Rijksdienst voor Ondernemend Nederland

Concept Verwerkersovereenkomst
Reisarrangementen ten behoeve van missies
Rijksdienst voor ondernemend Nederland - Internationaal Ondernemen– Missies / Derde partij

Vertrouwelijk

Contractnummer: […].

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag,
te dezen vertegenwoordigd door de Minister van Economische Zaken en Klimaat,
namens deze,

drs. J.G.M. Wijering
Afdelingsmanager Internationaal Ondernemen
Directie Internationale Programma's,

hierna te noemen: Opdrachtgever,

en

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

hierna gezamenlijk te noemen: 'Partijen'

OVERWEGENDE DAT:

- voor zover Opdrachtnemer Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, kwalificeert Opdrachtgever als Verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Opdrachtnemer als Verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer 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 ARVODI-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 ARVODI-2018: Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van Diensten 2018.

1.2 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

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

1.4 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.

1.5 Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de Persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk Persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als Ontvangers; de Verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn.

1.6 Overeenkomst: de overeenkomst tussen Opdrachtgever en Opdrachtnemer Raamovereenkomst ARVODI-2018 inzake Reisarrangementen ten behoeve van missies [Perceel 1 Inkomende missies /2 Uitgaande missies /3 Reizen met fullservice dienstverlening] van [datum], met kenmerk 202311003.

1.7 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Opdrachtnemer in het kader van de Overeenkomst ten behoeve van Opdrachtgever Verwerkt.

1.8 Toezichthoudende autoriteit: een door een lidstaat ingevolge artikel 51 van de Verordening ingestelde onafhankelijke overheidsinstantie.

1.9 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).

1.10 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens Verwerkt.

1.11 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.12 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 van gegevens.

1.13 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze Verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de Verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking door Opdrachtnemer in het kader van de Overeenkomst en is onlosmakelijk verbonden met 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 Opdrachtnemer 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 Opdrachtnemer 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 deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat Opdrachtnemer alle Persoonsgegevens heeft gewist, terugbezorgd en bestaande kopieën heeft verwijderd met inachtneming van artikel 10 van deze Verwerkersovereenkomst.

3.3 Deze Verwerkersovereenkomst is niet tussentijds opzegbaar.

Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer

4.1 Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever, tenzij een op Opdrachtnemer van toepassing zijnde wettelijk voorschrift hem tot Verwerking verplicht. In dat geval stelt Opdrachtnemer Opdrachtgever 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 Opdrachtnemer 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 Opdrachtnemer 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. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, treft Opdrachtnemer aanvullende maatregelen met het oog op de beveiliging van de Persoonsgegevens.

5.4 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de EER, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming, zo nodig voorzien van nadere voorwaarden, heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of tekortschieten (in de naleving van) technische en organisatorische beveiligingsmaatregelen zoals bedoeld in het eerste en tweede lid.

5.6 Opdrachtnemer 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 Opdrachtnemer

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 13.1 van de ARVODI-2018.

6.2 Opdrachtnemer waarborgt dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 13.2 van de ARVODI-2018.

Artikel 7. Subverwerker

Wanneer Opdrachtnemer, met inachtneming van het bepaalde in artikel 8 van de ARVODI-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

8.1 Voor zover mogelijk en rekening houdend met de aard van de Verwerking door middel van passende technische en organisatorische maatregelen, verleent Opdrachtnemer 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.

8.2 Partijen dragen elk de door henzelf in verband met de in het eerste lid te maken kosten.

8.3 Opdrachtnemer stuurt een verzoek vanuit een Betrokkene zo spoedig mogelijk aan Opdrachtgever.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Opdrachtnemer 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 Opdrachtnemer 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 te maken kosten gerelateerd aan de Inbreuk in verband met Persoonsgegevens.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Overeenkomst, of zoveel eerder als overeengekomen, draagt Opdrachtnemer er zorg voor dat hij, naar gelang de keuze van Opdrachtgever, alle Persoonsgegevens wist of terugbezorgt aan Opdrachtgever 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 Opdrachtnemer informeert hij Opdrachtgever zodra hij dit heeft gedaan.

10.2 Partijen kunnen voor afzonderlijke of categorieën Persoonsgegevens bewaartermijnen overeenkomen. Na afloop van de overeengekomen bewaartermijn draagt Opdrachtnemer 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.

10.3 Opdrachtnemer wist de Persoonsgegevens binnen 4 weken na afloop van de Overeenkomst, of zoveel eerder als overeengekomen, bij gebreke waarvan Opdrachtnemer een boete verschuldigd is van € 500,- per dag, met een maximum van €[maximale opdrachtwaarde]. Betaling van de boete laat de verplichtingen uit artikel 10 en de gehoudenheid van Opdrachtnemer om de schade die het gevolg is van de schending te vergoeden onverlet.

Artikel 11. Informatieverplichting en audit

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

11.2 Opdrachtgever kan een audit van de onder deze Verwerkersovereenkomst vallende verwerkingsactiviteiten (laten) uitvoeren als concrete omstandigheden daartoe aanleiding geven. Opdrachtnemer verleent alle medewerking aan audits, waaronder begrepen audits bij Personeel van Opdrachtnemer, tenzij dit redelijkerwijs niet van hem kan worden verwacht.

11.3 Opdrachtnemer stelt Opdrachtgever onmiddellijk in kennis indien naar zijn mening een instructie van Opdrachtgever in het kader van artikel 11 eerste en/of tweede lid van deze Verwerkersovereenkomst, inbreuk oplevert met een wettelijk voorschrift inzake gegevensbescherming.

11.4 Partijen dragen zelf de kosten die zij maken in verband met de in dit artikel bedoelde informatieverstrekking en audits, waaronder begrepen de kosten van door hen ingeschakelde derden.

11.5 Opdrachtgever is te allen tijde bevoegd om naar aanleiding van de op grond van dit artikel verkregen informatie nadere maatregelen voor te stellen. Opdrachtnemer is gehouden aan die maatregelen in redelijkheid uitvoering te geven.

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

Den Haag, [datum]	[Stad/Plaats, datum]
DE MINISTER/STAATSSECRETARIS VAN ECONOMISCHE ZAKEN EN KLIMAAT, namens en in opdracht van drs. J.G.M. Wijering, Afdelingsmanager Internationaal Ondernemen	Opdrachtnemer
J. van Putten Teammanager Inkoop	Naam ondertekenaar Functie Ondertekenaar

Bijlage 1. De Verwerking van Persoonsgegevens

In te vullen door Opdrachtgever (de Verwerkingsverantwoordelijke)	
Naam Verwerkingsverantwoordelijke inclusief contactgegevens	De Minister van Economische Zaken en Klimaat, namens deze de algemeen directeur Rijksdienst voor Ondernemend Nederland: Dhr. A. Choho (Algemeen directeur RVO) Postbus 93144, 2509 AC Den Haag
Contactgegevens vertegenwoordiger Verwerkingsverantwoordelijke	Directie Internationale Programma's, afdeling Internationaal Ondernemen drs. J.G.M. Wijering (Afdelingsmanager Internationaal Ondernemen) Postbus 93144, 2509 AC Den Haag
Contactgegevens FG van de Verwerkingsverantwoordelijke	Privacy Control Team RVO avg@rvo.nl
Het onderwerp/aard en doel van de Verwerking	1. Afhandelen reserveringen (reizen en diensten); 2. Aanbieden van reizen; 3. Aanbieden van nieuwsbrieven;
Het soort Persoonsgegevens	• Voor- en achternaam, geslacht, geboortedatum, nationaliteit, adres, telefoonnummer (vast en mobiel) en e-mailadres; • Bedrijfsnaam en vestigingsplaats van het bedrijf waar de reiziger werkzaam is; • Paspoortnummer en geldigheid paspoort; • creditcardnummer en vervaldatum; • Gebruikersnamen, wachtwoorden en andere inloggegevens; • Gegevens over maaltijdvoorkeuren en/of dieetwensen. • Gegevens over gezondheid ten behoeve van assistentie tijdens reis of voor faciliteiten die aansluiten bij de medische behoeften van de reiziger.
Beschrijving categorieën Persoonsgegevens	• Gewone persoonsgegevens • Gevoelige persoonsgegevens • Bijzondere persoonsgegevens
Beschrijving categorieën Betrokkenen	• Deelnemers van een missie en/of evenement die een reis maken; • Verwerker die namens de deelnemer reizen en diensten reserveert; • Medewerkers van Internationaal Ondernemen die betrokken zijn bij organisatie van missies en evenementen; • Organisaties die diensten (zoals autoverhuur, taxi, hotels) leveren en door de verwerkers namens deelnemer wordt gereserveerd.
Beschrijving categorieën ontvangers van Persoonsgegevens	• Verwerker die namens de deelnemer reizen en diensten reserveert; • Medewerkers van Internationaal Ondernemen die betrokken zijn bij organisatie van missies en evenementen; • Organisaties die diensten (autoverhuur, taxi, hotels) leveren en door de verwerkers namens

	deelnemer wordt gereserveerd.
Locatie Verwerking Persoonsgegevens	Nederland

In te vullen door Opdrachtnemer (de verwerker)	
Naam Verwerker inclusief contactgegevens	
Contactgegevens vertegenwoordiger Verwerker	
Contactgegevens FG van de Verwerker	
Worden de gegevens doorgegeven aan een of meer landen buiten de EER?	Ja

Naam en contactgegevens subverwerker	Organisaties die diensten leveren (missies en evenementen organiseren
Nummer handelsregister van subverwerker	
Het onderwerp/aard en doel van de Verwerking	Reservering van diensten (zoals autoverhuur, taxi, hotels) door de dienstenleverancier door de verwerker in naam van de deelnemer.
Het soort Persoonsgegevens	• Voor- en achternaam, geslacht, geboortedatum, nationaliteit, adres, telefoonnummer (vast en mobiel) en e-mailadres; • Bedrijfsnaam en vestigingsplaats van het bedrijf waar de reiziger werkzaam is; • Paspoortnummer en geldigheid paspoort; • creditcardnummer en vervaldatum; • Gebruikersnamen, wachtwoorden en andere inloggegevens; • Gegevens over maaltijdvoorkeuren en/of dieetwensen. • Gegevens over gezondheid ten behoeve van assistentie tijdens reis of voor faciliteiten die aansluiten bij de medische behoeften van de reiziger.
Beschrijving categorieën van Persoonsgegevens	• Gewone persoonsgegevens • Gevoelige persoonsgegevens • Bijzondere persoonsgegevens
Beschrijving categorieën Betrokkenen	• Deelnemers van een missie en/of evenement die een reis maken.
Beschrijving categorieën Ontvangers van Persoonsgegevens	Deelnemers van een missie en/of evenement die een reis maken.
Locatie Verwerking Persoonsgegevens	Zowel binnen als buiten de EER. Afhankelijk van locatie van de dienstenleveranciers.

Bijlage 2. Passende technische en organisatorische maatregelen

- Binnen de Rijksoverheid geldt de Baseline Informatiebeveiliging Overheid (BIO) 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: BBN-2
- 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:

De toepassing valt in risicoprofiel R3 van het cloudbeleid.

De leverancier dient, uitgaande van het publieke cloudbeleid van EZK, de volgende maatregelen te treffen:

1. De leverancier beschikt over een geldige ISO-27001 certificering (of gelijkwaardig) en de volledige lifecycle van de cloud toepassing valt binnen de scope van deze certificering.
2. Er zijn afspraken aanwezig hoe overdracht van data en/of software geschiedt in geval van beëindiging van de overeenkomst en welke verplichtingen de leverancier hierin heeft (exit strategie).
3. De leverancier verplicht zich beveiligingsincidenten relevant aan de dienstverlening voor RVO binnen 4 uur na constatering rechtstreeks te melden aan het Security Office van RVO (rvoinformatiebeveiliging@rvo.nl) onder vermelding van de opdrachtgever binnen RVO.
4. De leverancier verplicht zich geconstateerde beveiligingsissues t.a.v. de door hen geleverde public cloud toepassing op te lossen. Hiertoe meldt de leverancier binnen 48 uur aan RVO de termijn waarop de oplossing gerealiseerd is.
5. De leverancier verplicht zich mee te werken aan audits op het gebied van informatiebeveiliging en privacy geïnitieerd door de opdrachtgever.
6. De leverancier verplicht zich inzichtelijk te maken welke andere partijen betrokken zijn bij de invulling van de overeenkomst. Wijzigingen in de betrokken partijen worden schriftelijk gecommuniceerd aan de opdrachtgever binnen RVO én aan de RVO IMP Servicedesk.
7. Er zijn afspraken aanwezig op welke wijze de leverancier data binnen de contractuele doelbinding van de opdrachtgever doorgeeft aan derde partijen (bijv. backups, logfiles, telemetrie, etc.). Voor doorgifte van data binnen de contractuele doelbinding naar verwerkers buiten de EU/EER ruimte is expliciete toestemming nodig van de opdrachtgever.
   Er zijn afspraken aanwezig op welke wijze de leverancier deelneemt aan de door RVO ingerichte crisis organisatie.

Uit de expliciete risicoanalyse blijkt dat vertrouwelijkheid (V) een score van midden oplevert. In dit geval gelden aanvullend de volgende eisen:

8. De leverancier kan aantonen dat voldaan wordt aan ISO-270179.
9. De leverancier past encryptie toe op de data. Encryptie wordt gebruikt voor data-in-rest, data-in-use en data-in-transit. Er zijn expliciete afspraken gemaakt met de leverancier over beheer van de encryptiesleutels.
10. Met de leverancier dient een SLA afgesloten te worden met een periodieke rapportage van tenminste 1x per 4 maanden. In de SLA rapportage dient tenminste aandacht te zijn gegeven aan onderstaande punten: a) (ernstige) beveiligingsincidenten en de afhandeling daarvan b) gemaakte backups en verificatie van deze backups c) onderzoek van logfiles en resultaten hieruit d) gebruik van diagnostische gegevens en logboeken door derde partijen.
11. De leverancier kan aantonen dat deze voldoet aan ISO-2701810 .

Aanvullende maatregel:
Leverancier dient organisatorische en technische maatregelen te nemen op basis van risicoanalyse bij doorlevering van gegevens aan organisaties die missies en evenementen organiseren buiten de EER. Hiervoor wordt verwezen naar de website van de Autoriteit persoonsgegevens (Doorgifte persoonsgegevens buiten de EER | Autoriteit Persoonsgegevens).

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

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 c.q. Verwerkt 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
Opdrachtgever 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 (beschreven in bijlage 1) (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: rvoinformatiebeveiliging@rvo.nl

In te vullen door Opdrachtnemer:
Contactgegevens bij datalekken:
E-mail: