
Gemeente Haarlemmermeer

Bewerkersovereenkomst

behorend bij Overeenkomst betreffende schoolcoaches en gedragswetenschapper 2018 e.v.

met kenmerk



Datum : dd mm 2018

Tussen

Gemeente Haarlemmermeer, gevestigd aan het Raadhuisplein 1, (2132 TZ), te Hoofddorp, hierbij rechtsgeldig op grond van het Mandaat-, machtiging- en volmachtsbesluit 2015, nummer 2015.0058870 d.d. 15 december 2015, vertegenwoordigd door (naam directeur/clustermanager/teammanager), (functie)..... hierna te noemen: **“Verantwoordelijke”**;

en

[naam leverancier]., statutair gevestigd te ... en kantoorhoudende aan ... te ... te dezen rechtsgeldig vertegenwoordigd door: [naam], in zijn/haar hoedanigheid van [functie], hierna te noemen **“Bewerker”**,

Overwegingen:

- A. Verantwoordelijke met Bewerker op [datum] een overeenkomst met betrekking tot het uitvoeren van werkzaamheden op het gebied van [...] met kenmerk [...] heeft gesloten;
- B. in het kader van de uitvoering daarvan Persoonsgegevens in de zin van artikel 1, onder a, van de Wet bescherming persoonsgegevens (hierna te noemen: Wbp) worden verwerkt;
- C. krachtens het bepaalde in artikel 1 van de Wbp de gemeente Haarlemmermeer Verantwoordelijke is voor de Persoonsgegevens en [naam leverancier] Bewerker;
- D. Partijen in overeenstemming met de Wbp in deze Bewerkerovereenkomst hun afspraken over het verwerken van de Persoonsgegevens door [naam leverancier] als Bewerker wensen vast te leggen;
- E. deze Bewerkerovereenkomst is aan te merken als een Bewerkerovereenkomst in de zin van artikel 14, tweede lid, van de Wbp.

Partijen zijn het volgende overeengekomen:

Artikel 1. Definities

- 1.1 De hierna en hiervoor in deze bewerkerovereenkomst met een hoofdletter geschreven begrippen hebben de volgende betekenis:
 - 1. *Autoriteit Persoonsgegevens*: de instantie zoals bedoeld in artikel 51 van de Wet bescherming persoonsgegevens (Wbp);
 - 2. *Betrokkene*: degene op wie een Persoonsgegeven betrekking heeft;
 - 3. *Beveiligingsincident*: een inbreuk op de technische en/of organisatorische beveiliging van persoonsgegevens die in het kader van uitvoering van de Hoofdovereenkomst worden verwerkt. Hieronder vallen onder meer maar niet uitsluitend: verloren USB-sticks, malware op door Partijen gebruikte hardware, gestolen laptops, gehackte systemen en calamiteiten in datacentra;
 - 4. *Datalek*: wanneer als gevolg van een Beveiligingsincident persoonsgegevens verloren zijn gegaan of als redelijkerwijs niet kan worden uitgesloten dat als gevolg van het Beveiligingsincident persoonsgegevens onrechtmatig zijn verwerkt;

5. *Onderliggende Overeenkomst*: de overeenkomst betreffende levering van schoolcoaches en gedragswetenschapper d.d. 1 augustus 2018 met kenmerkwaarbij Verantwoordelijke aan Bewerker opdracht heeft gegeven om werkzaamheden te verrichten, waarbij de uitvoering behelst dat door Bewerker Persoonsgegevens worden verwerkt;
6. *Overeenkomst*: deze bewerkersovereenkomst;
7. *Persoonsgegevens*: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
8. *Sub-bewerker*: de partij die door Bewerker wordt ingeschakeld (als bewerker) ten behoeve van de Verwerking van de Persoonsgegevens in het kader van deze Overeenkomst en de Onderliggende Overeenkomst;
9. *Verwerken/Verwerking*: alle handelingen of reeks handelingen uitgevoerd op Persoonsgegevens, al dan niet door geautomatiseerde middelen, zoals verzamelen, vastleggen, structureren, opslaan, aanpassen of wijzigen, ophalen, raadplegen, gebruiken, bekendmaken door overdracht, verspreiding of anderszins beschikbaar maken, afstemmen of combineren, blokkeren, wissen of vernietigen.

Artikel 2. Toepasselijkheid, totstandkoming, duur en einde van de Bewerkersovereenkomst

- 2.1 Deze Bewerkersovereenkomst treedt niet eerder in werking dan op de datum waarop Partijen de Overeenkomst hebben ondertekend.
- 2.2 Deze Bewerkersovereenkomst zal van kracht zijn gedurende de looptijd van de Onderliggende Overeenkomst. Indien de Onderliggende Overeenkomst eindigt, eindigt deze Bewerkersovereenkomst, met dien verstande dat de bepalingen die naar hun aard nog voortduren, onverminderd van kracht blijven. Ingeval de Bewerkersovereenkomst eindigt, is het Bewerker niet langer toegestaan om persoonsgegevens voor Verantwoordelijke te verwerken. Verantwoordelijke heeft het recht om de Onderliggende Overeenkomst te beëindigen, indien deze niet kan worden uitgevoerd zonder dat Bewerker daadwerkelijk persoonsgegevens voor Verantwoordelijke verwerkt.
- 2.3 Geen van beide Partijen kan deze Bewerkersovereenkomst tussentijds opzeggen.
- 2.4 Tenzij Partijen anders schriftelijk zijn overeengekomen, zijn de bepalingen van deze Overeenkomst van toepassing op iedere Verwerking door Bewerker op grond van de Onderliggende Overeenkomst.
- 2.5 Partijen werken beiden in overeenstemming met de door de Autoriteit Persoonsgegevens opgestelde Beleidsregels welke te downloaden zijn op de website van Autoriteit Persoonsgegevens :
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf >

Artikel 3. Verwerking door Bewerker

- 3.1 Bewerker verwerkt in opdracht van Verantwoordelijke de in **Bijlage 2** beschreven Persoonsgegevens.

- 3.2 Bewerker zal de Persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met deze Overeenkomst, de Wbp en andere toepasselijke regelgeving betreffende de Verwerking van Persoonsgegevens Verwerken.
- 3.3 Bewerker Verwerkt Persoonsgegevens slechts in opdracht van Verantwoordelijke en volgt alle instructies van Verantwoordelijke dienaangaande op, behoudens afwijkende wettelijke verplichtingen.
- 3.4 Bewerker heeft geen zeggenschap over het doel en de middelen voor de Verwerking van Persoonsgegevens en neemt geen beslissingen over het gebruik van de Persoonsgegevens, de verstrekking aan derden en de duur van de opslag van Persoonsgegevens. De zeggenschap over de Persoonsgegevens verstrekt onder deze Bewerkersovereenkomst komt nimmer bij Bewerker te berusten. Het is Bewerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Verantwoordelijke (mondeling, schriftelijk dan wel elektronisch) aan Bewerker zijn opgedragen. Deze verplichting geldt zowel gedurende de looptijd van deze overeenkomst als na afloop daarvan.
- 3.5 Bewerker dient zorg te dragen voor de naleving van de voorwaarden die op grond van deze Overeenkomst, de Wet bescherming persoonsgegevens (Wbp) en andere (Europese) regelgeving worden gesteld aan het verwerken van Persoonsgegevens.
- 3.6 Bewerker schakelt geen derden in zonder voorafgaande toestemming van Verantwoordelijke. Verantwoordelijke kan aan de toestemming om derden in te schakelen nadere voorwaarden binden. Bewerker verzekert alsdan in ieder geval dat de derde zich richt naar de instructies van Opdrachtgever, tot geheimhouding verplicht is en de nodige beveiligingsmaatregelen ten opzichte van de gegevensverwerking neemt. Alle relevante verplichtingen uit deze Bewerkersovereenkomst voor de bescherming en beveiliging van de Persoonsgegevens en de verplichting de voorwaarden in deze Overeenkomst, alsmede de Wbp en overige (Europese) regelgeving na te leven, worden alsdan door Bewerker overgenomen in de overeenkomst met de derde. Tevens zullen de identiteit en vestigingsgegevens van de derde worden opgenomen in **Bijlage 3** bij deze Overeenkomst. Bewerker verplicht deze derde alsdan tevens contractueel om Persoonsgegevens niet verder te verwerken anders dan in het kader van deze Bewerkersovereenkomst is overeengekomen.
- 3.7 Het is Bewerker niet toegestaan Persoonsgegevens aan anderen dan Verantwoordelijke te verstrekken, tenzij op schriftelijk verzoek van Opdrachtgever, of met diens schriftelijke toestemming. Bewerker is verplicht schriftelijk te bevestigen dat een verstrekking heeft plaatsgevonden, waarbij hij exact de verstrekte Persoonsgegevens, de Betrokkene(n), de ontvanger(s) en het moment van verstrekking dient te beschrijven.
- 3.8 Indien Bewerker op grond van een wettelijke verplichting gegevens dient te verstrekken, verifieert Bewerker de grondslag van het verzoek en de identiteit van de verzoeker en informeert hij onmiddellijk Verantwoordelijke ter zake. Bewerker zal alsdan niet eerder overgaan tot het verstrekken van de gegevens, dan nadat is overlegd met Verantwoordelijke en deze daarvoor goedkeuring heeft gegeven. Bewerker zal Verantwoordelijke zo spoedig mogelijk schriftelijk in kennis stellen van de wettelijke verplichting en daarbij alle relevante informatie verstrekken die Verantwoordelijke redelijkerwijs nodig heeft om de benodigde maatregelen te treffen om te bepalen of verstrekking kan plaatsvinden en, zo ja, onder welke voorwaarden.

- 3.9 Bewerker verleent Verantwoordelijke volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de Wbp, meer in het bijzonder de rechten van Betrokkenen, zoals, maar niet beperkt tot, een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet.
- 3.10 Indien Bewerker onrechtmatige Verwerkingen of inbreuken op de in artikel 4.1 genoemde beveiligingsmaatregelen signaleert, zal hij Verantwoordelijke hierover onmiddellijk inlichten en alle redelijkerwijs benodigde maatregelen treffen om deze en verdere onrechtmatige Verwerkingen of inbreuken te beëindigen, te voorkomen of te beperken, een en ander onverminderd de verplichting van Bewerker om de eventueel door Verantwoordelijke daardoor geleden schade te vergoeden.
- 3.11 Bewerker verschaft enkel toegang tot de Persoonsgegevens aan haar werknemers voor zover dit nodig is voor het verrichten van de werkzaamheden op grond van de Onderliggende Overeenkomst.
- 3.12 Bewerker mag de Persoonsgegevens enkel buiten Nederland doch binnen de Europese Economische Ruimte (verder: EER) verwerken met voorafgaande schriftelijke toestemming van de Verantwoordelijke, aan deze toestemming kan Verantwoordelijke voorwaarden verbinden.
Partijen zien erop toe dat voor zover Persoonsgegevens buiten de Europese Economische Ruimte (verder: EER) met voorafgaande schriftelijke toestemming van de Verantwoordelijke worden Verwerkt, dit alleen plaatsvindt conform wettelijke voorschriften, en eventuele verplichtingen die in dit verband op Verantwoordelijke rusten. Ook aan deze toestemming kan Verantwoordelijke nadere voorwaarden verbinden.
Het is Bewerker nadrukkelijk niet toegestaan het beheer van de data bijv. door middel van datacenters buiten de EER te doen plaatsvinden. Indien met voorafgaande schriftelijke toestemming van Verantwoordelijke door Bewerker gegevens buiten de EER met in achtneming van dit artikel worden verwerkt, wordt dit in een afzonderlijke door Partijen op te stellen en aan deze Overeenkomst te hechten Bijlage aangegeven, inclusief een opgave van de landen waar de gegevens worden verwerkt.
- 3.13 Bewerker dient Verantwoordelijke onverwijld nadat Bewerker ervan kennis heeft gekregen, in kennis te stellen van iedere inbreuk op de beveiliging van Persoonsgegevens, met bijvoorbeeld de vernietiging, het verlies, de wijziging, onrechtmatige verwerking of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot Persoonsgegevens tot gevolg en Verantwoordelijke alle noodzakelijke informatie en medewerking te verlenen om de Verantwoordelijke in staat te stellen zo spoedig mogelijk de oorzaak en de omvang hiervan vast te stellen.
- 3.14 Bewerker dient Verantwoordelijke in kennis te stellen van alle verzoeken met betrekking tot inzage in de Persoonsgegevens die rechtstreeks van een Betrokkene zijn ontvangen. Bewerker geeft aan een dergelijk verzoek alleen gevolg indien Verantwoordelijke Bewerker daartoe schriftelijk opdracht heeft gegeven.
- 3.15 Bewerker handelt alle verzoeken om inlichtingen van Verantwoordelijke met betrekking tot de verwerking van de Persoonsgegevens vlot en behoorlijk af.

- 3.16 Bewerker is gehouden tot geheimhouding van alle Persoonsgegevens en informatie die Bewerker als uitvloeisel van deze Overeenkomst Verwerkt, behoudens in zoverre die Persoonsgegevens of informatie klaarblijkelijk geen geheim of vertrouwelijk karakter hebben, dan wel reeds algemeen bekend zijn. Bewerker draagt ervoor zorg dat de Persoonsgegevens niet direct of indirect ter beschikking (kunnen) komen van derden. Onder derden wordt hier ook het personeel van Bewerker begrepen voor zover het niet noodzakelijk is dat zij bij de Opdracht en/of deze overeenkomst kennis hoeft te nemen van de Persoonsgegevens als ook (medewerkers van) moeder- of zusterbedrijven waaraan Bewerker gelieerd is of toeleveranciers van Bewerker.
- Bewerker zorgt dat zijn personeel gebonden is aan de in dit artikel opgenomen geheimhoudingsplicht en dat Bewerker van die gebondenheid schriftelijk bewijs bezit. Op eerste verzoek van Verantwoordelijke verstrekt Bewerker aan Verantwoordelijke dat bewijs. Bewerker zal Verantwoordelijke onmiddellijk op de hoogte stellen van ieder verzoek tot kennisneming, verstrekking of andere vorm van opvragen en mededeling van de Persoonsgegevens in strijd met de in dit artikel opgenomen geheimhoudingsplicht. Bewerker is bij schending van de geheimhoudingsverplichting die ingevolge deze Bewerkersovereenkomst op hem en zijn personeel rusten, aan Verantwoordelijke een boete verschuldigd van € 1.500,- per gebeurtenis.
- 3.17 Indien en voor zover Verantwoordelijke daarom uitdrukkelijk schriftelijk verzoekt, zal Bewerker ten aanzien van de daarbij aangeduide Persoonsgegevens of informatie bijzondere maatregelen treffen met het oog op de geheimhouding daarvan, welke maatregelen onder meer kunnen inhouden de vernietiging van betrokken Persoonsgegevens of informatie zodra de noodzaak voor Bewerker om daarvan nog langer kennis te nemen, is komen te vervallen.
- 3.18 Bewerker zal in haar overeenkomsten met het personeel van Bewerker bedingen dat door die personen op overeenkomstige wijze als hiervoor in de leden 15 en 16 bepaald geheimhouding zal worden betracht ten aanzien van alle Persoonsgegevens en informatie die zij in het kader van hun werkzaamheden voor Opdrachtnemer Verwerken. Bewerker staat er jegens Verantwoordelijke voor in dat de bedoelde bedingen door de betrokken personen zullen worden nageleefd.
- 3.19 Na afloop van de Onderliggende Overeenkomst en deze Overeenkomst blijven leden 16 tot en met 18 van dit artikel 3 en de hierin besproken geheimhouding van kracht.

Artikel 4. Beveiligingsmaatregelen en inspectie

- 4.1 Bewerker neemt alle passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen, welke tenminste behelzen de door Bewerker in bijlage 3 [bijlage toevoegen na interne toetsing] gespecificeerde maatregelen, die deel uitmaakt van deze Overeenkomst, garanderen volgens Bewerker een passend beveiligingsniveau, gelet op de gevoelige aard van de Persoonsgegevens die de Bewerker verwerkt. Deze maatregelen liggen in het verlengde van de beveiligingsmaatregelen die de Verantwoordelijke moet treffen. Bewerker dient aan te tonen dat hij ten minste voldoet aan normen op het gebied van informatiebeveiliging en het servicemanagementsysteem, zoals de Baseline Informatiebeveiliging Gemeenten (BIG), NEN-ISO/IEC 27001:2005 en NEN-ISO-IEC 20000-1:2011 of daaraan gelijkwaardig.
- 4.2 De maatregelen zoals in artikel 4 lid 1 hiervoor genoemd omvatten in ieder geval:

- a) maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Persoonsgegevens die in het kader van de Bewerkersovereenkomst worden verwerkt;
 - b) maatregelen, waaronder maar niet uitsluitend encryptie, om de Persoonsgegevens te beschermen tegen met name onopzettelijke of onrechtmatige vernietiging, verlies, onopzettelijke wijziging, onbevoegde of onrechtmatige opslag, toegang of openbaarmaking;
 - c) maatregelen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Verantwoordelijke;
 - d) een passend informatiebeveiligingsbeleid voor de Verwerking van de Persoonsgegevens.
- 4.3 Bewerker zal de door haar getroffen informatiebeveiligingsmaatregelen evalueren en verscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven. De bewerker houdt een register bij van uitgevoerde beheersmaatregelen dat jaarlijks kan worden ingezien door de Verantwoordelijke.
- 4.4 In Bijlage 3 worden tevens de afspraken tussen Partijen vastgelegd over de inhoud en de frequentie van de rapportages die Bewerker aan Verantwoordelijke oplevert over de beveiligingsmaatregelen. Bewerker rapporteert periodiek met een frequentie van tenminste 2 (twee) maal per jaar aan Verantwoordelijke over de door Bewerker genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin. Daarnaast toont Bewerker alsdan aan dat hij voldoet aan normen op het gebied van informatiebeveiliging en/of het servicemanagementsysteem, zoals opgenomen in Bijlage 3 of gelijkwaardig. Opdrachtnemer kan aan de hand van geldige certificering of een gelijkwaardig bewijsmiddel aantonen dat hij hieraan voldoet. De met de rapportage gemoeide kosten zijn voor rekening van Opdrachtnemer.
- 4.5 De Bewerker stelt de Verantwoordelijke in staat om te kunnen voldoen aan zijn wettelijke verplichting om toezicht te houden op de naleving van de technische en organisatorische beveiligingsmaatregelen door de bewerker. Naast rapportages door de Bewerker kan dat aan de hand van, maar niet beperkt tot, de in artikel 4 lid 4 bedoelde geldige certificering of een gelijkwaardig controle- of bewijsmiddel.
- 4.6 Bewerker dient Verantwoordelijke te informeren indien een van de beveiligingsmaatregelen wijzigt. Partijen actualiseren de beveiligingsmaatregelen zoals bedoeld in lid 1 jaarlijks aan de stand der techniek.
- 4.7 Bewerker staat toe dat Verantwoordelijke op elk door haar gewenst moment de naleving van de beveiligingsmaatregelen door Bewerker inspecteert of dat op verzoek van Verantwoordelijke en op elk door haar gewenst moment de gegevensverwerkingsfaciliteiten van Bewerker door een door Verantwoordelijke aan te wijzen onderzoeksinstantie worden geïnspecteerd in verband met de verwerkingsactiviteiten die onder deze Overeenkomst vallen ('de Inspectie'). Bewerker zal alle redelijkerwijs benodigde medewerking verlenen aan de controle en er voor zorg dragen ook de door hem ingeschakelde derden hiertoe de redelijkerwijs benodigde medewerking zullen verlenen. De Inspectie wordt uitgevoerd door een onderzoeksinstantie, die naar het redelijk oordeel van Verantwoordelijke neutraal en deskundig is. Verantwoordelijke draagt zorg dat de onderzoeksinstantie is verplicht tot geheimhouding van haar bevindingen tegenover derden.
- 4.8 Het uitvoeren van de Inspectie zal niet tot een vertraging van de door Bewerker in het kader van de Onderliggende Overeenkomst en deze Overeenkomst te verrichten werkzaamheden

mogen leiden. Indien dat onverhoopt toch het geval is, zullen Partijen in overleg treden teneinde daarvoor zo snel mogelijk een oplossing te vinden.

- 4.9 Verantwoordelijke zal alle kosten, vergoedingen en onkosten in verband met de Inspectie betalen, met inbegrip van redelijke door Bewerker gemaakte interne kosten, tenzij uit de Inspectie blijkt dat Bewerker is tekortgeschoten in de nakoming van zijn verplichting(en) uit deze Overeenkomst en/of de Onderliggende Overeenkomst.
- 4.9 Verantwoordelijke zal Bewerker een exemplaar van het rapport van de Inspectie verstrekken.
- 4.10 Bewerker voert de door Verantwoordelijke aangegeven aanbevelingen ter verbetering uit binnen de daartoe door Verantwoordelijke te bepalen termijn.

Artikel 4A. Melding Datalek aan Verantwoordelijke

- 4A.1 Bewerker dient Verantwoordelijke onverwijld nadat Bewerker het heeft ontdekt, doch in ieder geval uiterlijk binnen één dag (ook in weekenden), in kennis te stellen van iedere mogelijke inbreuk op de beveiliging (van welke aard dan ook) die (mede) betrekking heeft of kan hebben op de verwerking van Persoonsgegevens en daarbij het hierna verder in artikelen 4A tot en met 4F bepaalde in acht te nemen.
- 4A.2 Melding van een -mogelijk- beveiligingslek en/of Datalek wordt door Bewerker schriftelijk aan Verantwoordelijke gedaan en gericht tot:
het college van burgemeester en wethouders van de gemeente Haarlemmermeer,
t.a.v. Functionaris Gegevensbescherming,
Postbus 250
2130 AG Hoofddorp
en tevens per e-mail aan privacy@haarlemmermeer.nl.
Melding van een Datalek kan telefonisch plaats vinden; een telefonische melding wordt altijd schriftelijk en per e-mail aan privacy@haarlemmermeer.nl door Bewerker bevestigd.
- 4A.3 Bewerker dient aan Verantwoordelijke melding te doen van alle mogelijke beveiligingsincidenten. De melding van een mogelijk beveiligingslek en/of Datalek bevat minimaal in ieder geval de volgende gegevens:
- a. de aard en mogelijke oorzaak van de mogelijke inbreuk, de (mogelijk) getroffen Persoonsgegevens waaronder ook het type gegevens; of Persoonsgegevens verloren zijn gegaan en of redelijkerwijs uitgesloten kan worden dat de persoonsgegevens onrechtmatig kunnen worden verwerkt door het Beveiligingsincident;
 - b. de datum en het tijdstip waarop het mogelijke Beveiligingsincident en/of mogelijke Datalek heeft plaatsgevonden;
 - c. de instanties waar meer informatie over het Beveiligingsincident kan worden verkregen;
 - d. een beschrijving van de vastgestelde en verwachte gevolgen van de inbreuk op de verwerking van de Persoonsgegevens en de daarbij betrokken personen;
 - e. de maatregelen die Bewerker heeft getroffen en zal treffen om de negatieve gevolgen van de inbreuk te beperken, te verhelpen en voor de toekomst te voorkomen.
- Bewerker zal alle maatregelen treffen die nodig zijn om de (mogelijke) schade te beperken en Verantwoordelijke ondersteunen bij meldingen aan betrokkenen en/of autoriteiten.

In geval Bewerker constateert dat een mogelijk beveiligingsincident en/of Datalek heeft plaatsgevonden, zal zij eindgebruikers van de webapplicaties informeren middels een algemene mededeling en een bericht via het controlepaneel dat eindgebruikers na inloggen ontvangen. De inhoud van de mededelingen zullen vooraf met Verantwoordelijke worden afgestemd.

Artikel 4B. Melding Datalek aan Autoriteit Persoonsgegevens

- 4B.1 Bewerker erkent dat Verantwoordelijke onder omstandigheden wettelijk verplicht is om een inbreuk op de beveiliging (van welke aard dan ook) die (mede) betrekking heeft of kan hebben op de Persoonsgegevens die Bewerker verwerkt, aan betrokkenen en/of autoriteiten te melden.
- 4B.2 Bewerker houdt Verantwoordelijke op de hoogte van alle relevante ontwikkelingen met betrekking tot het bij de Autoriteit Persoonsgegevens gemelde Datalek.
- 4B.3 Verantwoordelijke voorziet Bewerker op diens verzoek van alle benodigde informatie berustende bij Verantwoordelijke aangaande het gemelde Datalek, tenzij dit redelijkerwijs niet van Verantwoordelijke kan worden verwacht.

Artikel 4C. Melding Datalek aan Betrokkene, verzoeken van Betrokkenen

- 1. Wanneer een Datalek heeft plaatsgevonden en dit Datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de Betrokkene, stelt Verantwoordelijke Betrokkene overeenkomstig de bepalingen uit de Wet bescherming persoonsgegevens onverwijld op de hoogte van het Datalek.
- 2. In het geval een Betrokkene een verzoek omtrent inzage zoals bedoeld in artikel 35 Wbp, of verbetering, aanvulling of afscherming zoals bedoeld in artikel 36 Wbp, richt aan Bewerker, zal Bewerker het verzoek doorsturen aan Verantwoordelijke en zal Verantwoordelijke het verzoek verder afhandelen, tenzij Verantwoordelijke goedkeuring als hierna in lid 3 vermeld heeft verleend. Bewerker mag de Betrokkene op de hoogte stellen.
- 3. Ingeval van verzoeken tot inzage of correctie als in het voorgaande lid bedoeld, is Bewerker gemachtigd deze zelfstandig uit te voeren, mits Verantwoordelijke daarvoor eerste schriftelijke goedkeuring aan Bewerker heeft verleend. Bewerker informeert Verantwoordelijke onverwijld over het verzoek van Betrokkene, de wijze van afhandeling, alsmede van de afhandeling. Bewerker mag de kosten van de afhandeling aan Verantwoordelijke doorbelasten.

Artikel 4D. Registratie Datalekken

- 1. Bewerker houdt een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.
- 2. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, bedoeld in het derde lid, alsmede de tekst van de kennisgeving aan de betrokkene.
- 3. Bewerker legt het overzicht jaarlijks voor aan Verantwoordelijke .

Artikel 4F. Boetes

Indien aan Verantwoordelijke door de Autoriteit Persoonsgegevens een boete wordt opgelegd wegens het niet, niet tijdig of niet op juiste wijze melden van een Datalek dat is voorgevallen tijdens de uitvoering van de Onderliggende Overeenkomst is Bewerker verantwoordelijk voor voldoening van deze boete tenzij sprake is van verwijtbaar handelen dan wel nalaten door Verantwoordelijke.

Deze bepaling laat het recht van Verantwoordelijke op nakoming en schadevergoeding op grond van deze Bewerkersovereenkomst en de Onderliggende Overeenkomst onverlet.

Artikel 5. Verplichtingen Verantwoordelijke

- 5.1 Verantwoordelijke is ten aanzien van de Verwerking van Persoonsgegevens krachtens deze Overeenkomst de 'Verantwoordelijke' zoals omschreven in artikel 1 sub d Wbp.
- 5.2 Verantwoordelijke gaat ermee akkoord en staat ervoor in dat de verwerking van de Persoonsgegevens overeenkomstig de Bewerkersovereenkomst in overeenstemming is met de Wbp. Indien de Autoriteit Persoonsgegevens een audit houdt en besluit dat de gegevens niet adequaat beveiligd zijn en dit aan de Bewerker te wijten is, betaalt Bewerker de kosten, die verband houden met deze audit en het alsnog adequaat beveiligen en de eventuele boete, welke de Autoriteit Persoonsgegevens aan Verantwoordelijke en/of Bewerker oplegt.

Artikel 6. Aansprakelijkheid

- 6.1 Bewerker is aansprakelijk voor alle schade voortvloeiende uit of verband houdend met het niet-nakomen van deze Overeenkomst dan wel handelen in strijd met de Wbp en alle andere overige (Europese) regelgeving.
- 6.2 Bewerker vrijwaart Verantwoordelijke tegen aanspraken van derden, waaronder Betrokkenen, in verband met het toerekenbaar tekort schieten van Bewerker in de nakoming van de Overeenkomst of overtreding door Bewerker van de Wbp en zal alle daarmee verband houdende en daaruit voortvloeiende kosten (waaronder mede begrepen kosten van juridische bijstand) en schade van Verantwoordelijke vergoeden.
- 6.3 Bewerker zal zich gedurende deze Bewerkersovereenkomst en in geval van beëindiging gedurende de op basis van de Archiefwet verplichte bewaartermijn van Persoonsgegevens adequaat verzekerd hebben en houden voor aansprakelijkheid conform dit artikel.

Artikel 7. Voortdurende verplichtingen

Na afloop van de Onderliggende Overeenkomst en deze Overeenkomst blijven de lopende verplichtingen van Bewerker in stand, zoals, doch niet beperkt tot overdracht, signalering van ongeautoriseerde Verwerkingen en geheimhouding, als ook nader bepaald in de artikelen 3.9, 3.10, 4A.1 en 3.19.

Artikel 8. Teruggave Persoonsgegevens, wettelijke bewaartermijnen

- 8.1 Na afloop van de Onderliggende Overeenkomst en deze Overeenkomst dienen alle Persoonsgegevens, kopieën en bewerkingen daarvan, alsmede alle gegevensdragers waarop

de Persoonsgegevens, kopieën of bewerkingen daarvan zijn of zullen worden vastgelegd, onmiddellijk op eerste verzoek van Verantwoordelijke te worden geretourneerd c.q. verstrekt aan Verantwoordelijke (of een door Verantwoordelijke aan te wijzen derde), dan wel te worden vernietigd, een en ander naar keuze van Verantwoordelijk. Indien naar het redelijk oordeel van Bewerker een zelfstandige wettelijke verplichting van Bewerker het geheel of gedeeltelijk retourneren of vernietigen van de Persoonsgegevens door Bewerker verbiedt of beperkt zal hij Verantwoordelijke zo spoedig mogelijk schriftelijk in kennis stellen van de wettelijke verplichting en daarbij alle relevante informatie verstrekken die Verantwoordelijke redelijkerwijs nodig heeft om te bepalen of vernietiging kan plaatsvinden en, zo ja, onder welke voorwaarden. Indien naar het redelijk oordeel van Verantwoordelijke de wettelijke verplichting (gedeeltelijke) vernietiging van de Persoonsgegevens door Bewerker toelaat zal Bewerker daartoe op verzoek van Verantwoordelijke onverwijld overgaan. Is Verantwoordelijke van oordeel dat vernietiging niet mag plaatsvinden, dan zal zij Bewerker daarvan schriftelijk op de hoogte stellen. Op het moment dat deze Overeenkomst eindigt, zal Bewerker bovendien al zijn medewerking verlenen ter zake van de overdracht van de werkzaamheden inzake de Verwerking van de Persoonsgegevens aan Verantwoordelijke of een opvolgende Bewerker en wel op zo een wijze dat vanaf het moment dat de overdracht plaatsvindt de continuïteit van de dienstverlening maximaal gewaarborgd blijft, althans niet door handelen of nalaten van Bewerker wordt belemmerd. De kosten gemoeid met deze inspanningen van Bewerker, komen voor rekening van Verantwoordelijke voor zover deze kosten niet inbegrepen zijn in de overeengekomen prijzen en vergoedingen van Bewerker voortvloeiende uit de uitvoering van de Onderliggende Overeenkomst.

- 8.2 Verantwoordelijke zal Bewerker adequaat informeren over (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens door Bewerker. Bewerker zal de Persoonsgegevens niet langer Verwerken dan overeenkomstig deze bewaartermijnen. Verantwoordelijke verplicht Bewerker om de in opdracht van Verantwoordelijke Verwerkte Persoonsgegevens bij de beëindiging van de Bewerkerovereenkomst te (doen) vernietigen, tenzij de Persoonsgegevens langer bewaard moeten worden, zoals in het kader van (wettelijke) verplichtingen, dan wel op verzoek van de Verantwoordelijke. Verantwoordelijke kan op eigen kosten een controle laten uitvoeren of vernietiging heeft plaatsgevonden. Het hiervoor bepaalde geldt ook ten aanzien van Persoonsgegevens in back-ups van Bewerker.
- 8.3 Bewerker zal Verantwoordelijke (schriftelijk of elektronisch) bevestigen dat vernietiging van de Verwerkte persoonsgegevens (inclusief de Persoonsgegevens in back-ups) heeft plaatsgevonden. Bewerker zal -indien van toepassing- alle Sub-bewerker die betrokken zijn bij de Verwerking van de Persoonsgegevens op de hoogte stellen van een beëindiging van de Bewerkerovereenkomst en zal waarborgen dat alle Sub-bewerker de Persoonsgegevens (laten) vernietigen (inclusief Persoonsgegevens in back-ups).

Artikel 9. Overdracht rechten en plichten

Deze Overeenkomst en de rechten en verplichtingen uit deze Overeenkomst kunnen door Bewerker niet aan derden worden overgedragen zonder de voorafgaande schriftelijke toestemming van Verantwoordelijke. Verantwoordelijke kan aan haar toestemming voorwaarden verbinden.

Artikel 10. Deelbaarheid

Indien één of meer bepalingen van deze Overeenkomst niet rechtsgeldig blijkt te zijn, zal de Overeenkomst voor het overige van kracht blijven. Partijen zullen over de bepalingen welke niet rechtsgeldig zijn, overleg plegen, teneinde een vervangende regeling te treffen, die wel rechtsgeldig is en zoveel mogelijk aansluit bij de strekking van de te vervangen regeling.

Artikel 11. Toepasselijk recht, algemene voorwaarden en geschillen

- 10.1 Nederlands recht is van toepassing op deze Overeenkomst.
- 10.2 Algemene leveringsvoorwaarden dan wel andere algemene of bijzondere voorwaarden van Bewerker zijn niet van toepassing op deze Overeenkomst en worden door Verantwoordelijke uitdrukkelijk van de hand gewezen.
- 10.3 Deze Overeenkomst vormt een aanvulling op de Onderliggende Overeenkomst. Bij strijdigheid tussen bepalingen uit deze Overeenkomst en de Onderliggende Overeenkomst prevaleren de bepalingen uit deze Overeenkomst.
- 10.4 Alle geschillen voortvloeiende uit of samenhangende met deze Overeenkomst zullen uitsluitend worden voorgelegd aan de bevoegde rechter in het arrondissement Noord-Holland (locatie Haarlem).

ALDUS IN DUPLO OVEREENGEKOMEN

Te Hoofddorp, op [datum]

VERANTWOORDELIJKE
Gemeente Haarlemmermeer

BEWERKER

Bijlage 1 BELEIDSREGELS

<Conform art. 2.5.

Partijen werken beiden in overeenstemming met de door de Autoriteit Persoonsgegevens opgestelde Beleidsregels welke als Bijlage 1 [bijlage toevoegen] aan dit Addendum zijn gehecht.>

Dit document bestaat uit 62 pagina's, je kan er ook voor kiezen om in art. 2.5 te verwijzen naar de betreffende website

Zie voor de meest actuele versie op de website van Autoriteit Persoonsgegevens :

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf

CONCEPT

Bijlage 2 TECHNISCHE EN ORGANISATORISCHE BEVEILIGINGSMATREGELEN

Omschrijving van de maatregelen zoals bedoeld in artikel 4.1 Bewerkersovereenkomst

- 1 Omschrijving van de maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Verwerking van Persoonsgegevens.

Meer in het bijzonder de uitwerking welke (groepen) medewerkers van de Bewerker toegang hebben tot welke Persoonsgegevens, inclusief een omschrijving van handelingen die deze medewerkers uit mogen voeren met de persoonsgegevens.

A. (groepen van) medewerkers die toegang hebben tot welke Persoonsgegevens:

B. handelingen die deze medewerkers uitvoeren met de Persoonsgegevens:

- 2 Omschrijving van de maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, Verwerking, toegang of openbaarmaking.

Meer in het bijzonder de uitwerking van de door Bewerker getroffen technische en organisatorische (beveiligings-)maatregelen en de daarbij gehanteerde beveiligingsnorm.

[beschrijving beveiliging applicatie/platform]

[beschrijving wijze van identificatie/authenticatie/autorisatie en beveiliging daarvan]

[beschrijving beveiliging van wijze van uitwisseling/transport van gegevens]

- 3 Omschrijving van de maatregelen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Verantwoordelijke.

Zoals een periodieke analyse van (security) incidenten, het periodiek uitvoeren van een extern/intern kwetsbaarhedenonderzoek (ethical hack) of het periodiek uitvoeren van controles op beveiliging van systemen.

Rapportage (artikel 4.4 van de Bewerkersovereenkomst)

Bewerker rapporteert periodiek met een frequentie van tweemaal per jaar aan Verantwoordelijke over de door Bewerker genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin.

Bijlage 3 SPECIFIEKE MAATREGELEN

<Conform art. 4.2.

Bewerker neemt alle passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen, gespecificeerd in door Bewerker opgestelde bijlage 3 [bijlage toevoegen], die deel uitmaakt van deze Overeenkomst, garanderen een passend beveiligingsniveau gelet op de gevoelige aard van de Persoonsgegevens die de Bewerker verwerkt>

CONCEPT