gemeente Haarlemmermeer

Overeenkomst gezamenlijke verantwoordelijkheid

Contractpartijen:

1. Medeverantwoordelijke te weten [Naam opdrachtnemer], statutair gevestigd te [plaats], vertegenwoordigd door [naam en/of naam bestuurder]

hierna te noemen: '**Medeverantwoordelijke 1**',

en

2. Medeverantwoordelijke te weten Gemeente Haarlemmermeer, statutair gevestigd te Hoofddorp, vertegenwoordigd door [Directeur]

hierna te noemen: '**Medeverantwoordelijke 2**',

gezamenlijk aan te duiden als: '**Partijen**';

Overwegende dat:

Partijen hebben op [1 april 2020] een Hoofdovereenkomst met betrekking tot [Inhuur ICT-specialisten & Uitvoering resultaatsopdrachten] gesloten. Ter uitvoering van deze Hoofdovereenkomst worden Persoonsgegevens verwerkt.
Partijen hechten grote waarde aan het beschermen van deze Persoonsgegevens. Om die reden leggen Partijen de wederzijdse verantwoordelijkheden vast in deze Overeenkomst en de daarbij behorende bijlagen, te weten:
1. overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen
2. proces rondom het melden van Datalekken en de te verstrekken informatie

1. Definities
De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:

1.1 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de Betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

1.2 Verwerking: 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, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

1.3 Gezamenlijke verantwoordelijkheid: wanneer twee of meer verantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijk verantwoordelijk.

CONCEPT

1.4 Verantwoordelijke: 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; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verantwoordelijke is of volgens welke criteria deze wordt aangewezen.
1.5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte Persoonsgegevens betrekking hebben.
1.6 Hoofdovereenkomst: de hoofdovereenkomst waar deze Overeenkomst gezamenlijke verantwoordelijkheid aan ten grondslag ligt.
1.7 Inbreuk in verband met Persoonsgegevens: 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 (**'Datalek'**).
1.8 Overeenkomst: deze Overeenkomst gezamenlijke verantwoordelijkheid.
1.9 Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens.

2. Totstandkoming, duur en beëindiging van deze Overeenkomst

2.1 Deze Overeenkomst treedt in werking op de datum waarop Partijen deze ondertekenen.
2.2 Deze Overeenkomst is onderdeel van de Hoofdovereenkomst en zal gelden voor zolang de Overeenkomst duurt.
2.3 Indien de Hoofdovereenkomst eindigt, eindigt deze Overeenkomst automatisch; de Overeenkomst kan niet apart worden opgezegd.
2.4 Na beëindiging van deze Overeenkomst zullen de lopende verplichtingen, zoals het melden van Datalekken waarbij Persoonsgegevens van Partijen zijn betrokken en de plicht tot geheimhouding blijven voortduren.

3. Verwerken Persoonsgegevens

3.1 Partijen verwerken Persoonsgegevens alleen op de wijze zoals Partijen dit bij deze Overeenkomst overeenkomen en zullen Persoonsgegevens niet op een andere manier verwerken, tenzij Partijen dit gezamenlijk overeenkomen.
3.2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens Partijen precies zullen verwerken, voor welke verwerkingsdoeleinden en wie voor welk deel verantwoordelijk is.
3.3 Partijen houden zich bij het verwerken van Persoonsgegevens aan de wet en de gegevens worden verwerkt op een behoorlijke, zorgvuldige en transparante wijze.
3.4 Partijen mogen zonder voorafgaande schriftelijke toestemming van elkaar geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.
3.5 Wanneer Partijen met toestemming van elkaar andere organisaties inschakelen, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Overeenkomst.
3.6 Wanneer Partijen een verzoek van een Betrokkene ontvangen ten aanzien van het uitoefenen van zijn of haar rechten, zullen Partijen voor het deel waar zij verantwoordelijk voor zijn, zorgen dat de Betrokkene zijn of haar rechten effectief kan uitoefenen. Deze rechten bestaan uit een verzoek om inzage, correctie, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de Persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.
3.7 Partijen dienen op duidelijke en eenvoudige wijze te communiceren waar de Betrokkene voor het uitoefenen van zijn rechten terecht kan. Hierbij geven partijen aan welke Medeverantwoordelijken er zijn en wie voor welk deel verantwoordelijk is.

CONCEPT

4. Exporteren Persoonsgegevens

4.1 Partijen mogen geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), tenzij:

a.) de andere Partij daaraan voorafgaand schriftelijk toestemming heeft gegeven. De toestemming wordt geacht te zijn verleend indien de andere Partij binnen 15 werkdagen nadat de kennisgeving om een (Sub-)Verwerker in te schakelen per email is verzonden, geen bezwaar heeft gemaakt of bij het sluiten van deze Verwerkersovereenkomst door de acceptatie van de Verwerkers en Subverwerkers opgenomen in Bijlage 1; en

b.) er een besluit is van de Europese Commissie is dat de doorgifte naar het betreffende land over een adequaat beschermingsniveau beschikt; of

c.) de doorgifte geschiedt op basis van het EU Standaard Contract; of

d.) de doorgifte geschiedt op basis van binnen een concern geldende bindende bedrijfsvoorschriften zoals bedoeld in art 47 AVG.

5. Geheimhouding

5.1 Partijen zullen de verstrekte Persoonsgegevens geheimhouden, tenzij dit op basis van een wettelijke verplichting niet kan.

5.2 Partijen zorgen ervoor dat het personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-)contracten op te nemen.

6. Datalekken

6.1 In geval van een ontdekking van een Datalek zullen Partijen elkaar hierover informeren binnen 48 uur overeenkomstig de procedure zoals die is opgenomen in Bijlage 2.

6.2 Partijen zullen elkaar op de hoogte houden van ontwikkelingen rondom het Datalek. Verder zullen Partijen de getroffen maatregelen om het Datalek te beperken, te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen, met elkaar afstemmen.

6.3 Partijen doen elk voor dat deel van de persoonsgegevens waar zij verantwoordelijk voor zijn de melding van een Datalek bij de Toezichthouder. Hetzelfde geldt voor de melding aan de Betrokkenen.

6.4 Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

7. Aansprakelijkheid

7.1 Als een van de Partijen de verplichtingen uit deze Overeenkomst niet nakomt, kunnen zij voor hun deel van de verwerking aansprakelijk gesteld worden.

7.2 De ene Medeverantwoordelijke is niet aansprakelijk voor aanspraken van Betrokkenen of andere personen en organisaties waar de andere Medeverantwoordelijke de samenwerking mee is aangegaan, als dit het gevolg is van het onrechtmatig of nalatig handelen van die Medeverantwoordelijke.

8. Teruggave Persoonsgegevens en bewaartermijn

8.1 Partijen maken in de Hoofdovereenkomst afspraken over de beëindiging van de Hoofdovereenkomst en de daaruit voortvloeiende teruggave en wissing van Persoonsgegevens.

9. Slotbepalingen

9.1 Deze Overeenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op deze Overeenkomst.

CONCEPT

9.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Overeenkomst en de Hoofdovereenkomst, gelden de bepalingen uit deze Overeenkomst ten aanzien van de verwerking van Persoonsgegevens.
9.3 Afwijkingen van deze Overeenkomst zijn slechts geldig wanneer Partijen dit samen schriftelijk overeenkomen.

Aldus door Partijen overeengekomen en ondertekend:

Medeverantwoordelijke 1:
Ondertekend voor en namens [Naam opdrachtnemer]
Naam:
Functie:
Datum en plaats:
Handtekening:

Medeverantwoordelijke 2:
Ondertekend voor en namens gemeente Haarlemmermeer
Naam:
Functie:
Datum en plaats:
Handtekening:

CONCEPT

Bijlage 1: Overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen

Beschrijving verwerkingsactiviteiten door Medeverantwoordelijke 1:	
Verwerkingsdoelen:	
Medeverantwoordelijke 1: (naam, contactgegevens, contactgegevens van de functionaris Gegevensbescherming wanneer de organisatie een dergelijke functionaris heeft)	
Verwerkte Persoonsgegevens:	
Locatieverwerkingen:	
Subverwerkers:	
Bewaartermijn:	

Beschrijving verwerkingsactiviteiten door Medeverantwoordelijke 2:	
Verwerkingsdoelen:	
Medeverantwoordelijke 2: (naam, contactgegevens, contactgegevens van de functionaris Gegevensbescherming wanneer de organisatie een dergelijke functionaris heeft)	
Verwerkte Persoonsgegevens:	
Locatieverwerkingen:	

CONCEPT

Subverwerkers:	
Bewaartermijn:	

CONCEPT

Bijlage 2: Proces rondom het melden van Datalekken en de te verstrekken informatie

Wat is een beveiligingsincident en wanneer moet dit gemeld worden?
Een Datalek is een beveiligingsincident waarbij Persoonsgegevens, die de ene Medeverantwoordelijke namens de andere Medeverantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Elke Medeverantwoordelijke dient voor het deel waar hij/zij verantwoordelijk voor is een melding te maken bij de Toezichthoudende autoriteit wanneer er sprake is van een beveiligingsincident. Het gaat om gegevens die te koppelen zijn aan personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, login-gegevens, cookies, IP-adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens:
- De website met login-gegevens is gehackt of is toegankelijk voor derden.
- Verlies van een laptop of USB-stick met persoonsgegevens.
- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.
- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Een aanval van een hacker op het ICT-systeem.
- Een verloren of gestolen telefoon waar persoonsgegevens op aanwezig zijn.

Wat te doen bij twijfel?
Als je op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stel je jezelf in ieder geval alvast de volgende vragen als hulpmiddel:
- Is er een technisch of fysiek beveiligingsprobleem?
- Gaat het probleem over de beveiliging van Persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware zoals een IMEI-nummer, kunnen hieronder vallen.
- Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteits-)fraude mee kan worden gepleegd, zoals een Burgerservicenummer?
- Zijn er grote hoeveelheden Persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- Gaat het om gegevens van kwetsbare groepen zoals kinderen?
- Worden de Persoonsgegevens beheerd door een leverancier?

Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met:

Medeverantwoordelijke 1: [invoeren naam contactpersoon of afdeling]
Medeverantwoordelijke 2: [invoeren naam contactpersoon of afdeling]

CONCEPT

Waar meld je het beveiligingsincident?
Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met:

Medeverantwoordelijke 1:
[Contactgegevens]

Medeverantwoordelijke 2:
[Contactgegevens]

Geef in je e-mail beantwoording op de onderstaande vragen
De onderstaande vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt wanneer er van het Datalek een melding gemaakt moet worden.

De [invoeren naam contactpersoon of afdeling] kan je helpen met de beantwoording hiervan. Gaarne de vragen zo volledig mogelijk en schriftelijk beantwoorden.

1. Geef een samenvatting van het beveiligingslek/beveiligingsincident/Datalek: wat is er gebeurd? Vermeld hier ook de naam van het betrokken systeem.
2. Welke typen Persoonsgegevens zijn betrokken bij het beveiligingsincident?
   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.
3. Van hoeveel personen zijn de Persoonsgegevens betrokken bij het beveiligingsincident?
   Geef a.u.b. een minimum en maximum aantal personen.
4. Omschrijving groep personen om wiens gegevens het gaat.
   Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van kwetsbare groepen personen, zoals kinderen.
5. Zijn de contactgegevens van de betrokken personen bekend?
   Het kan zijn dat Betrokkenen geïnformeerd moeten worden over het Datalek, kunnen we deze personen in dat geval bereiken?
6. Wat is de oorzaak (root cause) van het beveiligingsincident?
   Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?
7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?
   Geef dit a.u.b. zo specifiek mogelijk aan.

CONCEPT