

Bijlage 3b Concept Verwerkersovereenkomst NIPV v2 bij aanbestedingen onder GIBIT-2023 [naam partij]

Hoofdovereenkomst: Applicatie veiligheidsbeeld NIPV2024-EA-03651

Inhoud

Artikel 1. Begrippen.....	2
Artikel 2. Voorwerp van deze Verwerkersovereenkomst	3
Artikel 3. Inwerkingtreding en duur	3
Artikel 4. Omvang verwerkingsbevoegdheid Verwerker	3
Artikel 5. Beveiliging van de Verwerking	3
Artikel 6. Geheimhouding door Personeel van Verwerker.....	4
Artikel 7. Subverwerker	4
Artikel 8. Bijstand vanwege rechten van Betrokkene.....	4
Artikel 9. Inbreuk in verband met Persoonsgegevens.....	4
Artikel 11. Terugbezorgen of wissen Persoonsgegevens	5
Artikel 12. Audits	5
Ondertekening	6
Bijlage 1. De Verwerking van Persoonsgegevens	7
Bijlage 2. Passende technische en organisatorische maatregelen.....	8
Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens.....	9

Verwerkersovereenkomst Applicatie veiligheidsbeeld

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 Algemeen Directeur I.J.J. Stelstra, hierna te noemen 'het NIPV' of 'Opdrachtgever'.

en

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

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- Partijen hebben op <datum> de Raamovereenkomst Applicatie veiligheidsbeeld, hierna Hoofdovereenkomst, afgesloten, op grond waarvan Verwerker de volgende dienst(en) levert aan de Verwerkingsverantwoordelijke: hosting, beheer, support en ontwikkeling van de applicatie veiligheidsbeeld;
- Verwerker verwerkt voor de uitvoering van de Hoofdovereenkomst Persoonsgegevens voor Verwerkingsverantwoordelijke;
- Op de verwerking van Persoonsgegevens door Verwerker zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing;
- Partijen willen in aanvulling op de AVG en de UAVG de volgende afspraken over de verwerking van Persoonsgegevens vastleggen in deze verwerkersovereenkomst (hierna: de Verwerkersovereenkomst);

KOMEN OVEREEN:

Artikel 1. Begrippen

1.1 In deze overeenkomst hebben de volgende (onderstreepte) begrippen de daaropvolgende betekenis:

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

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

Toepasselijke Privacy Wetgeving: Alle op het onderwerp van toepassing zijnde wetgeving met betrekking tot privacy, waaronder, maar niet uitsluitend, de AVG, UAVG, Wet politiegegevens (Wpg) en Telecommunicatiewet

Hoofdovereenkomst: de raamovereenkomst tussen Verwerkingsverantwoordelijke en Verwerker [titel] van [datum], met kenmerk [kenmerk] waar deze verwerkersovereenkomst op toe ziet.

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.

Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende Bijlagen.

1.2 Elk begrip dat hier niet is gedefinieerd, maar dat wel is gedefinieerd in de Toepasselijke Privacy Wetgeving (zoals "persoonsgegeven", "verwerken", etc.), heeft in deze overeenkomst dezelfde betekenis als in die wet.

- 1.3 Elk begrip dat hier niet is gedefinieerd, maar dat wel is gedefinieerd in de Inkoopvoorwaarden GIBIT-2023 heeft in deze overeenkomst dezelfde betekenis als in de GIBIT-2023.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

- 2.1 Deze Verwerkersovereenkomst regelt de Verwerking door Leverancier in het kader van de Hoofdovereenkomst en is onlosmakelijk verbonden met die 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 Verwerker 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 Verwerker garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking.

Artikel 3. Inwerkingtreding en duur

- 3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop de Hoofdovereenkomst door Partijen is ondertekend.
- 3.2 Deze Verwerkersovereenkomst eindigt voor zover en nadat Verwerker alle Persoonsgegevens heeft gewist, terugbezorgd en bestaande kopieën heeft verwijderd met inachtneming van artikel 11 van deze Verwerkersovereenkomst.
- 3.3 Deze Verwerkersovereenkomst is niet tussentijds opzegbaar.

Artikel 4. Omvang verwerkingsbevoegdheid Verwerker

- 4.1 Verwerker Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Verwerkingsverantwoordelijke, tenzij een op Verwerker van toepassing zijnde wettelijk voorschrift hem tot Verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de Verwerking in kennis van dat wettelijk voorschrift, tenzij dat wettelijk voorschrift deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
- 4.2 Verwerker heeft geen zeggenschap over het doel van en de middelen voor de Verwerking als bedoeld in de Verordening.

Artikel 5. Beveiliging van de Verwerking

- 5.1 Onverminderd artikel 2.3 van deze Verwerkersovereenkomst treft Verwerker de technische en organisatorische beveiligingsmaatregelen, zoals bedoeld in artikel 32 AVG. De wijze waarop Verwerker passende technische en organisatorische maatregelen aantoont, staat beschreven in Bijlage 2.
- 5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Verwerker waarborgt een op het risico afgestemd beveiligingsniveau.
- 5.3 Indien en voor zover Verwerkingsverantwoordelijke daarom uitdrukkelijk schriftelijk verzoekt, zal Verwerker aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.
- 5.4 Verwerker Verwerkt Persoonsgegevens niet buiten de EER, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming, zo nodig voorzien van nadere voorwaarden, heeft verkregen van Verwerkingsverantwoordelijke en behoudens afwijkende wettelijke verplichtingen.
- 5.5 Verwerker informeert Verwerkingsverantwoordelijke 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 Verwerker verleent Verwerkingsverantwoordelijke 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 Verwerker

- 6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 18.1 van de GIBIT-2023.
- 6.2 Verwerker waarborgt dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 18.3 van de GIBIT-2023.
- 6.3 De geheimhouding geldt ook nog na de beëindiging van deze Verwerkersovereenkomst.
- 6.4 Bij schending van dit geheimhoudingsartikel geldt de boeteclausule als bedoeld in artikel 18.6 van de GIBIT-2023.

Artikel 7. Subverwerker

- 7.1 De ten tijde van het afsluiten van deze Verwerkersovereenkomst bekende subverwerkers vermeldt Verwerker in tabel 3 van Bijlage 1. Verwerkingsverantwoordelijke verleent hierbij algemene toestemming voor de inschakeling van subverwerkers.
- 7.2 Verwerker houdt na de start van de werkzaamheden Verwerkingsverantwoordelijke op de hoogte van de beoogde inschakeling van nieuwe subverwerkers. Bij de inschakeling van subverwerkers blijven de artikelen 28.2 en 28.4 AVG onverkort van kracht.

Artikel 8. Bijstand vanwege rechten van Betrokkene

- 8.1 Voor zover mogelijk en rekening houdend met de aard van de Verwerking door middel van passende technische en organisatorische maatregelen, verleent Verwerker Verwerkingsverantwoordelijke 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.
- 8.2 Partijen dragen elk de door henzelf in verband met de in het eerste lid te maken kosten.

Artikel 9. Inbreuk in verband met Persoonsgegevens

- 9.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging, maar uiterlijk binnen 24 uur, zodra hij kennis heeft genomen van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.
- 9.2 Verwerker informeert Verwerkingsverantwoordelijke ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.
- 9.3 In geval van een Inbreuk in verband met Persoonsgegevens neemt Verwerker zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen en houdt de Verwerkingsverantwoordelijke hiervan voortdurend op de hoogte.
- 9.4 Verwerker heeft een gedetailleerd logboek van de Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat inzien, wanneer deze daarom vraagt.
- 9.5 Verwerkingsverantwoordelijke beslist of de Inbreuk moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene. Verwerker ondersteunt de Verwerkingsverantwoordelijke waar nodig bij de melding aan de toezichthoudende autoriteit en/of Betrokkene.
- 9.6 Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde Toezichthoudende autoriteit en Betrokkene te maken kosten.

Artikel 10. Aansprakelijkheid

- 10.1 Indien Verwerker tekortschiet in de nakoming van de verplichtingen uit deze Verwerkersovereenkomst kan Verwerkingsverantwoordelijke haar in gebreke stellen.
Verwerker is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichtingen anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is.
Ingebrekestelling geschiedt schriftelijk, waarbij aan de Verwerker 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 Verwerker in verzuim.

~~10.2 Verwerker vrijwaart Verwerkingsverantwoordelijke voor schade of nadeel voor zover ontstaan door aan de Verwerker verwijtbare gedragingen.~~

- 10.23 Indien Verwerker de in artikel 9, lid 1, van deze Verwerkersovereenkomst neergelegde verplichting niet of niet-tijdig nakomt en de toezichthouder de 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 niet vatbaar voor verrekening en opschorting en laat de rechten van Verwerkingsverantwoordelijke op nakoming en schadevergoeding onverlet. **Partijen treden eerst in overleg over het te voeren verweer tegen aanspraken, vorderingen of boetes van derden (toezichthouders) en/of over te voeren schikkingsonderhandelingen.**

Artikel 11. Terugbezorgen of wissen Persoonsgegevens

- 11.1 Na afloop van de Hoofdovereenkomst, of zoveel eerder als overeengekomen, draagt Verwerker er zorg voor dat hij, naar gelang de keuze van Verwerkingsverantwoordelijke, alle Persoonsgegevens wist of terugbezorgt aan Verwerkingsverantwoordelijke en bestaande kopieën verwijdert, tenzij opslag van de Persoonsgegevens op basis van een wettelijk voorschrift verplicht is. In geval van wissen en/of verwijderen van kopieën door Verwerker informeert hij Verwerkingsverantwoordelijke zodra hij dit heeft gedaan.
- 11.2 Partijen kunnen voor afzonderlijke of categorieën Persoonsgegevens bewaartermijnen overeenkomen. Na afloop van de overeengekomen bewaartermijn draagt Wederpartij zorg voor het wissen of terugbezorgen en het verwijderen van kopieën van de betreffende Persoonsgegevens, tenzij opslag van deze Persoonsgegevens op basis van een wettelijk voorschrift verplicht is.

Artikel 12. Audits

- 12.1 Verwerker verleent alle benodigde medewerking aan audits uitgevoerd door een gecertificeerde auditor over de nakoming van de afspraken binnen deze Verwerkersovereenkomst en bijlagen, tenzij Verwerker door middel van een geldige certificering, die periodiek door een geaccrediteerde instelling wordt getoetst, heeft aangetoond dat Verwerker de gemaakte afspraken nakomt.
- 12.2 De kosten van deze audit worden gedragen door Verwerkingsverantwoordelijke (zowel eigen kosten als kosten van Verwerker), tenzij de auditor één of meer tekortkomingen van niet ondergeschikte aard van Verwerker constateert die ten nadele zijn van Verwerkingsverantwoordelijke.

Artikel 13. Overige bepalingen

- 13.1 Op deze overeenkomst is Nederlands recht van toepassing. Alle geschillen, ook als alleen één Partij vindt dat er een geschil is, zullen in eerste instantie worden voorgelegd aan dezelfde bevoegde rechter als genoemd in de Hoofdovereenkomst.

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: 

Verwerker [naam], namens deze

Verwerker, 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	Hosting, beheer hostingomgeving, 3 ^e lijns support & doorontwikkeling t.a.v. Veiligheidsbeeld.nl
Het soort Persoonsgegevens	Gewone persoonsgegevens
Beschrijving categorieën Persoonsgegevens	Naam, functietitel, organisatie, zakelijke telefoonnummer en zakelijk e-mail adres
Beschrijving categorieën Betrokkenen	Gebruikers veiligheidsbeeld.nl
Beschrijving categorieën Ontvangers van Persoonsgegevens	[in te vullen door Verwerker]
Indien van toepassing, het doorgifte-instrument voor laden buiten de EER	[in te vullen door Verwerker]

Sub-verwerker(s)

Naam en contactgegevens sub-verwerker	[in te vullen door Verwerker]
Nummer handelsregister van sub-verwerker	[in te vullen door Verwerker]
Beschrijving van werkzaamheden	[in te vullen door Verwerker]
Locatie Verwerking Persoonsgegevens	[in te vullen door Verwerker]
Indien van toepassing, het doorgifte-instrument voor laden buiten de EER	[in te vullen door Verwerker]

Naam en contactgegevens sub-verwerker	[in te vullen door Verwerker]
Nummer handelsregister van sub-verwerker	[in te vullen door Verwerker]
Beschrijving van werkzaamheden	[in te vullen door Verwerker]
Locatie Verwerking Persoonsgegevens	[in te vullen door Verwerker]
Indien van toepassing, het doorgifte-instrument voor laden buiten de EER	[in te vullen door Verwerker]

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 Verwerker 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.

Het NIPV past conform wet- en regelgeving voor de eigen informatiebeveiliging van haar verwerkingen onder meer de Baseline Informatiebeveiliging Overheid (BIO) toe zoals dit voor alle overheidsorganisaties van toepassing is verklaard. Standaard wordt, tenzij expliciet is aangegeven vanuit de BIO het basisbeveiligingsniveau BBN2 toegepast.

Deze kaders zijn in het kader van deze overeenkomst ook van toepassing op de Verwerker. Als leverancier verklaart u te voldoen aan (privacy)wet- en regelgeving waaronder de AVG en de BIO. Aanvullende of afwijkende maatregelen dient u hieronder aan te geven:

Normenstelsel

- ☐ De verwerker werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten:
..... (vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS) en is volgens deze norm wel/niet gecertificeerd.
- ☐ De verwerker werkt volgens een algemeen erkende overheidsnorm zoals de BIO, of vergelijkbaar, te weten:
.....
- ☐ De verwerker werkt volgens een andere norm, te weten:
.....

Toereikendheid

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

- ☐ Verwerker verstrekt een actueel en geldig certificaat en verklaring van toepasselijkheid (VVT);
- ☐ Rapportages van periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II);
- ☐ Een assurance rapport (TPM) van een auditor die is aangesloten bij NOREA;
- ☐ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven (in lijn met de aanpak uit hoofdstuk 4.4 uit de BIO, een ICV):
.....

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.

Aansluiting bij goedgekeurde gedragscode

- ☐ Verwerker is aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode, te weten

Overige maatregelen:

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

In deze bijlage worden de afspraken over hoe Verwerker Verwerkingsverantwoordelijke 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(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".