, en de in deze Verwerkersovereenkomst nader gespecificeerde criteria rond het uitvoeren van pen- en hacktesten en de gewenste rapportagevorm. De resultaten van deze test dienen te worden overgelegd aan Verwerkingsverantwoordelijke. De kosten van de pen- en hacktest en de eventuele her-test uit te voeren door een daarin gespecialiseerde auditor worden door Verwerker gedragen.

Naast de jaarlijkse test zal Verwerker eveneens zijn volledige medewerking verlenen aan extra pen- en hacktesten indien Verwerkingsverantwoordelijke deze laat uitvoeren door een door hem geselecteerde partij, teneinde te bezien of de applicatie en de infrastructuur waarmee de persoonsgegevens worden bewerkt voldoen aan de OWASP criteria, en de in deze overeenkomst nader gespecificeerde criteria. De kosten van een extra pen- en hacktest en de eventuele her-test worden door Verwerkingsverantwoordelijke gedragen. De datum van uitvoering zal in onderling overleg tussen Verwerkingsverantwoordelijke en Verwerker worden bepaald.

Let op bij 6.3!

In geval van een minder zware verwerking; kan er voor worden gekozen om deze bepaling aan te passen

Dit kan nadat hierover afstemming met de Privacy Officer heeft plaatsgevonden.

6.4 Verwerker voert de uitkomsten van de pen- en hacktest en de naar aanleiding daarvan aangegeven aanbevelingen uit binnen de daartoe door Verwerkingsverantwoordelijke te bepalen termijn.

6.5 Verwerkingsverantwoordelijke behoudt zich het recht voor om de Informatie-beveiligingsdienst Gemeenten dan wel een andere derde in te schakelen voor ondersteuning en advisering met betrekking tot in het kader van audits en/of in pen- en hacktest aangetroffen bevindingen. Verwerker stemt hiermee in.

Artikel 7. Inschakeling subverwerkers

7.1 Verwerker is slechts gerechtigd de verwerking van persoonsgegevens geheel of ten dele uit te besteden aan subverwerkers na voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke.

7.2 Verwerkingsverantwoordelijke kan aan de toestemming voorwaarden verbinden die dienen ter naleving van de verplichtingen uit deze Verwerkersovereenkomst. Verwerker dient in ieder geval contractueel verzekerd te hebben dat de subverwerker gehouden is aan de verplichtingen die deze Verwerkersovereenkomst aan Verwerker oplegt. Verwerkingsverantwoordelijke dient in staat te worden gesteld toe te zien op de naleving van de afspraken van de subverwerker met Verwerker. Verwerker garandeert dat deze subverwerker schriftelijk minimaal dezelfde plichten heeft als tussen de Verwerkingsverantwoordelijke en de Verwerker zijn overeengekomen en zal de Verwerkingsverantwoordelijke inzage verschaffen in de overeenkomsten met deze derden, waarin deze verplichten zijn opgenomen.

7.3 Verwerker blijft te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit de Hoofdovereenkomst en deze Verwerkersovereenkomst. Wanneer de subverwerker zijn verplichtingen niet nakomt, blijft Verwerker ten aanzien van Verwerkingsverantwoordelijke volledig aansprakelijk voor het nakomen van de verplichtingen door de subverwerker.

7.4 De Verwerker houdt een actueel register bij van de door hem ingeschakelde subverwerkers en onderaannemers waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van deze subverwerkers zijn opgenomen, alsmede eventuele door de Verwerkingsverantwoordelijke gestelde aanvullende voorwaarden. Dit register zal als bijlage IV aan deze verwerkingsovereenkomst worden toegevoegd.

Artikel 8. Doorgifte

8.1 Verwerker is gehouden de persoonsgegevens te verwerken in landen binnen de Europese Economische Ruimte (EER). Het is Verwerker verboden de persoonsgegevens door te geven, waaronder ter beschikking stellen, aan organisaties die gevestigd zijn buiten de Europese Unie en Internationale Organisaties, tenzij op uitdrukkelijke instructie van de Verwerkingsverantwoordelijke.

8.2 Indien Verwerker op grond van een in Nederland en/of in de Europese Economische Ruimte (EER) geldende wettelijke verplichting gegevens aan enige Derde dient te verstrekken, zal Verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal Verwerker onmiddellijk, voorafgaand aan de verstrekking, Verwerkingsverantwoordelijke ter zake informeren, tenzij de wet dit verbiedt om gewichtige redenen van algemeen belang.

Artikel 9. Audit op verwerking van persoonsgegevens

9.1 Verwerkingsverantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens te doen controleren door middel van een audit. Verwerker is verplicht Verwerkingsverantwoordelijke of de - in opdracht van Verwerkingsverantwoordelijke- controlerende instantie toe te laten en alle medewerking te verlenen, waaronder het verlenen van de verlangde informatie, zodat de controle daadwerkelijk uitgevoerd kan worden. De met de audit gemoeide kosten zijn voor rekening van Verwerker indien er niet conform de verwerkersovereenkomst blijkt te zijn gewerkt, en/of er fouten worden gevonden in de bevindingen, die toegerekend moeten worden aan Verwerker. In ieder ander geval zullen de kosten van de audit worden gedragen door Verwerkingsverantwoordelijke. Verwerkingsverantwoordelijke zal de audit slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan Verwerker.

9.2 Verwerker garandeert de aanbevelingen die voortvloeien uit een audit binnen de daartoe door Verwerkingsverantwoordelijke te bepalen redelijke termijn uit te voeren.

Artikel 10. Wijziging overeenkomst

10.1 Verwerkingsverantwoordelijke en Verwerker treden met elkaar in overleg over wijzigingen in deze Verwerkersovereenkomst als een wijziging in regelgeving of een wijziging in de uitleg van de regelgeving daartoe aanleiding geven.

10.2 Wijziging van deze Verwerkersovereenkomst kan slechts als beide partijen een daartoe opgesteld document ondertekenen en deze als bijlage opnemen bij deze Verwerkersovereenkomst.

Artikel 11. Aansprakelijkheid en boetebepaling

11.1 Indien Verwerker tekortschiet in de nakoming van de verplichtingen uit deze overeenkomst kan Verwerkingsverantwoordelijke hem in gebreke stellen. Ingebrekestelling geschiedt schriftelijk, waarbij aan Verwerker een redelijke termijn wordt gegund om alsnog zijn verplichtingen na te komen.

Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is Verwerker in verzuim. Verwerker is onmiddellijk in verzuim als de nakoming van desbetreffende verplichting anders dan door overmacht zoals gedefinieerd in de Hoofdovereenkomst binnen de overeengekomen termijn reeds blijvend onmogelijk is.

11.2 Verwerker is aansprakelijk voor alle schade of nadeel voortvloeiende uit het niet-nakomen van, of in strijd handelen met de bij of krachtens de AVG gegeven voorschriften en/of het niet-nakomen van, of in strijd handelen met het in deze Verwerkersovereenkomst bepaalde, onverminderd de aanspraken op grond van wettelijke regels. Verwerker is aansprakelijk voor schade of nadeel voor zover ontstaan door zijn werkzaamheid, daaronder begrepen ontstane inbreuken op de persoonlijke levenssfeer van Betrokkenen. De aansprakelijkheid van Verwerker is, tenzij sprake is

van opzet of bewuste roekeloosheid, beperkt tot het in de Hoofdovereenkomst overeengekomen bedrag.

11.3. Verwerker vrijwaart Verwerkingsverantwoordelijke tegen aanspraken van derden, waaronder Betrokkenen, in verband met het handelen van Verwerker in strijd met de Verwerkersovereenkomst, de AVG en/of andere regelgeving waarin eisen aan het verwerken van persoonsgegevens worden gesteld. Verwerker zal alle daarmee verband houdende en daaruit voortvloeiende kosten (waaronder mede begrepen kosten van juridische bijstand) en schade van de gemeente vergoeden.

11.4 Indien Verwerker enige in deze Verwerkersovereenkomst neergelegde verplichtingen niet of niet-tijdig nakomt en de Autoriteit persoonsgegevens Verwerkingsverantwoordelijke dientengevolge een bestuurlijke boete oplegt, is Verwerker aansprakelijk en zal Verwerkingsverantwoordelijke een contractuele boete ter hoogte van hetzelfde bedrag opleggen aan Verwerker. Deze boete is zonder rechterlijke tussenkomst, ingebrekestelling of aanmaning direct opeisbaar. Deze boete is niet vatbaar voor verrekening. Oplegging van deze boete laat alle andere rechten of vorderingen van Verwerkingsverantwoordelijke (inclusief o.a. het recht op nakoming, schadevergoeding) onverlet.

11.5 Indien Verwerker enige in artikel 5 (Geheimhoudingsplicht) of artikel 7 (inschakeling subverwerkers) van deze Verwerkersovereenkomst genoemde verplichting niet of niet-tijdig nakomt, is Verwerker een boete verschuldigd van € 25.000,- per gebeurtenis. De boete is zonder rechterlijke tussenkomst, ingebrekestelling of aanmaning direct opeisbaar. De boete is niet vatbaar voor verrekening. De boete laat alle andere rechten of vorderingen, waaronder, doch niet uitsluitend, de vordering van Verwerkingsverantwoordelijke tot nakoming en het recht op schadevergoeding onverlet.

Artikel 12. Toepasselijk recht

12.1 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. Partijen zullen trachten geschillen die ontstaan naar aanleiding van deze Verwerkersovereenkomst eerst minnelijk op te lossen. Indien het geschil niet minnelijk wordt opgelost, wordt het geschil voorgelegd aan de bevoegde rechter te Amsterdam.

Aldus in tweevoud opgesteld en getekend op: <…DATUM…>

Namens Verwerkingsverantwoordelijke: directeur <organisatieonderdeel> van de gemeente Amsterdam

Namens Verwerker: <nader in te vullen gegevens Verwerker>

Bijlagen

I Omschrijving van te verwerken categorie persoonsgegevens (dataset), categorie betrokkenen en de werkzaamheden van de Verwerker.

II De technische beveiligingsnormen en standaards van Verwerkingsverantwoordelijke, en de te nemen organisatorische maatregelen

III Inlichtingen om (mogelijke) Datelekken te beoordelen

IV Lijst van subverwerkers (indien van toepassing)

Bijlage I:
Omschrijving van te verwerken categorie persoonsgegevens (dataset), categorie betrokkenen en de werkzaamheden van de Verwerker (als bedoeld in artikel 3.1 van de Verwerkersovereenkomst)

1. De werkzaamheden van Verwerker (de verleende diensten en de bijbehorende verwerking).
Hier een lijstje opnemen met werkzaamheden die veel voorkomen **zoals:**

- Hosting bestaande uit activiteiten zoals…
- Back-ups maken en restoren
- Applicatiebeheer bestaande uit activiteiten zoals…
- Technisch beheer bestaande uit activiteiten zoals…
- Database beheer bestaande uit activiteiten zoals…
- Helpdesk bestaande uit activiteiten zoals…
- Communicatievoorziening (zoals berichtenverkeer)
- Archiefbeheer
- Vernietiging van gegevensdragers
- Printing, scanning, kopiëren (lease van Multifunctionals)
- Inhoudelijke werkzaamheden die namens de gemeente worden uitgevoerd zoals:
  - Uitgifte parkeervergunningen
  - Voeren salarisadministratie

Indien de werkzaamheden in de hoofdovereenkomst specifiek omschreven zijn, kan dit lijstje achterwege blijven. Of hier verwijzen naar de Hoofdovereenkomst. De achtergrond van de beschrijving is dat je voldoende duidelijk maakt wat er beveiligd moet worden. Het is de bedoeling dat de zinnen afgemaakt worden met specifieke omschrijvingen!

2. Omschrijving van de werkzaamheden van de derden (subverwerkers) als deze er zijn, als bedoeld in artikel 8 van de Verwerkersovereenkomst.

Lijstje opnemen met werkzaamheden die veel voorkomen **zoals:**

- Hosting bestaande uit activiteiten zoals…-Back-ups maken en restoren
- Applicatiebeheer bestaande uit activiteiten zoals…
- Technisch beheer bestaande uit activiteiten zoals…
- Database beheer bestaande uit activiteiten zoals…
- Helpdesk bestaande uit activiteiten zoals…
- Communicatievoorziening (zoals berichtenverkeer)
- Onderhoud aan multifunctionals

De achtergrond van de beschrijving is dat er voldoende duidelijk gemaakt wordt wat er beveiligd moet worden. Ook hier geldt dat de zinnen afgemaakt worden met specifieke omschrijvingen!

3. Categorieën personen/betrokkenen en soorten persoonsgegevens

Personen/ betrokkenen
Algemene omschrijving van de categorieën personen waar de gegevens die verwerkt worden betrekking op hebben zoals: personeelsleden, burgers, ingeschrevenen, vergunning aanvragers, voorziening aanvragers (cliënten).

Categorie persoonsgegevens
[Beschrijf de categorie van persoonsgegevens.]

*Denk daarbij ook aan de vraag of er gegevens van gevoelige aard worden verwerkt, **zoals**:*

- Bijzondere persoonsgegevens Het gaat hierbij om persoonsgegevens over iemands ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. En gegevens over strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

- Gegevens over de financiële of economische situatie van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.

- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen

- Gebruikersnamen, wachtwoorden en andere inloggegevens. De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar deinloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

- Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het BSN.

- Is er sprake van de verwerking van gegevens over kwetsbare groepen zoals:
  - minderjarigen;
  - mensen die te maken hebben met stalking;
  - die in een blijf-van-mijn-lijfhuis verblijven.

- Voor bepaalde categorieën van betrokkenen:
  - kinderen en mensen met een verstandelijke handicap.

Bijlage II: Beschrijving beveiligingsmaatregelen ter uitwerking van artikel 3.2, en artikel 6.1, van deze Verwerkersovereenkomst en de te nemen organisatorische maatregelen.

1. Normenstelsel (kies a of b)

a. De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk: *(vermeld normenstelsel, zoals bijvoorbeeld NEN/ISO 27001, NEN7510, PCI/DSS).*
b. De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm zoals de BIG of de BIR of vergelijkbaar.

2. De toereikendheid van de informatiebeveiliging blijkt uit (cumulatief):

a. Verwerker is ISO 27001 gecertificeerd;
b. Verwerker toont zelf aan dat hij aan de eisen uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) voldoet (door een GAP analyse);
c. Verwerker levert jaarlijks een audit of TPM: een ISAE 3402 type 2 rapport, waarmee een onafhankelijke externe auditor rapporteert over de opzet, bestaan en werking van beheersmaatregelen:
d. Verwerkingsverantwoordelijke ontvangt jaarlijks dit rapport en heeft een right-to audit om eventueel aanvullend te toetsen; **en,**
e. De Verwerker hanteert een integriteitscode dan wel een interne gedragscode voor zijn medewerkers waaruit blijkt dat de medewerkers en door de Verwerker ingeschakelde derden de vertrouwelijkheid in acht nemen. (artikel 28 lid 3 AVG: verwerker moet bewijsbaar integere medewerkers in dienst hebben).

LET OP: gemotiveerd afwijken is toegestaan! Denk hierbij onder andere aan het risico van de verwerking of de waarde van het contract.

LET OP: bij een risico dat het niveau van beveiliging van de BIG overstijgt moeten deze risico's worden geïdentificeerd en aanvullende passende maatregelen worden bepaald en in deze bijlage worden vastgelegd. Als in de hoofdovereenkomst hierover passende afspraken gemaakt zijn, dan in deze bijlage hierbij aansluiten.

3. Criteria voor de uitvoering van een pentest als bedoeld in artikel 6.3:

Voor het uitvoeren van een initiële en een vervolg pen- en hacktest dient gebruik te worden gemaakt van gespecialiseerde bedrijven, die medewerkers kunnen inzetten die voldoende ervaring hebben en gecertificeerd zijn. Tevens dienen de medewerkers in het bezit te zijn van een verklaring omtrent gedrag en dient een geheimhoudingsverklaring te worden overlegd.

Voordat gestart wordt met de pen- en hacktest dient door verwerkingsverantwoordelijke een vrijwaringsverklaring aan de testende partij te worden overhandigd en dienen afspraken te worden gemaakt over de soort test en het moment waarop deze zal plaatsvinden. Ook dient de hostende partij schriftelijk van te voren te worden ingelicht over het moment van test en de IP-reeks waar vanaf de test zal gaan plaatsvinden.

Indien persoonsgegevens worden verwerkt dan dient de pen- en hacktest te worden uitgevoerd vanuit een crystal- en blackbox benadering, waarbij de pen- en hacktester door de verwerker van te voren worden voorzien van netwerk tekeningen, technisch ontwerp en de meest recente technische documentatie.

De rapportage dient plaats te vinden in de Nederlandse taal. Voor omvangrijkere testen is de volgende inhoud van de rapportage vereist:

- Management samenvatting
- Inleiding
    - Opdrachtomschrijving
    - Scope en doelstelling
    - Auditomgeving en objecten
    - Gebruikte methoden en technieken
    - Risico niveaus
- Bevindingen
    - Oorzaak van de bevinding
    - Risico beschrijving incl. risicomatrix zie afbeelding
    - Bewijs
    - Aanbeveling
- Conclusies en aanbevelingen

Risico matrix per bevinding:

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid van optreden	Laag	LAAG	LAAG	GEMIDDELD
	Gemiddeld	LAAG	GEMIDDELD	HOOG
	Hoog	GEMIDDELD	HOOG	ZEER HOOG

Tevens dient de partij die de pen- en hacktest heeft uitgevoerd de loggegevens van de test ter beschikking te stellen aan de opdrachtgever van de test zodat altijd achteraf kan worden geconstateerd of de aangetroffen kwetsbaarheden te repliceren zijn.

Bij de ontwikkeling van webapplicaties hanteren wij naast de richtlijnen uit de BIG aanvullende kaders.

Deze kaders zijn:
https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

Tevens zijn nog het Amsterdamse beleidsstuk v.w.b. beveiliging webapplicaties van kracht evenals het laatste audit framework op basis van de OWASP top 10.

Herstel bevindingen:
H/H, M/H, H/M bevinding dienen per direct hersteld te worden.
De M/M bevindingen dienen zo snel mogelijk hersteld te worden en de mindere zaken kunnen worden meegenomen in reguliere releases (L/L en M/L.)

4. Overige organisatorische maatregelen

- Niet limitatief:

- Welke (groepen) van medewerkers van Verwerker hebben toegang tot welke persoonsgegevens:
    -
    -
    -
- Welke handelingen mogen de medewerkers van Verwerker met de persoonsgegevens uitvoeren.

-
-
-
- De persoonsgegevens worden na XX (termijn invullen) vernietigd.

Bijlage III: Inlichtingen om (mogelijke) Datalekken te beoordelen te uitwerking van art. 3.7, onder a, van de Verwerkersovereenkomst.

Verwerker zal alle inlichtingen verschaffen die Verwerkingsverantwoordelijke noodzakelijk acht om het (mogelijke) Datalek (hierna: de inbreuk) te kunnen beoordelen. Daarbij verschaft Verwerker in ieder geval de volgende informatie aan Verwerkingsverantwoordelijke:

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

Bijlage IV: Omschrijving werkzaamheden ter uitwerking van artikel 7.4, van deze Verwerkersovereenkomst

Verwerker maakt bij de uitvoering van de verwerkersovereenkomst gebruik van de subverwerkers die in deze bijlage zijn vermeld. De Verwerker zal deze bijlage conform artikel 7.4 van deze Verwerkersovereenkomst bijwerken indien er wijzigingen plaatsvinden in de ingeschakelde subverwerkers en deze lijst onverwijld ter beschikking stellen aan de Verwerkingsverantwoordelijke.

Partij 1:	<naam>
Vestigingsplaats:	
Inschrijvingsnummer handelsregister:	
Beschrijving van de werkzaamheden:	
Voorwaarden van de verwerkingsverantwoordelijke gesteld aan toestemming:	

Partij 2:	<naam>
Vestigingsplaats:	
Inschrijvingsnummer handelsregister:	
Beschrijving van de werkzaamheden:	
Voorwaarden van de verwerkingsverantwoordelijke gesteld aan toestemming:	