Model Verwerkersovereenkomst ARIV-2018 NIPV - [naam bedrijf]

Contractnummer: […].
(Datum: ……..)

Inhoud

Verwerkersovereenkomst ARIV-2018

Contractnummer: […].

De ondergetekenden:

1. Het Nederlands Instituut Publieke Veiligheid, zelfstandig bestuursorgaan en publiekrechtelijk rechtspersoon, gevestigd aan de Kemperbergerweg 783, 6816 RW te Arnhem, KVK 56802633, in deze rechtsgeldig vertegenwoordigd door IJle Stelstra, hierna te noemen het 'NIPV' of 'Opdrachtgever'.

en

2. [volledige naam en rechtsvorm contractant], (statutair) gevestigd te [plaats], KVK [KVKnummer] te dezen vertegenwoordigd door ..... *(en .....)* [naam ondertekenaar]
hierna te noemen: [evt verkorte naam], leverancier of Wederpartij,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- voor zover Wederpartij Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, kwalificeert Opdrachtgever als Verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Wederpartij als Verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Wederpartij wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen

In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in de ARIV-2018 of de Verordening, met dien verstande dat een aantal begrippen op de Verwerkersovereenkomst zijn toegespitst. Aldus en in aanvulling daarop wordt onder de volgende begrippen, ongeacht of ze in meervoud of enkelvoud, of als werkwoord of zelfstandig naamwoord worden gebruikt, in deze Verwerkersovereenkomst verstaan:

1.1 ARIV-2018: Algemene Rijksinkoopvoorwaarden 2018

1.2 AVG: Algemene Verordening Gegevensbescherming (In Engels GDPR), ook genoemd De Verordening

1.3 Betrokkene, Derde, Ontvanger, Persoonsgegevens, Toezichthoudende Autoriteit, Verwerker, Verwerking van Persoonsgegevens en Verwerkingsverantwoordelijke: de begrippen zoals gedefinieerd in artikel 4 van de Verordening.

1.4 EER: Europese Economische Ruimte, zijnde alle EU-landen plus Liechtenstein, Noorwegen en IJsland.

1.5 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.

1.6 Overeenkomst: de overeenkomst tussen Opdrachtgever en Wederpartij [titel] van [datum], met kenmerk [kenmerk].

1.7 De Verordening: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (AVG, Algemene Verordening Gegevensbescherming).

1.8 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Leverancier in het kader van de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en ontvangers zijn in Bijlage 1 omschreven.

2.3 Leverancier garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Leverancier garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat en voor zover Leverancier alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang verwerkingsbevoegdheid Leverancier

4.1 Leverancier Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Koper behoudens afwijkende wettelijke voorschriften die op Leverancier van toepassing zijn.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Leverancier in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Koper daarvan voorafgaand aan de Verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.

4.3 Indien Leverancier op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken, informeert hij Koper onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.

4.4 Leverancier heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

Artikel 5. Beveiliging van de Verwerking

5.1 Onverminderd artikel 2.3 treft Leverancier de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Leverancier waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Koper daarom uitdrukkelijk schriftelijk verzoekt, zal Leverancier aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.

5.4 Leverancier Verwerkt Persoonsgegevens niet buiten de EER tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Koper en behoudens afwijkende wettelijke verplichtingen.

5.5 Leverancier informeert Koper zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het eerste en tweede lid.

5.6 Leverancier verleent Koper bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

Artikel 6. Geheimhouding door Personeel van Leverancier

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 8.1 van de ARIV-2018.

6.2 Leverancier toont op verzoek van Koper aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 8.2 van de ARIV-2018.

Artikel 7. Subverwerker

7.1 Bij het uitvoeren van de Overeenkomst mag Leverancier alleen met voorafgaande schriftelijke toestemming van Koper een andere verwerker inschakelen. Deze toestemming, waaraan door Koper nadere voorwaarden kunnen worden verbonden, wordt niet zonder redelijke grond geweigerd.

7.2 Toestemming van Koper laat de eigen verantwoordelijkheid en aansprakelijkheid van Leverancier voor de nakoming van de krachtens de Overeenkomst op hem rustende verplichtingen en de krachtens de belasting-, zorgverzekerings- en sociale verzekeringswetgeving op hem als werkgever rustende verplichtingen, onverlet.

7.3 Wanneer Leverancier met inachtneming van het bepaalde in dit artikel een andere verwerker inschakelt om ten behoeve van Koper verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Artikel 8. Bijstand vanwege rechten van Betrokkene

Leverancier verleent Koper bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Leverancier informeert Koper zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

9.2 Leverancier informeert Koper ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Verwerker bewaart de persoonsgegevens niet langer dan strikt noodzakelijk en in geen geval langer dan tot het einde van deze verwerkersovereenkomst of, indien tussen partijen een bewaartermijn is overeengekomen, niet langer dan deze termijn.

10.2 Bij beëindiging van de verwerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijk verzoek van Verwerkingsverantwoordelijke zal Verwerker de persoonsgegevens vernietigen, doorsturen aan door Betrokkene aangewezen nieuwe Verwerkingsverantwoordelijke of teruggeven aan Verwerkingsverantwoordelijke, naar keuze van Betrokkene/Verwerkingsverantwoordelijke. Het staat de Verwerkingsverantwoordelijke vrij om nadere

redelijke eisen te stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het in de praktijk gangbare bestandsformaat (Recht op dataportabiliteit), en de termijn.

10.3 Op verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker bewijs van het feit dat de gegevens op verzoek van Betrokkene vernietigd of verwijderd zijn. Indien teruggave, vernietiging of verwijdering niet mogelijk is, stelt Verwerker Verwerkingsverantwoordelijke daarvan onmiddellijk op de hoogte. In dat geval garandeert Verwerker dat hij de persoonsgegevens vertrouwelijk zal behandelen en niet langer zal verwerken.

10.4 Bij het einde van de verwerkersovereenkomst zal Verwerker alle derden die betrokken zijn bij het verwerken van persoonsgegevens op de hoogte stellen van de beëindiging van de verwerkersovereenkomst en zal waarborgen dat alle betrokken derden de persoonsgegevens vernietigen of aan Verwerkingsverantwoordelijke overdragen, naar keuze van Verwerkingsverantwoordelijke.

Artikel 11. Informatieverplichting en audit

11.1 Leverancier stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

11.2 Leverancier verleent alle benodigde medewerking aan audits.

Ondertekening

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Het Nederlands Instituut Publieke Veiligheid, namens deze,

NIPV, functienaam: .....

Naam Functionaris .....

Arnhem. Datum: .....

Handtekening:

Wederpartij [naam], namens deze

Wederpartij, functienaam: .....

Naam Functionaris .....

Plaats. Datum: .....

Handtekening:

Bijlage 1. De Verwerking van Persoonsgegevens

In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Overzicht Verwerkingen

Het onderwerp/aard en doel van de Verwerking	
Het soort Persoonsgegevens	
Beschrijving categorieën Persoonsgegevens	
Beschrijving categorieën Betrokkenen	
Beschrijving categorieën Ontvangers van Persoonsgegevens	
Locatie Verwerking Persoonsgegevens	
……	

Sub-verwerker(s)

Naam en contactgegevens sub-verwerker	
Nummer handelsregister van sub-verwerker	
Het onderwerp/aard en doel van de Verwerking	
Het soort Persoonsgegevens	
Beschrijving categorieën van Persoonsgegevens	
Beschrijving categorieën Betrokkenen	
Beschrijving categorieën Ontvangers van Persoonsgegevens	
Locatie Verwerking Persoonsgegevens	
……..	

Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

Bijlage 2. Passende technische en organisatorische maatregelen

In deze bijlage moeten de normen en maatregelen die Wederpartij in het kader van de beveiliging van de Verwerking moet hanteren respectievelijk treffen worden gespecificeerd. Hiervoor kan worden verwezen naar documenten waarin normen en maatregelen zijn vastgelegd, zoals in voorkomend geval het programma van eisen of de offerteaanvraag.

Bij voorkeur is de leverancier ("(sub)Verwerker") ISO27001 en/of NEN7510 gecertificeerd en/of kan jaarlijks een ISAE3402/TPM-verklaring overleggen. Minimaal dient de leverancier ("(sub)Verwerker") onderstaande maatregelen aantoonbaar te hebben getroffen[1]:

- De leverancier gaat bewust om met informatiebeveiliging. De leverancier beschikt hiertoe onder andere over een actueel informatiebeveiligingsbeleid, niet ouder dan 2 jaar.
- Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
- Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
- Het aantal gebruikers met administrator bevoegdheden (in de relevante toepassingen) is beperkt en in overeenstemming met functieniveau en verantwoordelijkheden.
- Er bestaat functiescheiding tussen medewerkers die wijzigingen ontwikkelen en medewerkers die deze in productie zetten. Dit reflecteert zich in de autorisaties binnen de productieomgeving.
- Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie.
- De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.
- De leverancier ("(sub)Verwerker") beschikt over een vorm van compatibiliteit voor SSO (Single Sign On) tegen onze infrastructuur, indien dit niet mogelijk is zal er een vorm van MFA (Multi Factor Authenticatie) afgedwongen moeten worden.
- De leverancier ("(sub)Verwerker") beschikt over een procedure die waarborgt dat gebruikersaccounts (tijdig) worden geblokkeerd en/of verwijderd bij uitdiensttreding.
- Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.
- Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.
- De leverancier ("(sub)Verwerker") heeft inzicht in op welke manieren toegang kan worden verkregen tot de data, buiden de toepassing om. Bijvoorbeeld via ODBC-koppelingen of DBA onderhoudswerkzaamheden op de database.
- Autorisaties op het netwerk en bedrijfs-kritische toepassingen worden periodiek gecontroleerd op juistheid.
- Toegang tot de programmabroncode behoort te worden beperkt.
- De leverancier ("(sub)Verwerker") heeft fysieke maatregelen getroffen om haar informatiesystemen te beveiligen tegen ongeautoriseerde toegang. Het aantal medewerkers met toegang tot de serverruimte is beperkt en in overeenstemming met functieniveau en verantwoordelijkheden.
- Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.
- De leverancier ("(sub)Verwerker") beschikt over een formeel ChangeManagement proces, zodat wordt gewaarborgd dat alleen geautoriseerde en geteste wijzigingen in productie worden genomen. Dit is vastgelegd in een procedure.

[1] De (C)ISO van het NIPV bepaalt welke beveiligingsmaatregelen uit de lijst van toepassing zijn.

- De leverancier (“(sub)Verwerker”) heeft maatregelen getroffen om te voorkomen dat computervirussen en/of wormen het bedrijfsnetwerk en de systemen infecteren.
- De leverancier (“(sub)Verwerker”) beschikt over een back-up en restore procedure om te waarborgen dat er, met het oog op eventuele calamiteiten, actuele back-ups van zowel programmabestanden als gegevensbestanden beschikbaar zijn.
- De leverancier (“(sub)Verwerker”) bewaart back-up tapes op een externe locatie.
- Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.
- Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de “Verwerkingsverantwoordelijke” en de “(sub)Verwerker”.
- Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.
- Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.
- Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.
- Er wordt gewaarborgd dat het ontwerp aansluit op de gewenste functionaliteiten.

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens (waaronder datalekken)

In deze bijlage worden de afspraken over hoe Wederpartij Opdrachtgever over Inbreuken in verband met Persoonsgegevens gaat informeren gespecificeerd.

1. In het geval van beveiligingsincidenten dient zo spoedig mogelijk, doch uiterlijk binnen 24 uur, het NIPV daarover geïnformeerd te worden. Het beveiligingsincident wordt via de e-mail verstuurd aan servicedesk@nipv.nl
2. In het geval van een (mogelijk) datalek dient de mail tevens verstuurd te worden aan privacy@nipv.nl
3. In de e-mail dient u zo concreet en volledig mogelijk het volgende aan te geven:
    - Datum, plaats en tijdstip van de constatering van de (vermoedelijke) Inbreuk in verband met Persoonsgegevens
    - Aard van de Inbreuk in verband met Persoonsgegevens (mogelijke) reden van het incident
    - De categorieën en soort Persoonsgegevens
    - Betrokkene(n)
    - De hoeveelheid persoonsgegevens (records)
    - Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
    - Eventueel logbestand(en)
    - Maatregelen die Wederpartij heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan
    - Uw contactgegevens om u te benaderen voor nader onderzoek
4. In geval van een ernstig beveiligingsincident of datalek dient tevens direct telefonisch contact opgenomen te worden met de NIPV Servicedesk via **088-2747424**
5. Als het NIPV een verzoek tot verwijdering van privacygegevens van “Betrokkene” krijgt, dan stuurt het NIPV vervolgens het verzoek door aan de “Verwerker” om de betreffende gegevens uit haar informatiesyste(e)m(en) te verwijderen. Dit is indien mogelijk inclusief back-up!
   De “Verwerker” dient het verzoek zo spoedig mogelijk, doch binnen 72 uur, uit te voeren en dient hiervan een bevestiging middels e-mail aan het NIPV te sturen via privacy@nipv.nl
   De Functionaris Gegevensbescherming van het NIPV houdt een register bij van alle verwijderingsverzoeken van “Betrokkenen”.
6. Als “Betrokkene” een vraag of een klacht heeft inzake de verwerking van persoonsgegevens door “Verwerkers”, dan zal het NIPV de betreffende “Verwerker” hierover middels e-mail informeren. De “Verwerker” dient zo spoedig mogelijk, doch binnen 24 uur na binnenkomst van de melding (met uitzondering van weekenden en/of officiële feestdagen), te reageren via e-mailadres privacy@nipv.nl
   Afhankelijk van de reactie zal de Functionaris Gegevensbescherming contact opnemen met de klachtencoördinator van het NIPV voor opvolging. De Functionaris Gegevensbescherming houdt een register bij van alle klachten door “Betrokkenen”.