**Verwerkersovereenkomst <onderwerp overeenkomst> VNOG**

**Veiligheidsregio Noord- en Oost-Gelderland**, gevestigd aan de Molenmakershoek 14 (7328 JK) te Apeldoorn, te dezen vertegenwoordigd door dhr./mw. <NAAM> , algemeen directeur, hierna te noemen: **Verwerkingsverantwoordelijke**,

en

**<Naam organisatie>,** (statutair) gevestigd aan de <adres>, te <vestigingsplaats> dezen vertegenwoordigd door <naam>, <Functie>, hierna te noemen: Verwerker

hierna afzonderlijk te noemen “Partij”, of gezamenlijk “Partijen”

**OVERWEGENDE DAT**

- Partijen hebben op <datum> de Overeenkomst <onderwerp> hierna Hoofdovereenkomst, afgesloten, op grond waarvan Verwerker de volgende dienst(en) levert aan de Verwerkingsverantwoordelijke: <beschrijving dienstverlening>;
- 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);

**en komen als volgt overeen:**

**Artikel 1 Definities**

1.1 Begrippen uit de AVG en de UAVG die in deze Verwerkersovereenkomst worden gebruikt, hebben dezelfde betekenis.
1.2 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die onlosmakelijk deel uitmaken van deze Verwerkersovereenkomst.

**Artikel 2 Ingangsdatum en duur**

2.1 Deze Verwerkersovereenkomst gaat in op het moment dat de Hoofdovereenkomst tot stand is gekomen, tenzij Partijen anders overeenkomen.
2.2 Deze Verwerkersovereenkomst eindigt op het moment dat de Hoofdovereenkomst is beëindigd en de op basis van artikel 7 van deze Verwerkersovereenkomst gemaakte afspraken over het teruggeven en/of wissen van Persoonsgegevens zijn nagekomen.
2.3 Wanneer Partijen een (nieuwe) Verwerkersovereenkomst overeenkomen, betekent dat dat de oude Verwerkersovereenkomst komt te vervallen.

**Artikel 3 Onderwerp van deze Verwerkersovereenkomst**

3.1 Verwerker verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke voor de uitvoering van de Hoofdovereenkomst en uitsluitend overeenkomstig schriftelijke instructies van Verwerkingsverantwoordelijke, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke wettelijke bepaling hem tot verwerking verplicht. In dat geval zal Verwerker Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, daarvan zonder onredelijke vertraging in kennis stellen, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

3.2 Als een instructie als bedoeld in 3.1 naar het oordeel van Verwerker in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Verwerkingsverantwoordelijke daarvan voorafgaand aan de verwerking in kennis.

3.3 De door Verwerker uit te voeren verwerkingen staan beschreven in tabel 1 van Bijlage 1.

**Artikel 4 Inhoudelijke afspraken**

4.1 **Beveiligingsmaatregelen**
Verwerker zorgt voor passende technische en organisatorische maatregelen om de Persoonsgegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG. Verwerker treft minimaal de technische en organisatorische maatregelen die zijn beschreven in Bijlage 2. Als Verwerkingsverantwoordelijke gedurende de looptijd uitdrukkelijk schriftelijk verzoekt, zal Verwerker aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.

4.2 **Audits**
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.

4.3 **Verwerking buiten de EER**
Verwerker mag geen Persoonsgegevens buiten de Europese Economische Ruimte (EER) (laten) verwerken, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Verwerkingsverantwoordelijke. Voor de verwerkingen buiten de EER die in Bijlage 1 zijn opgenomen heeft de Verwerker toestemming van de Verwerkingsverantwoordelijke.

4.4 **Geheimhouding**
De Persoonsgegevens hebben een vertrouwelijk karakter en Verwerker waarborgt dat degenen die onder zijn gezag persoonsgegevens verwerken, gebonden zijn aan geheimhouding. De personen die werken voor Verwerker en subverwerkers hebben daarom een geheimhoudingsverklaring getekend, of zich op een andere manier schriftelijk gebonden aan de geheimhouding. De geheimhouding geldt ook nog na beëindiging van deze Verwerkersovereenkomst.

4.5 **Subverwerkers**
De ten tijde van het afsluiten van deze Verwerkersovereenkomst bekende subverwerkers vermeldt Verwerker in tabel 3 van Bijlage 1. Bij het uitvoeren van de Hoofdovereenkomst mag Verwerker alleen met voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke een subverwerker inschakelen. Deze toestemming, waaraan door Verwerkingsverantwoordelijke nadere voorwaarden kunnen worden verbonden, wordt niet zonder redelijke grond geweigerd. Bij de inschakeling van subverwerkers blijven de artikelen 28.2 en 28.4 AVG onverkort van kracht.

4.6 **Rechten van betrokkenen**
Als een betrokkene een beroep doet op zijn rechten zoals genoemd in artikel 12 t/m 22 AVG helpt Verwerker, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3, Verwerkingsverantwoordelijke om daarop binnen de wettelijke termijnen een beslissing te nemen.

4.7 **Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging**
Op verzoek van Verwerkingsverantwoordelijke werkt Verwerker altijd mee aan een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG. Verwerker zal tijdig alle relevante informatie en documentatie verschaffen die noodzakelijk is om een DPIA en voorafgaande raadpleging correct en volledig uit te voeren. Indien uit een DPIA blijkt dat aanvullende maatregelen noodzakelijk zijn om de risico's voor betrokkenen te beperken, zal Verwerker meewerken aan implementatie van deze maatregelen.

**Artikel 5 Inbreuk in verband met Persoonsgegevens**

5.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging, zodra hij kennis heeft genomen van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

5.2 Verwerker informeert Verwerkingsverantwoordelijke ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens en verleent bijstand aan Verwerkingsverantwoordelijke.

5.3 In geval van een Inbreuk neemt Verwerker zonder onredelijke vertraging alle mogelijke maatregelen om de Inbreuk te herstellen, de gevolgen te beperken en verdere Inbreuken te voorkomen.

5.4 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.

**Artikel 6 Aansprakelijkheid**

6.1 Eventuele in de Hoofdovereenkomst overeengekomen beperkingen van de aansprakelijkheid hebben ook betrekking op de Verwerkersovereenkomst.

**Artikel 7 Terugbezorgen of wissen persoonsgegevens**

7.1 Na afloop van de Hoofdovereenkomst, of zoveel eerder als overeengekomen, draagt Verwerker er zorg voor dat hij en alle derden die betrokken zijn bij het verwerken van Persoonsgegevens, 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. Op verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker bewijs van het feit dat de gegevens vernietigd of verwijderd zijn.

7.2 Partijen kunnen voor afzonderlijke of categorieën Persoonsgegevens bewaartermijnen overeenkomen. Na afloop van de overeengekomen bewaartermijn draagt Verwerker 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 8 Overige bepalingen**

8.1 Op deze Verwerkersovereenkomst 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,

<Plaats>, <Datum>

<Naam>
Algemeen directeur

<Plaats> , <Datum>

<Naam>
<Functie>

**Bijlage 1: Overzicht van te verwerken persoonsgegevens, contactgegevens partijen en overzicht ingeschakelde subverwerkers**

## 1. Beschrijving van de verwerkingen

| Naam verwerking | Doel van de verwerking | Categorieën Betrokkenen | Categorieën Persoonsgegevens | Categorieën ontvangers | Doorgifte gegevens naar buiten de EER? | Doorgifte-instrument (indien doorgifte gegeven naar buiten de EER) | Aanvullende maatregelen (indien doorgifte gegeven naar buiten de EER) |
|---|---|---|---|---|---|---|---|
| | | | | | [vermeldt bij ja het land] | | |
| | | | | | | | |
| | | | | | | | |

## 2. Contactgegevens

| | |
|---|---|
| **Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)** | Naam:<br><br>Contactgegevens: |
| **Contactpersoon Verwerker (NB: Ook buiten kantooruren)** | Naam:<br><br>Contactgegevens: |

## 3. Ingeschakelde subverwerkers

| Naam en contactgegevens subverwerker | KvK-nummer | Uitbestede verwerkingen | Toepassing (geautomatiseerd systeem) | Doorgifte gegevens naar buiten de EER? | Doorgifte-instrument (indien doorgifte gegeven naar buiten de EER) | Aanvullende maatregelen (indien doorgifte gegeven naar buiten de EER) |
|---|---|---|---|---|---|---|
| | | | | [vermeldt bij ja het land] | | |
| | | | | | | |
| | | | | | | |

**NB:** Substantiële wijzigingen in bovenstaande tabellen geven partijen op korte termijn aan elkaar door.

**Bijlage 2: Passende technische en organisatorische maatregelen**

Naast onderstaande maatregelen dienen er afspraken te worden gemaakt over het melden van security incidenten aan de VNOG. Met name in het kader van de meldplicht datalekken.
De VNOG wil periodiek op de hoogte gebracht worden van voorgevallen beveiligingsincidenten en direct indien het een ernstig beveiligingsincident betreft. Een datalek valt onder een ernstig beveiligingsincident.

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 ("(sub)Verwerker") gaat bewust om met informatiebeveiliging. De leverancier ("(sub)Verwerker") 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, buiten 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 tot die medewerkers die in overeenstemming zijn met functieniveau en verantwoordelijkheden voor die toegang.
- 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.
- De leverancier (“(sub)Verwerker”) heeft maatregelen getroffen om te voorkomen dat systemen of data worden verminkt, beschadigt of onklaar gemaakt.
- 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 media ook 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 over Inbreuken in verband met Persoonsgegevens en rechten van betrokkenen**

1. In het geval van beveiligingsincidenten en/of Inbreuken in verband met Persoonsgegevens dient zo spoedig mogelijk, doch uiterlijk binnen 24 uur, de VNOG daarover geïnformeerd te worden. Het beveiligingsincident en/of Inbreuk wordt via de e-mail verstuurd aan: privacy-security@vnog.nl en ook aan servicedesk@vnog.nl .
2. In de e-mail dient u zo concreet en volledig mogelijk het volgende aan te geven:
    - Aard van het incident
    - (mogelijke) reden van het incident
    - Eventueel logbestand(en)
    - Plaats en tijdstip van het incident
    - Al genomen maatregelen om het incident te mitigeren
    - Uw contactgegevens om u te benaderen voor nader onderzoek
3. In geval van een ernstig beveiligingsincident of Inbreuk dient ook direct telefonisch contact opgenomen te worden met de VNOG servicedesk via **088-3104333**
4. Als de VNOG een verzoek tot verwijdering van persoonsgegevens van “Betrokkene” krijgt, dan stuurt de VNOG vervolgens het verzoek door aan de “Verwerker” om de betreffende gegevens uit haar informatiesyste(e)m(en) te verwijderen. Dit is 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 de VNOG te sturen via privacy-security@vnog.nl .
5. Als “Betrokkene” een vraag of een klacht heeft over de verwerking van persoonsgegevens door “Verwerkers”, dan zal de VNOG de betreffende “Verwerker” hierover via e-mail informeren. De “Verwerker” dient zo spoedig mogelijk, doch binnen 72 uur na binnenkomst van de melding (met uitzondering van weekenden en/of officiële feestdagen), te reageren via e-mailadres privacy-security@vnog.nl.