



Concept Beveiligingsovereenkomst (BVO)

van

<Opdrachtnemer> en UWV

bij Overeenkomst voor

Buitenlandse Reizen

Versie:	1.0
Status:	Definitief
Datum:	26 januari 2022

Inhoud

Sectie A: Algemene bepalingen	4
Artikel 1 Begripsbepalingen en onderliggende documenten.....	4
Artikel 2 Looptijd.....	4
Artikel 3 Onderaanneming	4
Artikel 4 Algemene Verordening Gegevensbescherming – bepalingen ten aanzien van de verwerkingsverantwoordelijke	5
Artikel 5 Informatiebeveiliging	5
Bijlage 1: Begripsomschrijvingen BVO	6
Bijlage 2: Dienstenbeschrijving (globaal overzicht)	9

De Partijen:

1. Uitvoeringsinstituut werknemersverzekeringen (UWV), rechtspersoon naar de wet als bedoeld in artikel 2 Wet Structuur uitvoering werk en inkomen, gevestigd te Amsterdam, vertegenwoordigd door <....>, <functie> hierna te noemen: "Opdrachtgever",

en

2. "Opdrachtnemersnaam", gevestigd te "plaatsnaam", vertegenwoordigd door "naam 1^e vertegenwoordiger", lid "bestuursorgaan", en (voor zover van toepassing) "naam 2^e vertegenwoordiger", directeur "afdelingsnaam", hierna te noemen: "Opdrachtnemer".

Middels deze BVO nemen Partijen het volgende in overweging

- Partijen hebben op <datum> een Overeenkomst gesloten voor het organiseren van buitenlandse reizen (de te leveren Diensten) zoals beschreven in de Raamovereenkomst met kenmerk RLA.2022.31.
- Opdrachtnemer is verwerkingsverantwoordelijke.
- Partijen van deze BVO leggen afspraken vast betreffende de te nemen passende technische en organisatorische maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en de bedrijfsvoering van Opdrachtgever te waarborgen.
- De Baseline Informatiebeveiliging Overheid is van toepassing en is op onderdelen nader uitgewerkt in deze BVO.

En komen het volgende overeen:

Sectie A: Algemene bepalingen

Artikel 1 Begripsbepalingen en onderliggende documenten

1. In deze BVO wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan is gegeven in bijlage 1.
2. Van de BVO maken de volgende bijlagen deel uit:
 - a. Begripomschrijvingen
 - b. Dienstenbeschrijving

Artikel 2 Looptijd

1. Deze BVO treedt in werking op de datum van ondertekening van Overeenkomst door contracterende partijen en loopt gedurende de gehele duur van de Dienst zoals gespecificeerd in de Overeenkomst. Jaarlijks vindt een evaluatie plaats op de actualiteit van deze BVO. Aan de hand van de evaluatie is Opdrachtgever gerechtigd deze BVO aan te passen. Partijen gaan bij een aanpassing van de BVO in overleg over de consequenties die de aangepaste BVO heeft op de Dienst.
2. Opdrachtnemer voert de onder de Overeenkomst overeengekomen Diensten uit conform de in/bij deze BVO vastgelegde afspraken.
3. De nietigheid van enige bepaling van deze BVO tast de geldigheid van de overige bepalingen niet aan.
4. Voorwaarden van deze BVO die naar hun aard bedoeld zijn om voort te duren, blijven naar hun strekking van kracht na beëindiging van de BVO.
5. In geval van strijdigheid tussen bepalingen van de BVO en de Overeenkomst, prevaleert de bepaling van de Overeenkomst, tenzij expliciet anders overeengekomen.
6. Partijen zijn niet gerechtigd zonder voorafgaande schriftelijke toestemming van de andere Partij de rechten en/of plichten voortvloeiende uit deze BVO aan een Derde over te dragen.
7. Aan het einde van de Overeenkomst of wanneer Opdrachtgever dit verzoekt, worden bedrijfsmiddelen van Opdrachtgever die aan Opdrachtnemer, zijn Personeel of Onderaannemers ter beschikking zijn of worden gesteld, geretourneerd.
8. Opdrachtnemer waarborgt dat bij de verwerking en opslag van gegevens, te allen tijde de bij de Opdrachtnemer opgeslagen gegevens kunnen worden overgedragen aan Opdrachtgever zodra deze daarom verzoekt.

Artikel 3 Onderaanneming

1. Indien Opdrachtnemer bij de uitvoering van een Overeenkomst, gebruik wil maken van een Onderaannemer, dan zal hij daartoe slechts bevoegd zijn na verkregen Schriftelijke toestemming van Opdrachtgever. De toestemming zal niet zonder redelijke grond worden geweigerd; Opdrachtgever is echter gerechtigd aan het verlenen van deze toestemming voorwaarden te verbinden dan wel deze in tijd te beperken.
2. Wanneer Opdrachtnemer een Onderaannemer inschakelt om ten behoeve van Opdrachtgever activiteiten te verrichten, legt bij een overeenkomst Opdrachtnemer aan deze Onderaannemer dezelfde verplichtingen inzake Beveiliging en gegevensverwerking op als die welke in deze BVO zijn opgenomen.

Artikel 4 Algemene Verordening Gegevensbescherming – bepalingen ten aanzien van de verwerkingsverantwoordelijke

1. Deze sectie is alleen van toepassing indien Opdrachtnemer Verwerkingsverantwoordelijke is voor de verwerking van Persoonsgegevens in het kader van de uitvoering van de Overeenkomst.
2. Opdrachtnemer verwerkt de Persoonsgegevens in overeenstemming met de AVG en eventuele andere van toepassing zijnde wet- en regelgeving met betrekking tot het verwerken van Persoonsgegevens.
3. Opdrachtnemer verwerkt de in het kader van de Overeenkomst ontvangen of verzamelde Persoonsgegevens alleen voor zover dat noodzakelijk is voor de uitvoering van de Diensten op grond van de Overeenkomst.
4. Partijen verstrekken elkaar die informatie en verlenen elkaar die medewerking die nodig is om te voldoen aan de AVG en eventuele andere toepasselijke wet- en regelgeving.
5. Opdrachtnemer heeft passende technische en organisatorische maatregelen, als bedoeld in artikel 32 AVG, getroffen om de Persoonsgegevens te verwerken voor de uitvoering van de Overeenkomst. Opdrachtnemer zal de getroffen maatregelen periodiek evalueren en verscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven. Opdrachtnemer rapporteert op verzoek, Opdrachtgever over de naleving van de getroffen maatregelen. Opdrachtgever zal zo'n verzoek in principe maximaal éénmaal per jaar doen. Indien daar naar het oordeel van Opdrachtgever gegronde redenen voor zijn, kan Opdrachtgever zo'n verzoek vaker doen. Het rapport wordt opgesteld door een onafhankelijk gecertificeerde externe deskundige die een Derden-verklaring afgeeft.
6. Opdrachtnemer zal, onverminderd zijn verplichting tot het melden van Inbreuken in verband met persoonsgegevens aan de Autoriteit persoonsgegevens, Opdrachtgever direct informeren over (vermeende) Inbreuken in verband met persoonsgegevens. Opdrachtnemer zal de consequenties van een Inbreuk in verband met persoonsgegevens gelijktijdig met het informeren van Opdrachtgever over de (vermeende) Inbreuk in verband met persoonsgegevens of, als gelijktijdig met het informeren niet mogelijk is zo spoedig mogelijk na het informeren van Opdrachtgever, inzichtelijk maken. Over de aard en reikwijdte van de te melden Inbreuken in verband met persoonsgegevens zullen Partijen nadere afspraken vastleggen. Opdrachtnemer verstrekt op verzoek van Opdrachtgever informatie over de geïdentificeerde Inbreuken in verband met persoonsgegevens en de genomen maatregelen.
7. Opdrachtgever beslist na overleg met Opdrachtnemer of en hoe de Inbreuk in verband met persoonsgegevens leidt tot een (al dan niet tijdelijke) aanpassing of stopzetting van de Dienst op grond van de Overeenkomst en over het moment dat de aanpassing of stopzetting van de Dienst wordt opgeheven.

Artikel 5 Informatiebeveiliging

1. Opdrachtnemer dient, voor de onder de Overeenkomst overeengekomen Diensten, op basis van ISO 27001:2017 (of gelijkwaardig), gecertificeerd te zijn en te blijven of over een aantoonbare gelijkwaardige baseline op het gebied van Informatiebeveiliging te beschikken.
2. Bij uitzondering, en alleen indien dit in of bij de Overeenkomst nadrukkelijk is bepaald, kan Opdrachtnemer bij het ondertekenen van de Overeenkomst niet ISO 27001:2017 (of gelijkwaardig) gecertificeerd zijn, of over een aantoonbare gelijkwaardige baseline op het gebied van Informatiebeveiliging beschikken, voor de overeengekomen Diensten. Opdrachtnemer dient in dat geval zorg te dragen voor dat hij binnen 60 kalenderdagen (of een door Opdrachtgever en Opdrachtnemer overeengekomen periode) na de ondertekening van de Overeenkomst beschikt over een ISO 27001:2017 (of gelijkwaardig) certificering of over een aantoonbare gelijkwaardige baseline op het gebied van Informatiebeveiliging voor de Diensten die onder deze Overeenkomst vallen.

Bijlage 1: Begripsomschrijvingen BVO

AVG	Algemene Verordening Gegevensbescherming
Bedrijfskritische processen	De processen in de bedrijfsvoering van Opdrachtgever die essentieel zijn voor Opdrachtgever om te voldoen aan zijn verplichtingen.
Beschikbaarheid	De toegang voor geautoriseerde gebruikers op de overeengekomen momenten tot gegevens en aanverwante bedrijfsmiddelen zoals informatiesystemen, oftewel het zorgen voor een ongestoorde voortgang van de informatievoorziening.
Betrokkene	Natuurlijk Persoon op wie een Persoonsgegeven betrekking heeft.
Beveiliging	Het geheel van maatregelen dat getroffen is om de Dienst en/of gegevens tegen een ongewenste verstoring of inbreuk te beschermen.
Beveiligingsincident	Gebeurtenis of actie waarbij de beveiliging van hardware, software, informatie, een proces of organisatie mogelijk in gevaar is gebracht of geheel of gedeeltelijk is doorbroken.
Beveiligingskader	De tussen Opdrachtgever en Opdrachtnemer gemaakte afspraken omtrent de eisen waaraan de beveiliging moet voldoen alsmede het stelsel van toetsen
Beveiligingsplan	Een plan waarin de organisatie van Opdrachtnemer wordt beschreven en waarin staat wat er beveiligd moet worden en hoe deze beveiliging plaats dient te vinden.
Beveiligingsprogramma	Een door Opdrachtnemer opgesteld en door Opdrachtgever goed te keuren overzicht van alle beveiligingsinspanningen en –maatregelen, waarmee Opdrachtnemer een nadere invulling geeft aan het Beveiligingskader en het Beveiligingsplan, voor zover inspanningen en maatregelen buiten de normale werkwijze van de partijen vallen. Opdrachtgever zal dit programma prioriteren en in de tijd uitzetten.
BVO	De onderhavige beveiligingsovereenkomst.
Continuïteitsplan	Plan waarin staat wat te doen bij storingen die ernstige gevolgen hebben voor de organisatie
Derde	Ieder, niet zijnde de betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch de personen die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd zijn om de Persoonsgegevens te verwerken.
Dienst(en)	De door Opdrachtnemer volgens de Overeenkomst te verrichten werkzaamheden of het tot stand te brengen resultaat
Dienstenbeschrijving	Overzicht van de beschrijvingen van de door Opdrachtnemer volgens de Overeenkomst te verrichten werkzaamheden of het tot stand te brengen resultaat.
Doelbinding	Het principe dat iemand (persoon of organisatie) alleen informatie mag vragen, opslaan, gebruiken, delen ten behoeve van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.
GEB	Gegevensbeschermingseffectenbeoordeling (ook wel Data Privacy Impact Assessment – DPIA). Onderzoek waarmee een organisatie inzicht krijgt in de privacy risico's.

Inbreuk in verband met persoonsgegevens (Datalek)	Een inbreuk als bedoeld in artikel 4 sub 12 van de AVG. Het betreft 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 ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Hierbij moet bijvoorbeeld worden gedacht aan het verlies van gegevensdragers waarop Persoonsgegevens staan, het verzenden van Persoonsgegevens naar een geadresseerde voor wie de Persoonsgegevens niet zijn bedoeld, of een gehackte database met Persoonsgegevens.
Informatiebeveiliging	Alles wat men doet om ervoor te zorgen dat men bij informatie kan komen wanneer men dat wil, dat de informatie klopt en de informatie niet bij anderen terecht komt. Het gaat daarbij vaak om een computersysteem, maar dat hoeft niet. Het gaat om maatregelen, procedures en processen die beveiligingsproblemen voorkomen, opsporen, onderdrukken en oplossen. Ontstaat er wel een probleem met de informatie? Dan zorgt Informatiebeveiliging ervoor dat de gevolgen zoveel mogelijk beperkt worden.
Informatiebeveiligingsrisico	Zie risico.
Integriteit	De juistheid, tijdigheid, actualiteit en volledigheid van gegevens en de verwerking daarvan. Een onderdeel van Integriteit betreft de onweerlegbaarheid (non-repudiation). Dit is de mate waarin kan worden aangetoond dat acties of gebeurtenissen hebben plaatsgevonden, zodat deze acties of gebeurtenissen later niet kunnen worden ontkend.
IoT-devices:	Een netwerk van 'slimme' apparaten, sensoren en andere objecten die (vaak verbonden met het internet), gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi)autonome beslissingen en/of acties nemen die van invloed zijn op hun omgeving.
Onderaannemer	Een Derde partij die door Opdrachtnemer wordt ingeschakeld om (delen van) de Diensten te leveren aan Opdrachtgever.
Opdrachtnemer	De contractspartij bij een Overeenkomst met Opdrachtgever.
Overeenkomst	Iedere rechtsbetrekking tussen Opdrachtgever en Opdrachtnemer met betrekking tot levering van een Prestatie, waarvan deze BVO onderdeel uitmaakt.
Personeel	De door partijen bij de uitvoering van de Overeenkomst in te schakelen personeelsleden en/of hulppersonen.
Persoonsgegeven	Een persoonsgegeven als bedoeld in artikel 4 sub 1 van de AVG. Een persoonsgegeven betreft alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
Risico	Een bedreiging of een omstandigheid die de Beschikbaarheid, Vertrouwelijkheid of Integriteit van gegevens of de continuïteit van de levering van de Dienst volgens deze Overeenkomst in gevaar brengt.
Schriftelijk	Onder Schriftelijk wordt in deze BVO verstaan op schrift. Als partijen enig ander communicatiemiddel zoals e-mail, internet of enig ander elektronisch medium gelijk wens te stellen met Schriftelijk, dient dat uitdrukkelijk in de Overeenkomst te worden bepaald.
Weerbaarheid	De mogelijkheid voor te bereiden en aan te passen aan veranderende risico's en bedreigingen en het weerstaan van alle gevaren en het vermogen van de Diensten tot preventie en bescherming en tot snel herstel van verstoringen door incident- en calamiteitafhandeling en mitigatie.
Vertrouwelijke gegevens	Gegevens die naar hun aard alleen met een gerechtvaardigd doel aan Derden mogen worden verstrekt of ter inzage gegeven. Hieronder worden in

	ieder geval de volgende gegevens begrepen (bijzondere) persoonsgegevens, financiële gegevens, competitieve strategie gegevens of marketingplannen.
Vertrouwelijkheid	Het classificeren van de toegankelijkheid van gegevens en waarborgen dat deze alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd, dat wil zeggen vanuit de functie, taken en verantwoordelijkheden hiertoe gerechtigd zijn.
Verwerken	Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, ver/-bewerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Verwerkingsverantwoordelijke	De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van Persoonsgegevens vaststelt.

Bijlage 2: Dienstenbeschrijving (globaal overzicht)

Naam product en/of Dienst	• Organiseren van buitenlandse dienstreizen • Organiseren van pakketreizen • Als intermediair aanbieden van reisverzekeringen • 7*24 uur Duty of Care
Soort product en/of Dienst	Vliegtickets, vouchers voor treinreizen, hotelovernachtingen, taxi, autohuur etc.
Beknopte uitleg en werking product en Dienst	1. UWV vraagt een buitenlandse reis aan bij het aanspreekpunt van Opdrachtnemer 2. Opdrachtnemer werkt een drietal reisalternatieven uit 3. Opdrachtnemer en UWV stemmen bilateraal af welk reisalternatief gewenst is voor de reiziger. 4. UWV bevestigt de definitie reisofferte. 5. Opdrachtnemer boekt/reserveert de reis. 6. Opdrachtnemer verstrekt de reisdocumenten aan de reiziger. 7. Tijdens de reis is Opdrachtnemer beschikbaar voor ondersteuning (Duty of Care).
Doelgroep product en/of dienst	1. Medewerkers van UWV 2. Klanten van UWV (veelal Europese burgers)
Gebruik van Onderaannemers of Subverwerkers in levering Dienst? Zo ja, welke en waarvoor?	<in te vullen door Opdrachtnemer>
Beveiligingsmaatregelen op hoofdlijnen	<in te vullen door Opdrachtnemer>