



**Bijlage 28
Verwerkersovereenkomst
ARBIT-2018**

**IWR2021 | Werkplek-
hardware | Diensten**

ICT Werkomgeving Rijk

Status:
Referentie

versie 1.0
IUC 202006119-5

Inhoud

Artikel 1. Begrippen.....	2
Artikel 2. Voorwerp van deze Verwerkersovereenkomst	3
Artikel 3. Inwerkingtreding en duur	3
Artikel 4. Omvang verwerkingsbevoegdheid Wederpartij	3
Artikel 5. Beveiliging van de Verwerking	4
Artikel 6. Geheimhouding door Personeel van Wederpartij.....	4
Artikel 7. Subverwerker	4
Artikel 8. Bijstand vanwege rechten van Betrokkene.....	4
Artikel 9. Inbreuk in verband met Persoonsgegevens.....	4
Artikel 10. Terugbezorgen of wissen Persoonsgegevens	5
Artikel 11. Informatieverplichting en audit.....	5
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

Instructie:

- Voor zover teksten '<OPTIONEEL>' zijn is dat aangegeven in de tekst.
- Bij teksten waar 'OF' tussen de bepalingen in staat en bij '<OPTIONEEL>', dient de Deelnemer die een Nadere offerteaanvraag uitvoert onder de Raamovereenkomst een keuze tussen de verschillende opties te maken. De overige optie(s) verwijderen uit de overeenkomst. De door de Deelnemer bijgewerkte Verwerkersovereenkomst wordt als concept meegestuurd bij de Nadere oproep tot medediging door de Deelnemer. Inkoop van de Deelnemer vult vervolgens in wat de klant aangeeft.
- Deze Verwerkersovereenkomst kan alleen in combinatie met een Nadere overeenkomst worden gesloten.

N.B. Bij gebruik van de overeenkomst, deze instructie verwijderen.

Verwerkersovereenkomst ARBIT-2018

Contractnummer: [...].

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag,
te dezen vertegenwoordigd door de Minister/Staatssecretaris van/voor [naam portefeuille],
namens deze,
[functienaam en naam ondertekenaar]
hierna te noemen: Opdrachtgever,

en

2. [volledige naam en rechtsvorm contractant],
(statutair) gevestigd te [plaats],
te dezen vertegenwoordigd door
..... (en) [naam ondertekenaar]
hierna te noemen: Wederpartij,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- voor zover Wederpartij Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening kwalificeert 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 artikel 1 van de Algemene Rijksvoorwaarden bij IT-overeenkomsten 2018 (ARBIT-2018). In afwijking daarvan of in aanvulling daarop wordt onder de volgende begrippen in deze Verwerkersovereenkomst verstaan:

- 1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.
- 1.2 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.
- 1.3 Overeenkomst: de Nadere overeenkomst tussen Opdrachtgever en Wederpartij van [datum], met kenmerk [kenmerk] bij de Raamovereenkomst IWR2021|WpHW|Diensten met kenmerk IUC 202006119-5.
- 1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Wederpartij in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

1.5 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 (algemene verordening gegevensbescherming).

1.6 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.7 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst 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, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Wederpartij 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 Wederpartij 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 Wederpartij 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 Wederpartij alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang verwerkingsbevoegdheid Wederpartij

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

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

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

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

Artikel 5. Beveiliging van de Verwerking

- 5.1 In aanvulling op artikel 19 van de ARBIT-2018 en onverminderd artikel 2.3 treft Wederpartij 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. Wederpartij waarborgt een op het risico afgestemd beveiligingsniveau.
- 5.3 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Wederpartij aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.
- 5.4 Wederpartij Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.
- 5.5 Wederpartij informeert Opdrachtgever 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 Wederpartij verleent Opdrachtgever 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 Wederpartij

- 6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 17.1 van de ARBIT-2018.
- 6.2 Wederpartij toont op verzoek van Opdrachtgever aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 17.2 van de ARBIT-2018.

Artikel 7. Subverwerker

Wanneer Wederpartij, met inachtneming van het bepaalde in artikel 23 van de ARBIT-2018, een andere verwerker inschakelt om ten behoeve van Opdrachtgever 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

Wederpartij verleent Opdrachtgever 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 Wederpartij informeert Opdrachtgever 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 Wederpartij informeert Opdrachtgever 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 Na afloop van de Overeenkomst draagt Wederpartij, naar gelang de keuze van Opdrachtgever, zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle Persoonsgegevens. Wederpartij verwijdt kopieën, behoudens afwijkende wettelijke voorschriften.

10.2 **<OPTIONEEL>** Opdrachtnemer [wist of retourneert] de Persoonsgegevens binnen [aantal] [dagen/weken] na afloop van de Overeenkomst, bij gebreke waarvan Opdrachtnemer een boete verschuldigd is van €[bedrag] per dag, met een maximum van €[bedrag].

10.3 **<OPTIONEEL>** Persoonsgegevens worden in de door Opdrachtgever aangegeven vorm en op de door Opdrachtgever aangegeven wijze terugbezorgd.

OF

10.3 **<OPTIONEEL>** De Persoonsgegevens worden als volgt terugbezorgd: [bestandsformaat] [wijze] [adres].

Artikel 11. Informatieverplichting en audit

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

11.2 Wederpartij verleent alle benodigde medewerking aan audits.

11.3 **<OPTIONEEL>** Opdrachtgever laat eenmaal per [...] een audit uitvoeren door een onafhankelijke partij.

OF

11.3 **<OPTIONEEL>** Opdrachtnemer verstrekt met een frequentie van eenmaal per [...], uiterlijk op [datum] aan Opdrachtgever een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de genoemde naleving.

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

Den Haag, [datum]

[Plaats], [datum]

DE MINISTER/STAATSSECRETARIS VAN/VOOR
[naam portefeuille]

[naam Wederpartij]

namens deze,

[functienaam ondertekenaar]

[naam ondertekenaar]

[functie en naam ondertekenaar]

Bijlage 1. De Verwerking van Persoonsgegevens

Instructie:

Voor alle drie de bijlagen geldt:

De interne klant van de Deelnemer, waar nodig in afstemming met een privacy adviseur van de Deelnemer, dient deze in te vullen. Om hierbij faciliterend op te treden, kan Inkoop van de Deelnemer de klant de drie bijlagen die deels al zijn ingevuld, verstrekken.

N.B. Bij gebruik van de overeenkomst, deze instructie verwijderen.

In te vullen door Opdrachtnemer (de verwerker)	
Naam verwerker inclusief contactgegevens	
Contactgegevens vertegenwoordiger verwerker	
Contactgegevens FG van de verwerker	
Naam en contactgegevens subverwerkers	
Worden de gegevens doorgegeven aan één of meer landen buiten de EU?	

In te vullen door Opdrachtgever (de verwerkingsverantwoordelijke)	
Naam verwerkingsverantwoordelijke inclusief contactgegevens	
Contactgegevens vertegenwoordiger verwerkingsverantwoordelijke	
Contactgegevens FG van de verwerkingsverantwoordelijke	
Het onderwerp/aard en doel van de Verwerking	
Het soort Persoonsgegevens	
Beschrijving categorieën Persoonsgegevens	
Beschrijving categorieën Betrokkenen	
Beschrijving categorieën ontvangers van Persoonsgegevens	

Bijlage 2. Passende technische en organisatorische maatregelen

Instructie:

In deze bijlage moeten de normen en maatregelen die Opdrachtnemer 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.

N.B. Bij gebruik van de overeenkomst, deze instructie verwijderen.

- Binnen de Rijksoverheid geldt de [Baseline Informatiebeveiliging Overheid](#) als basis voor de inrichting van informatiebeveiliging.
De beveiliging van Opdrachtnemer dient minstens aan dezelfde eisen te voldoen als de BIO dat voorschrijft op de onderdelen: <<in te vullen door de Deelnemer. Voorafgaand aan het versturen van de offerteaanvraag/het aanbestedingsdocument, dient de afdeling in afstemming met de privacy-contactpersoon van zijn afdeling hier het minimale niveau aan te geven. Houd bij het bepalen van dit niveau o.a. rekening met het soort en de hoeveelheid persoonsgegevens waarover het gaat en daarmee een inschatting van de risico's die spelen, de waarde van de opdracht. >>.
- Opdrachtnemer richt aanvullende maatregelen in op basis van het risico van de Verwerking, die bijvoorbeeld naar aanleiding van een Privacy Impact Assessment (PIA) zijn vastgesteld. Een overzicht van deze maatregelen is hieronder opgenomen.

In te vullen door Opdrachtnemer:

Certificaten	Organisatieonderdeel/ dienst waarop certificaat betrekking heeft	Geldigheidsduur certificaat	Verklaring van toepasselijkheid

Overige kwalificaties:

In te vullen door Opdrachtgever:

Aanvullende beveiligingseisen:

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

Aanleiding

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de Betrokkenen (de mensen van wie de Persoonsgegevens zijn gelekt).

Aangezien Opdrachtnemer Persoonsgegevens gaat verwerken in het kader van het uitvoeren van de Overeenkomst, heeft Opdrachtnemer de verplichting om bij het constateren van een Inbreuk in verband met Persoonsgegevens (art. 33 lid 2 AVG), zonder onredelijke vertraging, dit te melden aan Opdrachtgever.

Verlenen van medewerking

Het <team/afdeling die geïnformeerd moet worden over datalekken invullen door Deelnemer> van <naam Deelnemer of ministerie waartoe de Deelnemer behoort> verzorgt/coördineert de afhandeling van het datalek naar en de melding aan de Autoriteit Persoonsgegevens en zo nodig aan Betrokkenen. Opdrachtnemer dient volledige medewerking te verlenen door alle door Opdrachtgever gevraagde informatie te verstrekken.

Opdrachtgever zal onder meer de volgende gegevens aan Opdrachtnemer vragen:

- Gegevens van zijn organisatie (naam organisatie, adres, postcode, vestigingsplaats, registratie beroeps- of handelsregister);
- Gegevens van de melder (naam, functie, e-mailadres, telefoonnummer(s));
- Gegevens over het datalek (korte samenvatting van het incident waarbij er een Inbreuk is geweest op de beveiliging van Persoonsgegevens, minimaal en maximaal aantal Betrokkenen waarop de Inbreuk op de Persoonsgegevens betrekking heeft, een omschrijving van de groep Betrokkenen waarop de Inbreuk betrekking heeft, wanneer de Inbreuk heeft plaatsgehad (exacte datum of periode), wanneer de Inbreuk is ontdekt);
- Gegevens over de aard van de Inbreuk (lezen, kopiëren, veranderen, verwijderen, vernietigen, diefstal);
- Soort Persoonsgegevens (NAW-gegevens, telefoonnummers, e-mailadressen of andere adressen voor elektronische communicatie, toegangs- of identificatiegegevens, financiële gegevens, BSN, paspoort of kopieën van andere legitimatiebewijzen, geslacht, geboortedatum en/ leeftijd, bijzondere persoonsgegevens (zoals: etniciteit, politieke opvattingen, levensbeschouwing, lidmaatschap vakbond, genetische gegevens, biometrische identificatie, gezondheid, seksuele leven en strafrechtelijke gegevens);
- Welke technische en organisatorische maatregelen genomen zijn om het datalek aan te pakken en om verdere Inbreuken te voorkomen?;
- Technische beschermingsmaatregelen (waren de Persoonsgegevens op het moment van het ontdekken van het datalek (deels) versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? Op welke manier waren de Persoonsgegevens geheel of gedeeltelijk onbegrijpelijk dan wel ontoegankelijk gemaakt?).

Ook indien bovenstaande informatie nog niet bekend is, wordt er direct door Opdrachtnemer contact opgenomen met de contactpersoon/het contactpunt datalekken van Opdrachtgever.

Voorbeelden van datalekken

- Verlies of diefstal van een laptop, smartphone, USB-stick etc. Ook wanneer sprake is van encrypted data!
- Per ongeluk openbaar maken van Persoonsgegevens.
- Het versturen van een e-mail met namen in de CC in plaats van BCC terwijl de geadresseerden niets met elkaar te maken hebben. Of het versturen van een e-mail naar het verkeerde adres.
- Slachtoffer zijn van een phishing mail of hack.

- Het illegaal doorgeven van gebruikersnamen/inlogcodes of toegang hebben tot bestanden waarvoor je niet (meer) bent geautoriseerd.
- Vernietiging van een database met Persoonsgegevens als gevolg van een menselijke fout terwijl een back-up ontbreekt.

In te vullen door Opdrachtgever:

Contactgegevens bij datalekken:

E:

T:

Bereikbaarheid:

In te vullen door Opdrachtnemer:

Contactgegevens bij datalekken:

E:

T:

Bereikbaarheid: