Bijlage B – concept
Verwerkersovereenkomst
op basis van de ARVODI-2025

tussen

het ministerie van Buitenlandse Zaken
de directie Vertalingen (AVT)

en

<Opdrachtnemer>

inzake

Vertaaldiensten Nederlands–Engels

met kenmerk
201865003.001.144_A

Verwerkersovereenkomst ARVODI-2025

Contractnummer: 201865003.001.144_A

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag,
   hierbij vertegenwoordigd door de minister van Buitenlandse Zaken,
   namens deze,
   Directeur directie Vertalingen (AVT), de heer drs. W.G. Metz,
   hierna te noemen: Opdrachtgever,

en

2. <volledige naam en rechtsvorm contractant>,
   (statutair) gevestigd te <plaatsnaam>,
   hierbij vertegenwoordigd door,
   <functienaam en naam ondertekenaar>,
   hierna te noemen: Opdrachtnemer.

Hierna gezamenlijk te noemen: de 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:

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-2025 of de Verordening, met dien verstande dat een aantal begrippen op de Verwerkersovereenkomst is 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-2025: Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het uitvoeren van Diensten 2025.

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 <titel Overeenkomst> van <datum>, met kenmerk <kenmerk>.

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.

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.

3. Inwerktreding 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.

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.

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.

6. Geheimhouding door Personeel van Opdrachtnemer

6.1. De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 11.1 van de ARVODI-2025.

6.2. Opdrachtnemer waarborgt dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 11.2 van de ARVODI-2025.

7. Subverwerker

7.1. Wanneer Opdrachtnemer, met inachtneming van het bepaalde in artikel 6 van de ARVODI-2025, 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.

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.

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

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

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.

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.

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.

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.

Plaats: ……	Plaats: ……
Datum: ……-……-……	Datum: ……-……-……
De minister van Buitenlandse Zaken,	<naam Opdrachtnemer>,

namens deze, Directeur directie Vertalingen (AVT),	namens deze, <functie gevolmachtigde>,
de heer drs. W.G. Metz	<Naam gevolmachtigde>

Bijlagen:
1. De Verwerking van Persoonsgegevens
2. Passende technische en organisatorische maatregelen
3. Afspraken betreffende Inbreuken in verband met Persoonsgegevens

Bijlage 1. De Verwerking van Persoonsgegevens

Het onderwerp/aard en doel van de Verwerking	Vervaardigen van vertalingen van documenten die persoonsgegevens bevatten.
Het soort Persoonsgegevens	Het gaat hier om alle persoonsgegevens welke in de te vertalen teksten zijn opgenomen.
Beschrijving categorieën Persoonsgegevens	Alle persoonsgegevens als opgenomen in de bronteksten. Deze zullen vermoedelijk incidenteel ook bijzondere persoonsgegevens bevatten.
Beschrijving categorieën Betrokkenen	Personen welke herleidbaar zijn aan de hand van de te vertalen teksten.
Beschrijving categorieën Ontvangers van Persoonsgegevens	Opdrachtgevers die AVT verzocht hebben om vertaling van het document dat persoonsgegevens bevat; AVT/Minbuza met als doel de vertaling te organiseren; de opdrachtnemer/externe vertalers die de vertaling vervaardigen.

CONCEPT Bijlage 2. Passende technische en organisatorische maatregelen

Het Nederlandse ministerie van Buitenlandse Zaken (BZ) is verplicht om zeker te stellen dat alle processen en informatiesystemen voldoen aan de Baseline Informatiebeveiliging Overheid (BIO) en de Baseline BZ 2021. Het is met deze reden dat aanvullende vereisten worden gesteld aan dienstverleners indien deze BZ-informatie verwerken. De dienstverlener verplicht zich om zich te houden aan de volgende vereisten.

A. Veilig en betrouwbaar personeel

☐ Al het personeel met toegang tot informatie betreffende deze overeenkomst dient een Non-Disclosure/Confidentiality agreement te hebben ondertekend.

☐ Al het personeel met toegang tot informatie betreffende deze overeenkomst dient een positieve Verklaring Omtrent Gedrag (VOG) te hebben overhandigd. Een VOG mag niet ouder zijn dan 4 jaar en dient dan opnieuw aangevraagd te worden.

☐ Alle personen met (fysieke) toegang tot systemen waarin deze informatie wordt verwerkt zijn aantoonbaar bekend met de voor hun rol of werkzaamheden relevante informatiebeveiligingsrisico's (bijvoorbeeld phishing) en weten hoe zij hiermee zorgvuldig moeten omgaan; dit blijkt bijvoorbeeld uit het volgen van een passende training of een vergelijkbare vorm van bewustwordingsactiviteiten.

☐ Geleverde vertalingen dienen zonder uitzondering door een mens verwerkt en vervaardigd te zijn. In dit licht is het uitdrukkelijk niet toegestaan gebruik te maken van automatische vertaalsystemen of -diensten of AI-systemen of LLM's als Google Translate, DeepL, Bing Translator, Systran, ChatGPT of systemen of diensten van andere aanbieders, ook niet om gebruikt te worden als basis voor post-editing. Deze verplichtingen gelden onverkort voor alle bij de opdracht betrokken personen van de Dienstverlener, waaronder in ieder geval vertalers, proeflezers/revisors en administratief medewerkers/projectmanagers. Het voorgaande geldt tenzij Opdrachtgever voor een specifieke opdracht vooraf uitdrukkelijk en schriftelijk toestemming heeft verleend voor het gebruik van een door Opdrachtgever geaccepteerde AI-toepassing of machinevertaaltool. Opdrachtgever kan aan deze toestemming nadere voorwaarden verbinden.

B. Onderhoud van producten en systemen

☐ Alle producten en systemen welke worden ingezet bij het uitvoeren van de Overeenkomst, inclusief de informatie- en fysieke beveiligingssystemen, moeten worden onderhouden volgens de geadviseerde onderhoudsspecificaties van de fabrikant. De systemen dienen zich altijd binnen de 'vendor lifecycle' te bevinden.

☐ Onderhoud van de systemen moet worden uitgevoerd, als onderdeel van het verandermanagementproces. De wijzigingen aan de configuratie worden steeds schriftelijk vastgelegd (het liefst conform een beheermethodiek zoals een wijzigingslog), zodat duidelijk is welke wijzigingen wanneer en door wie zijn aangebracht.

☐ Indien (gemotiveerd) niet kan worden voldaan aan de twee hiervoor genoemde onderhoudseisen, dient BZ te worden geïnformeerd, inclusief een onderbouwde inschatting van het risico.

☐ Indien de fabrikant geen specificaties heeft meegegeven, dienen internationale best practices te worden ingezet.

☐ Het is toegestaan gebruik te maken van een CAT-tool (bijv. SDL Trados Studio, MultiTrans, memoQ of CAT-tools van andere aanbieders) mits daarbij koppelingen met automatische vertaalsystemen of -diensten, bijvoorbeeld door middel van een API, en/of vertaalgeheugens die gevuld zijn met machinevertalingen, zijn uitgeschakeld.

C. Systeem- en Web Applicatie Hardening – Niet van toepassing

D. Versleuteling van data – Niet van toepassing

E. Multi Factor Authenticatie
☐ Alle accounts waarmee toegang tot systemen met BZ-data kan worden verkregen via het 'open internet' dienen voorzien te zijn van twee-factor authenticatie.

☐ Alle beheerder- en andere accounts met hoge privileges van systemen met toegang tot BZ-informatie dienen voorzien te zijn van twee-factor authenticatie en deze beheerinterfaces mogen niet direct via internet bereikbaar zijn.

F. Toegangscontrole
☐ Een toegangscontrolematrix dient te zijn opgesteld (bijvoorbeeld in Excel, template beschikbaar), te worden onderhouden en te worden toegepast voor alle toegang tot data en systemen welke worden gebruikt ter invulling van de Overeenkomst. Deze verplichting geldt niet voor individuele freelancevertalers die uitsluitend zelf toegang hebben tot de gebruikte systemen en data.

☐ De Dienstverlener stelt de bronteksten en producten voortvloeiend uit opdrachten van AVT, door AVT eventueel aangeleverde terminologie en documentatie (glossaria, eerdere vertalingen, achtergrondstukken, correspondentie, etc.) in generlei vorm aan derden beschikbaar, behoudens voor zover dit noodzakelijk is voor de uitvoering van de overeenkomst en hiervoor voorafgaande, uitdrukkelijke en schriftelijke toestemming van BZ is verkregen.

G. Fysieke beveiliging
☐ Fysieke toegang tot systemen en/of data dient enkel te worden verstrekt aan geautoriseerd personeel dat de juiste backgroundchecks heeft doorlopen en de juiste 'Confidentiality agreements' heeft ondertekend.

☐ Alle informatie in niet-digitale vorm, zoals op papier, die BZ-informatie bevat, wordt na levering van de gevraagde dienst vernietigd binnen een in overleg met BZ te bepalen termijn. Uitgeprinte brondocumenten en vertalingen en handgeschreven of geprinte kladversies worden met behulp van een papierversnipperaar vernietigd.

H. Communication security
☐ E-mail dient niet gebruikt te worden voor het verzenden van gevoelige/bijzondere of grote hoeveelheden data. Tenzij de data in een op correcte wijze versleutelde container is toegevoegd aan de bijlagen.

☐ Er is een duidelijke werkwijze voor het verwijderen van BZ-informatie uit systemen en opslagmedia zodra deze informatie niet meer nodig is. Daarbij wordt ervoor gezorgd dat de gegevens niet meer kunnen worden teruggehaald, bij voorkeur in lijn met algemeen aanvaarde richtlijnen voor veilig wissen (zoals NIST Special Publication 800-88, Guidelines for Media Sanitization). Dit geldt ook voor systemen voor uitwijk, mirrors, back-upmedia, draagbare opslagmiddelen zoals USB-sticks en geheugenkaarten, vertaalgeheugens en versies die zich in de prullenbak van het besturingssysteem bevinden.

I. Doorgifte van data
☐ Andere partijen dan onderdeel van deze overeenkomst (subverwerkers en onderaannemers) zullen geen data of toegang tot systemen met data van BZ (inclusief bronteksten en producten voortvloeiend uit opdrachten van AVT, door AVT eventueel aangeleverde terminologie en

documentatie zoals glossaria, eerdere vertalingen, achtergrondstukken, correspondentie, etc.) ontvangen via dienstverlener, tenzij hiertoe expliciet en schriftelijk toestemming is verkregen vanuit BZ. De opdrachtnemer moet in de aanbieding duidelijk aangeven welke subverwerkers en/of onderaannemers deel uitmaken van de dienstverlening.

☐ Indien het dienstverlener is toegestaan om aan derden deze data door te geven, dan dient dienstverlener alle vereisten inclusief de eisen in deze informatiebeveiligingsbijlage en de privacyvereisten in de verwerkersovereenkomst vast te leggen in formeel geaccepteerde contractuele afspraken met deze derden. De eerste dienstverlener blijft verantwoordelijk en aansprakelijk voor de juiste naleving van de uitvoering van de contractuele afspraken. En dient te borgen dat gedurende de duur van de Overeenkomst de aanbieder hieraan blijft voldoen.

K. Beveiligingsincidentmanagement
☐ Ieder informatiebeveiligingsincident, datalek of vermoedelijk incident gerelateerd aan confidentialiteit, integriteit of beschikbaarheid zal direct zonder onnodige vertraging en altijd binnen 24 uur gemeld worden aan Information Security Centre (i-SecurityCentre@minbuza.nl), waarna eventuele instructies door BZ naar aanleiding van dit incident direct opgevolgd moeten worden.

L. Business Continuity and Disaster Recovery
☐ Opdrachtnemer neemt alle in redelijkheid* te verwachten maatregelen om de integriteit en beschikbaarheid van de data te garanderen.

☐ Dit betekent in elk geval dat opdrachtnemer zorg draagt dat data beschikbaar is bij uitval of verlies van de hostinglocatie. De opdrachtnemer zorgt zelf voor de afweging in implementatie, bijvoorbeeld een versleutelde back-upset op een andere locatie of uitwijk. Hierbij dient voldaan te worden aan het huidig geldende back-upbeleid.

M. Logging en monitoring
☐ Toegang tot data en systemen die voor deze Overeenkomst worden gebruikt wordt gelogd in een centraal logsysteem, voor een periode van minimaal 6 maanden (bijvoorbeeld in Excel, template beschikbaar). Deze logs bevatten bij voorkeur het van- en naar-IP-adres, gebruikersnamen, datum, tijd en de uitgevoerde acties (zoals lezen, wijzigen en verwijderen). Deze verplichting geldt niet voor individuele freelancevertalers die uitsluitend zelf toegang hebben tot de gebruikte systemen en data.

☐ De opdrachtnemer dient als onderdeel van de dienstverlening zelf de omgeving actief te monitoren en verdachte activiteiten zelf op te pakken.

☐ De opdrachtnemer dient als onderdeel van de dienstverlening ervoor te zorgen dat systemen en data beschermd worden tegen virussen, malware en alle andere vergelijkbare dreigingen.

O. Audits
☐ Het ministerie moet minimaal jaarlijks de mogelijkheid krijgen om een audit te doen of laten uitvoeren op alle vereisten zoals in de Overeenkomst genoemd.

☐ In toevoeging op het bovenstaande moet het ministerie in staat worden gesteld om gedurende of na informatiebeveiligingsincidenten controles uit te oefenen op de naleving van de in de Overeenkomst genoemde vereisten. De opdrachtnemer moet volledige en tijdige medewerking verlenen aan BZ.

☐ Bevindingen vanuit audits waaruit niet-naleving van de in dit contract genoemde informatiebeveiligingseisen blijkt dienen onmiddellijk of binnen een met het ministerie afgestemde

* De marge van redelijkheid wordt in het PvE vastgesteld en is afhankelijk van overige eisen.

termijn te worden verholpen. Anders zal er worden overgegaan tot ontbinding van de Overeenkomst.

P. Non Compliance
Het niet voldoen aan de in dit contract en/of deze bijlage gestelde eisen kan leiden tot beëindiging van dit contract, boetes en/of strafrechtelijke vervolging.

Bijlage 3. Afspraken betreffende Inbreuken in verband met Persoonsgegevens

Een nieuwe/vermoedelijke melding doen

Conform de AVG-wet- en -regelgeving dient het ministerie van Buitenlandse Zaken (BZ) datalekken **binnen 72 uur** te melden bij de Autoriteit Persoonsgegevens (AP). Hierbij kan er ook een voorlopige melding gedaan worden indien nog niet alles bekend is of indien BZ twijfelt of het een datalek is. Het is derhalve van belang dat (sub)verwerkers een (vermoeden van) een datalek **uiterlijk binnen 24 uur** melden bij het BZ Information Security Centre via dit formulier met de contactpersoon van de opdrachtgever in de CC.

NB: ook **vermoedens van datalek** dienen aan BZ gemeld te worden.

Het BZ Information Security Centre is bereikbaar via **i-SecurityCentre@minbuza.nl**.

Na ontvangst van het formulier voert het Information Security Centre een analyse uit om te bepalen of het een datalek is en neemt hiervoor waar nodig contact op met de (sub)verwerker. Dit betekent dat de melding niet automatisch wordt doorgezet naar de AP.

Let op! Graag alle velden invullen, ook al weet je het antwoord niet. Maak de beste keuze en geef ons een toelichting onderaan het formulier. Voor de melding aan de AP zijn veel van deze velden verplicht, vandaar het verzoek alle vragen altijd te beantwoorden.

1. Melding Datalek door (sub)verwerker

LET OP: deze velden zijn verplicht. Zelfs indien er (nog) geen juist antwoord mogelijk is, probeer deze dan zo accuraat mogelijk te beantwoorden.

1.1 Wie meldt het datalek en is de contactpersoon?

Naam

Functie

E-mailadres

Telefoonnummer

Organisatie

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie (subverwerker) betrokken bij de inbreuk?

Kies er een

Naam van de andere organisatie die betrokken was bij de inbreuk

In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?

1.3 Tijdlijn

Exacte datum waarop de inbreuk heeft plaatsgevonden (indien bekend)

Startdatum van de periode waarbinnen de inbreuk was

Einddatum van de periode waarbinnen de inbreuk was

Duurt de inbreuk op dit moment nog voort?

Kies er een

Wanneer werd de inbreuk ontdekt?

Als u de inbreuk later dan 24 uur na ontdekking meldt, wat is daarvan de reden?

1.4 Gegevens over het datalek

1.4.1 *Aard van de inbreuk*

Inbreuk op de vertrouwelijkheid van de gegevens

Kies er een

Inbreuk op de integriteit van de gegevens

Kies er een

Inbreuk op de beschikbaarheid van de gegevens

Kies er een

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

Kies er een

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

1.5 Persoonsgegevens die betrokken zijn bij het datalek

1.5.1 *Persoonsgegevens in het algemeen*

Naam

Kies er een

Geslacht, geboortedatum en/of leeftijd

Kies er een

Burgerservicenummer (BSN)

Kies er een

Contactgegevens

Kies er een

Toegangs- of identificatiegegevens

Kies er een

Financiële gegevens

Kies er een

(Kopieën van) paspoorten of andere legitimatiebewijzen

Kies er een

Locatiegegevens

Kies er een

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

Kies er een

Onbekend / anders, namelijk

1.5.2 *Bijzondere categorieën van persoonsgegevens*

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt

Kies er een

Persoonsgegevens waaruit iemands politieke opvattingen blijken

Kies er een

Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken

Kies er een

Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt

Kies er een

Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid

Kies er een

Gegevens over iemands gezondheid

Kies er een

Genetische gegevens

Kies er een

Biometrische gegevens

Kies er een

1.5.3 *Hoeveelheid persoonsgegevens*

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk

1.6 **De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek**

Werknemers

Kies er een

Klanten (huidig en potentieel)

Kies er een

Leerlingen of studenten

Kies er een

Patiënten

Kies er een

Minderjarigen

Kies er een

Personen uit kwetsbare groepen

Kies er een

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

1.7 Maatregelen die getrokken zijn voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?

Kies er een

Als de persoonsgegevens deels onbegrijpelijk of ontoegankelijk waren, om welk deel gaat dat dan?

Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd?

1.8 Gevolgen van het datalek

1.8.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens

Onbevoegden hebben kennis kunnen nemen van de gegevens

Kies er een

De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt

Kies er een

Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt

Kies er een

Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties

Kies er een

Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen

Kies er een

Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen

Kies er een

Anders, namelijk

1.8.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie

Kies er een

Identiteitsdiefstal of -fraude

Kies er een

Financiële verliezen

Kies er een

Reputatieschade

Kies er een

Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens

Kies er een

Ongeoorloofde ongedaanmaking van pseudonimisering

Kies er een

Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen

Kies er een

Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen

Kies er een

Andere gevolgen, namelijk

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen

Kies er een

1.9 Vervolgacties naar aanleiding van het datalek

1.9.1 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

1.9.2 Informeren van partijen

Heeft u betrokkenen en/of andere partijen geïnformeerd?

1.9.3 Internationale aspecten

In welke landen heeft de inbreuk zich voorgedaan?

1.9.4 Overige informatie welke bruikbaar zou kunnen zijn

Voorzie ons waar mogelijk van informatie die van belang is of zou kunnen zijn voor eventueel vervolgonderzoek en waar niet naar is gevraagd of waar onvoldoende ruimte was om te antwoorden in de voorgaande vragen.

Verstuur dit formulier naar i-SecurityCentre@minbuza.nl met de contactpersoon van de opdrachtgever in de CC na het ontdekken van een datalek. Altijd zo spoedig mogelijk, maar nooit later dan 24 uur na het ontdekken van het datalek!