

Bijlage 4b Concept Verwerkersovereenkomst ARBIT-2022

Contractnummer: 202302158.

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag,
te dezen vertegenwoordigd door de De Minister van Economische Zaken en Klimaat,
namens deze,
de heer drs. J.P. van Kaam, Directeur Directie Bestuur, JZ en Communicatie van de Rijksinspectie
Digitale Infrastructuur,
Rijksinspectie Digitale Infrastructuur,
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, kwalificeert Opdrachtgever 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 de ARBIT-2022 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 ARBIT-2022: Algemene Rijksvoorwaarden voor IT-overeenkomsten 2022.
- 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 Wederpartij [titel] van [datum], met kenmerk [kenmerk].
- 1.7 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Wederpartij in het kader van de Overeenkomst ten behoeve van Opdrachtgever Verwerkt.
- 1.8 Toeziethoudende 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 Wederpartij 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 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.

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 voor zover en nadat Wederpartij 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 Wederpartij

- 4.1 Wederpartij Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever, tenzij een op Wederpartij van toepassing zijnde wettelijk voorschrift hem tot Verwerking verplicht. In dat geval stelt Wederpartij 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 Wederpartij 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 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 EER, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming, zo nodig voorzien van nadere voorwaarden, 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-2022.
- 6.2 Wederpartij waarborgt dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 17.2 van de ARBIT-2022.

Artikel 7. Subverwerker

Wanneer Wederpartij, met inachtneming van het bepaalde in artikel 23 van de ARBIT-2022, 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 Wederpartij 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.

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, of zoveel eerder als overeengekomen, draagt Wederpartij er zorg voor dat hij, naar gelang de keuze van Opdrachtgever, alle Persoonsgegevens wist of terugbezorgt aan Opdrachtgever en bestaande kopieën verwijderd, tenzij opslag van de Persoonsgegevens op basis van een wettelijk voorschrift verplicht is.
In geval van wissen en/of verwijderen van kopieën door Wederpartij 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 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.
- 10.3 Wederpartij bezorgt terug de Persoonsgegevens binnen 30 dagen na afloop van de Overeenkomst, of zoveel eerder als overeengekomen, bij gebreke waarvan Wederpartij een boete verschuldigd is van € 500,- excl. btw per dag, met een maximum van:
 - laag risico: boete is € 500,- per dag, tot een maximum van de opdrachtwaarde;
 - midden risico: boete is € 1.000,- per dag, tot een maximum van de opdrachtwaarde;
 - hoog risico: boete is € 2.500,- per dag, tot een maximum van de opdrachtwaarde.Betaling van de boete laat de verplichting uit dit lid en de gehoudenheid van Wederpartij om de schade die het gevolg is van de schending te vergoeden onverlet.
- 10.4 Persoonsgegevens worden in de door Opdrachtgever aangegeven vorm en op de door Opdrachtgever aangegeven wijze terugbezorgd.

Artikel 11. Informatieverplichting en audit

Om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst door Wederpartij zijn en worden nagekomen kan Opdrachtgever overeenkomstig artikel 5 van de ARBIT-2022 Wederpartij om informatie verzoeken of een audit laten uitvoeren.

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

Den Haag, [datum]

[Plaats], [datum]

De Minister van Economische Zaken en Klimaat
namens deze,
de heer drs. J.P. van Kaam
Directeur Directie Bestuur, JZ en Communicatie
Rijksinspectie Digitale Infrastructuur:

[naam Wederpartij]

mevrouw drs. M. Jacobs
Teammanager Inkoop Uitvoering Centrum EZK

[naam ondertekenaar]
Functie

Bijlage 1. De Verwerking van Persoonsgegevens

In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

In te vullen door Wederpartij (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?	

Overzicht Verwerkingen

In te vullen door Opdrachtgever (de verwerkingsverantwoordelijke)	
Naam verwerkingsverantwoordelijke inclusief contactgegevens	Rijksinspectie Digitale Infrastructuur Emmasingel 1 9726 AH Groningen
Contactgegevens vertegenwoordiger verwerkingsverantwoordelijke	Helma ter Horst (Privacy Coördinator) Helma.thorst@rdi.nl Natalie Nieuwland (Privacy Coördinator) Natalie.nieuwland@rdi.nl
Contactgegevens FG van de verwerkingsverantwoordelijke	FG van ministerie van EZK en LNV Carola Overdevest c.c.m.overdevest@minezk.nl
Het onderwerp/aard en doel van de Verwerking	De RDI heeft een lopend contract lopen voor het uitvoeren van KTO's waarbij het contract in oktober 2023 afloopt. De RDI is daarom op zoek naar een nieuwe leverancier. Voor de komende vier jaar wenst de RDI een Raamovereenkomst te sluiten met een Opdrachtnemer voor het meten van de klanttevredenheid. De RDI streeft ernaar de door haar verkregen informatie van de klant en stakeholders over hoe de dienstverlening van de RDI (in meest brede zin van het woord) in de maatschappij wordt ervaren, te benutten om de dienstverlening te verbeteren. De informatie gebruikt de RDI om de resultaten en processen verder te optimaliseren om klanten en stakeholders (nog) sneller en beter van informatie te voorzien. De KTO's zijn voor de RDI een belangrijk instrument om deze informatie en ervaringen op te halen. De RDI heeft te maken met heel diverse doelgroepen, hierdoor is maatwerk noodzakelijk. De RDI werkt daarom momenteel met losse eenmalige KTO's gericht op een specifieke doelgroep. In een dergelijk KTO kan de RDI heel gericht ervaringen en behoeftes opvragen bij haar klanten en stakeholders. Momenteel heeft de RDI geen behoefte aan doorlopende KTO's,

	maar aan eenmalige KTO's in combinatie met advies. De RDI streeft ernaar om per jaar vier eenmalige KTO's uit te voeren. De KTO's bestaan uit online vragenlijsten waarin de tevredenheid over de dienstverlening en communicatie van de RDI wordt uitgevraagd. Tevens is er in deze onderzoeken voor klanten de ruimte voor toelichtingen en verbeter suggesties. Naast het ophalen van cijfers, is het vooral belangrijk om uit de respons verbeteracties te destilleren. De KTO's worden voor specifieke doelgroepen (bijvoorbeeld vergunninghouders voor portofoongebruik en maritieme registratiehouders) ingezet en hebben geen continu karakter. De RDI heeft geen kant-en-klare planning voor de onderzoeken. Er wordt gekeken naar wat er op een bepaald moment leeft binnen en buiten de organisatie. Het is van belang dat er een online Systeem met Dashboard(s) beschikbaar wordt gesteld, waarin onderzoeken worden ingericht, van waaruit de uitnodigingen worden verstuurd aan de doelgroep en waarin de resultaten elke 30 minuten worden ververs en te raadplegen zijn. De responsdata kan de RDI downloaden in een (bij voorkeur) Excel-bestand. (Eenvoudige) onderzoeken moeten door de RDI zelf kunnen worden gedaan met behulp van het KTO-systeem. Deze onderzoeken moeten ten minste op een eenvoudige manier resultaten kunnen laten zien middels een export naar Excel en via een "basis" Dashboard.
Het soort Persoonsgegevens	<u>Van respondenten:</u> • E-mailadressen • Telefoonnummers • Inge vulde enquête <u>Van medewerkers van de RDI</u> • E-mailadres <i>Dit overzicht kan op termijn verder aangevuld worden.</i>
Beschrijving categorieën Persoonsgegevens	Gewone Persoonsgegevens (e-mailadressen en telefoonnummers) zijnde alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gevoelige persoonsgegevens (ingevulde enquête) brengen een groter privacyrisico met zich mee dan gewone persoonsgegevens, maar worden wettelijk niet anders behandeld.
Beschrijving categorieën Betrokkenen	• De respondenten op het onderzoek • Medewerkers van de RDI

	Medewerkers van de partij die de onderzoeken gaat uitvoeren <i>Dit overzicht kan op termijn verder aangevuld worden.</i>
Beschrijving categorieën Ontvangers van Persoonsgegevens	- Behandelend medewerkers van de Opdrachtgever - Behandelend medewerkers van de RDI <i>Dit overzicht kan op termijn verder aangevuld worden.</i>
Locatie Verwerking Persoonsgegevens	

Subverwerker(s)

Naam en contactgegevens subverwerker	
Nummer handelsregister van subverwerker	
Het onderwerp/aard en doel van de Verwerking	
Het soort Persoonsgegevens	
Beschrijving categorieën van Persoonsgegevens	
Beschrijving categorieën Betrokkenen	
Beschrijving categorieën Ontvangers van Persoonsgegevens	
Locatie Verwerking Persoonsgegevens	
.....	

Bijlage 2. Passende technische en organisatorische maatregelen

Waar onderstaand wordt gesproken over Wederpartij, wordt bedoeld <naam Wederpartij> (hierna:..), alsmede derden aan wie <naam Wederpartij> werkzaamheden uitbesteed. Deze derden treden op als subverwerker van <naam Wederpartij> Op de Wederpartij en subverwerker is Artikel 7 van deze Verwerkersovereenkomst van toepassing.

- Specifieke uitwerking van de van toepassing zijnde maatregelen vindt plaats op basis van het karakter van de door Opdrachtgever aan Wederpartij gevraagde dienstverlening.
- Opdrachtgever dient Wederpartij te voorzien van alle benodigde informatie die nodig is om de door Wederpartij te verrichten werkzaamheden uit te kunnen voeren binnen de voor de Opdrachtgever geldende kaders.
- Wederpartij dient Opdrachtgever tijdig op de hoogte te stellen van omstandigheden die het passend implementeren van de volgens Opdrachtgever geldende kaders niet of niet volledig mogelijk maken.
- Bij afwijking van de geldende kaders bepalen Opdrachtgever en Wederpartij in goed overleg met welke alternatieven toch een passend niveau qua beveiliging kan worden gerealiseerd.
- Indien er middelen die door Opdrachtgever in bruikleen worden gegeven aan Wederpartij, worden de van toepassing zijnde maatregelen vastgelegd in de bruikleenovereenkomst.

Overige afspraken:

- Binnen de Rijksoverheid geldt de [Baseline Informatiebeveiliging Overheid](#) als basis voor de inrichting van informatiebeveiliging. Opdrachtgever verwacht van Wederpartij met wie zij samenwerkt, dat Wederpartij bij de inrichting van informatiebeveiliging zoveel mogelijk voldoet aan dezelfde eisen. Wederpartij neemt in ieder geval passende technische en organisatorische maatregelen om de informatie afdoende te beveiligen.
- Wederpartij 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.
- Wederpartij rapporteert minstens jaarlijks of op verzoek van Opdrachtgever over de status van informatiebeveiliging middels een rapportage aan Opdrachtgever. Wederpartij gaat in de rapportage in op de door Wederpartij genomen (beveiligings)maatregelen. Voor de rapportage zal Wederpartij geen kosten in rekening brengen.
- Wederpartij heeft het recht om de door Wederpartij gehanteerde beveiligingseisen door een (onafhankelijke) deskundige te laten inspecteren.
- Indien zich een beveiligingsincident voordoet dat directe impact heeft op de beveiliging van de (Persoons)gegevens wordt door Wederpartij direct contact gezocht met Opdrachtgever. Zie hiervoor ook bijlage 3.
- Wederpartij waarborgt dat de gegevens van de verwerkingsverantwoordelijke niet verwerkt worden in een land buiten de Europese Unie.

In te vullen door Wederpartij:

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 (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 Wederpartij Persoonsgegevens gaat verwerken in het kader van het uitvoeren van de Overeenkomst, heeft Wederpartij 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. Wederpartij dient volledige medewerking te verlenen door alle door opdrachtgever gevraagde informatie te verstrekken.

Opdrachtgever zal onder meer de volgende gegevens aan Wederpartij 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 Wederpartij 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: datalek@rdi.nl

T: 06 – 52 40 20 42 en 06 2528 5561

Bereikbaarheid: **maandag tot en met vrijdag: van 8.00 tot 17.30**

In te vullen door Wederpartij:

Contactgegevens bij datalekken:

E:

T:

Bereikbaarheid: