Overeenkomst Gemeente Nijmegen – [Medeverantwoordelijke] inzake Gezamenlijke Verantwoordelijkheid onder de AVG

Artikel 26 AVG

Overeenkomst in het kader van de Algemene verordening gegevensbescherming tussen de gemeente Nijmegen en [medeverantwoordelijke]

ONDERGETEKENDEN:

de publiekrechtelijke rechtspersoon GEMEENTE , zetelende te Nijmegen aan Korte Nieuwstraat 6 Nijmegen ten dezen rechtsgeldig vertegenwoordigd, door [vertegenwoordiger], [functie],

hierna te noemen: " **de gemeente**'';

en

[medeverantwoordelijke], gevestigd en kantoorhoudende te [adres] , hierbij rechtsgeldig vertegenwoordigd door [vertegenwoordiger]

hierna te noemen: " **medeverantwoordelijke**";

alle bovengenoemde partijen gezamenlijk te noemen: " **partijen**",

Overwegende dat:

- artikel 26 van de Algemene Verordening Gegevensbescherming partijen verplicht tot het sluiten van overeenkomst in het geval er sprake is van gezamenlijke verwerkingsverantwoordelijkheid;
- deze gezamenlijke verwerkingsverantwoordelijkheid toe ziet op het feit dat partijen zelfstandig (bijzondere)(persoons)gegevens verwerken voor (een) gezamenlijk overeengekomen doeleinde(n);
- de partijen op transparante wijze de verdeling met betrekking tot de verantwoordelijkheden uit hoofde van de AVG willen vastleggen in de onderhavige overeenkomst.

VERKLAREN ALS VOLGT TE ZIJN OVEREENGEKOMEN:

Artikel 1 Definities

1.1 Bijlage: ieder aanhangsel bij deze verwerkersovereenkomst, welke een onlosmakelijk deel daarvan uitmaakt.
1.2 Hoofdovereenkomst: de raamovereenkomst] tussen partijen aangegaan op [datum] met inkoopmerk [nummer] en opvolgende overeenkomsten.
1.3 Contactpersoon: degene die belast is met de naleving en handhaving van hetgeen overeengekomen is in deze overeenkomst.
1.4 Toezichthouder: de Autoriteit Persoonsgegevens (AP) is het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens.
1.5 Waar in deze overeenkomst termen worden gebruikt die overeenstemmen met definities uit artikel 4 AVG, wordt aan deze termen de betekenis van de definities uit de AVG toegekend, tenzij anders aangegeven.

Artikel 2 Ingangsdatum en duur

2.1 Deze overeenkomst gaat in op het moment van ondertekening en duurt voort zolang de hoofdovereenkomst van kracht is .

2.2 Deze overeenkomst kan slechts worden opgezegd of ontbonden onder dezelfde voorwaarden als de hoofdovereenkomst.

Artikel 3 Verwerken persoonsgegevens

3.1 Ieder der partijen is zelfstandig verantwoordelijk voor de verwerking van persoonsgegevens, indien en voor zover in de hoofdovereenkomst is vastgelegd dat de verwerking valt onder verantwoordelijkheid van die partij. 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 verantwoordelijke 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 beperking, 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 wie voor welk deel verantwoordelijk is.

Artikel 4 Geheimhouding

4.1 Partijen zullen de verstrekte persoonsgegevens geheim houden, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht.

4.2 Bij een verplichting tot verstrekking zal de partij die eigenaar is van de gegevens direct in kennis gesteld worden van de verstrekking.

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

Artikel 5 Datalekken en beveiligingsincidenten

5.1. In het geval van een datalek is iedere partij zelfstandig verantwoordelijke een afweging te maken of er melding dient te worden gedaan aan de Autoriteit Persoonsgegevens voor zover vallende onder de verantwoordelijkheid van de betreffende partij.

5.2 Vanwege de aard van de samenwerking en de daarbij op iedere partij rustende contextuele verwerkingsverantwoordelijkheid voor de verwerking, is het niet altijd duidelijk of de betrokkenen rechtstreeks geïnformeerd worden over een datalek. In voorkomende gevallen is de partij onder wiens verantwoordelijkheid het datalek valt, ook verantwoordelijke voor het duidelijk en rechtstreeks informeren van de betrokkenen.

5.3 Zodra een van de partijen op de hoogte is van een beveiligingsincident – in dit geval enkel ten aanzien van de verstrekking van persoonsgegevens – moet die partij alle noodzakelijke en passende maatregelen nemen om de gevolgen van het beveiligingsincident te onderzoeken, te reduceren en te herstellen. Daarnaast moet zij de andere partij helpen ervoor te zorgen dat de andere partij kan voldoen aan de privacywetgeving en eventuele wettelijke en/of contractuele verplichtingen (zoals verplichtingen om derden in kennis te stellen, inclusief toezichthouders en betrokkenen) in verband met het beveiligingsincident. Dit betekent dat partijen over en weer- in dit geval enkel ten aanzien van de verstrekking van persoonsgegevens, dus gericht op het transport van de data tot aan de poort van ontvanger – hun medewerking verlenen in het kader van het hiervoor gestelde en eventuele nader instructies van de ene aan de andere partij adequaat zullen opvolgen. Daarbij verschaft de ene partij in ieder geval de informatie aan de andere zoals omschreven in bijlage 2.

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

Artikel 6 Beveiligingsmaatregelen en controle

6.1 Partijen ontwikkelen, implementeren en onderhouden een schriftelijk informatieveiligheidsbeleid dat vereist dat beide partijen passende, technische en organisatorische maatregelen nemen om persoonsgegevens, in het licht van de huidige stand van de techniek, te beschermen tegen inbreuken op beveiliging, vertrouwelijkheid of integriteit en andere ongeautoriseerde of onwettige vormen van verwerking. Deze maatregelen zullen een passend veiligheidsniveau garanderen om een op het risico – in dit geval enkel ten aanzien van de verstrekking van persoonsgegevens, afgestemd beveiligingsniveau te waarborgen.

6.2 Partijen onderkennen dat de hiervoor bedoelde technische en organisatorische maatregelen in de loop van de tijd kunnen veranderen en dat effectieve beveiligingsmaatregelen regelmatige evaluatie en aanpassing van de maatregelen vereisen en dat zij derhalve regelmatig, dan wel periodiek, althans zo vaak als nodig, met elkaar overleggen om de maatregelen op elkaar af te stemmen.

6.3 Partijen zorgen op basis van wederkerigheid voor adequate beveiligingsmaatregelen en treffen hiertoe de (wettelijke)noodzakelijke passende technische en organisatorische maatregelen ter zake van beveiligingsincidenten, waaronder datalekken. Waar mogelijk zullen partijen elkaar bijstand verlenen bij het vervullen van de verplichting om verzoeken te beantwoorden van betrokken, natuurlijke personen die op grond van de AVG de hun toekomende privacyrechten uitoefenen.

Artikel 7 Aansprakelijkheid[1]

7.1 Met betrekking tot het aansprakelijk stellen van één der partijen geldt het bepaalde in de hoofdovereenkomst.

7.2 Indien een partij tekortschiet in de nakoming van een verplichting of verplichtingen uit deze overeenkomst dan is de ene partij jegens de andere partij aansprakelijk conform het bepaalde in de hoofdovereenkomst.

7.3 Indien de ene partij tekortschiet in de nakoming van een verplichting of verplichtingen uit deze overeenkomst, dan kan de andere partij hem in gebreke stellen. De ene partij is echter onmiddellijk in gebreke als de

nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan de partij 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 partij in verzuim.

7.4 Op iedere partij rust een vergaande inspanningsverplichting om te bewerkstelligen dat de verwerking van persoonsgegevens op basis van deze overeenkomst niet onrechtmatig is en geen inbreuk maakt op de rechten van betrokkene(n).

7.5 Partijen zijn aansprakelijk op grond van het bepaalde in artikel 82 AVG, schade of nadeel voortvloeiend uit het niet nakomen van bepalingen uit deze overeenkomst daaronder begrepen. De ene partij is niet aansprakelijk voor schade die het gevolg is van het door de andere partij niet naleven van de AVG of andere wet- of regelgeving. Partijen vrijwaren elkaar voor aanspraken van derden op grond van zulke schade. De vrijwaring geldt niet alleen voor de schade die derden hebben geleden (materieel, maar ook immaterieel), maar ook voor de kosten die de partij moet maken.

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

7.7 De partijen zijn aansprakelijk op grond van het bepaalde in artikel 82 AVG, schade of nadeel voortvloeiende uit het niet nakomen van deze overeenkomst daaronder begrepen.

7.8 De ene partij is aansprakelijk voor de aan de andere partij opgelegde bestuurlijke boete door de toezichthouder als de schade het gevolg is van het onrechtmatig of nalatig handelen van die partij.

7.9 Indien een partij de in artikel 5 lid 1 van deze overeenkomst neergelegde verplichting niet of niet-tijdig nakomt en de toezichthouder de andere partij dientengevolge een bestuurlijke boete oplegt, is die partij aansprakelijk en zal de andere partij een contractuele boete ter hoogte van hetzelfde bedrag opleggen aan die partij. Deze boete is niet vatbaar voor verrekening en opschorting en laat de rechten van de andere partij op nakoming en schadevergoeding onverlet.

Artikel 8 Teruggave persoonsgegevens en bewaartermijn

8.1 Partijen bewaren de persoonsgegevens niet langer dan strikt noodzakelijk en volgen de wettelijke voorschriften inzake de bewaartermijn.

8.2 Bij beëindiging van deze overeenkomst geven partijen de persoonsgegevens aan elkaar terug.

8.3 De overgebleven persoonsgegevens zullen partijen vernietigen na het verstrijken van de wettelijke bewaartermijn.

Artikel 9 Toepasselijk recht en bevoegde rechter

9.1 Op deze overeenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is het Nederlands recht van toepassing.

9.2 Alle geschillen welke betrekking hebben op, voortvloeien uit, of verband houden met deze verwerkersovereenkomst zullen in de eerste plaats onderworpen worden aan geschillenbeslechting buiten rechte, alvorens deze

ter beslechting worden voorgelegd aan de Rechtbank Gelderland, locatie Arnhem, gevestigd te Arnhem aan de Walburgstraat 2-4 (6811 CD), behoudens voor zover dwingende competentie-regels aan deze forumkeuze in de weg zouden staan.

Artikel 10 Overige bepalingen

10.1 De overeenkomst kan worden aangehaald als 'Overeenkomst Gemeente Nijmegen – Medeverantwoordelijke inzake Gezamenlijke Verantwoordelijkheid onder de AVG'.

Aldus overeengekomen en in tweevoud ondertekend te

Nijmegen, ……..

[plaats], ……

……
Gemeente Nijmegen
namens het college van B&W,
[vertegenwoordiger]

……
[Medeverantwoordelijke]
[Vertegenwoordiger]

Bijlage 1: Overzicht van te verwerken persoonsgegevens en verwerkingsdoelen

Het onderstaande geeft een volledig overzicht van de persoonsgegevens die verwerkt zullen worden en voor welk deel van de persoonsgegevens welke partij verantwoordelijke is. Op basis van dit overzicht is het mogelijk om aan te kunnen tonen waar, door wie en voor welk doel de persoonsgegevens worden verwerkt. Daarnaast is het ook mogelijk om op basis van dit overzicht de betrokkenen te kunnen informeren dat hun persoonsgegevens worden verwerkt, zoals is vereist op grond van artikel 13 AVG.

Gemeente Nijmegen

1. Naam verwerking, doeleinden, werkzaamheden, categorieën van betrokkenen, (bijzondere) persoonsgegevens en bewaartermijn(en)

Naam verwerking	Verwerkingsdoeleinden	Werkzaamheden	Categorieën van Betrokkenen	(Bijzondere) persoonsgegevens	Bewaartermijn(en)

Werkzaamheden

[opties hieronder, invullen in tabel]

- Hosting van websites en/of applicaties
- Back-ups maken en restoren
- Applicatiebeheer
- Technisch beheer
- Database beheer
- Helpdesk
- Communicatievoorziening (zoals berichtenverkeer)
- Archiefbeheer
- Vernietiging van gegevensdragers
- Printing, scanning, kopiëren
- Inhoudelijke werkzaamheden die namens de gemeente worden uitgevoerd
- Overig, namelijk:

2. Contactgegevens

Contactpersoon Gemeente Nijmegen	Naam: <contractmanager> E-mail: <algemeen adres afdeling contractmanager> Telefoonnummer:

Medeverantwoordelijke

1. Naam verwerking, doeleinden, werkzaamheden, categorieën van betrokkenen, (bijzondere) persoonsgegevens en bewaartermijn(en)

Naam verwerking	Verwerkingsdoeleinden	Werkzaamheden	Categorieën van Betrokkenen	(Bijzondere) persoonsgegevens	Bewaartermijn(en)

Werkzaamheden

[opties hieronder, invullen in tabel]

- Hosting van websites en/of applicaties
- Back-ups maken en restoren
- Applicatiebeheer
- Technisch beheer
- Database beheer
- Helpdesk
- Communicatievoorziening (zoals berichtenverkeer)
- Archiefbeheer
- Vernietiging van gegevensdragers
- Printing, scanning, kopiëren
- Inhoudelijke werkzaamheden die namens de gemeente worden uitgevoerd
- Overig, namelijk:

2. Contactgegevens

Contactpersoon Medeverantwoordelijke	Naam: E-mail: Telefoonnummer:

Bijlage 2: Aantonen passend niveau van beveiliging

□ Normenstelsel

□ De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk:
…….. (vermeld normenstelsel, gedragscode zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS).

□ De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm zoals de BIO of vergelijkbaar, namelijk:
……..
□ Anders, nl.
……..

□ 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:
  ……

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.

Bijlage 3: 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 partij beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Elke partij dient 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:

Gemeente Nijmegen: de CISO	Medeverantwoordelijke: [contactpersoon]

Waar meld je het beveiligingsincident?
Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met: de CISO via informatiebeveiliging@nijmegen.nl

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 contactpersoon 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.