



Bijlage 2B

(Concept) Verwerkersovereenkomst ARIV-2018 inzake Eindejaarsgeschenken

tussen

de **Staat der Nederlanden**, namens het ministerie van Financiën,
namens het Directoraat-Generaal Belastingdienst

en

<N.T.B.>

Horende bij de openbare Europese aanbesteding:
IUC22-713 Eindejaarsgeschenken

Centrum voor Facilitaire Dienstverlening (CFD)

Inkoopuitvoeringscentrum (IUC)
Belastingdienst

Tiberdreef 12-24
3561 GG Utrecht

Postbus 9799
3561 GT Utrecht

**De ondergetekenden:**

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag, te dezen vertegenwoordigd door de Staatssecretaris van Financiën, namens deze rechtsgeldig vertegenwoordigd door mevrouw drs. M.N. van Dooren, directeur Shared Service Organisatie Centrum voor Facilitaire Dienstverlening (SSO CFD), hierna te noemen: Opdrachtgever,

en

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

beide afzonderlijk respectievelijk gezamenlijk te noemen: 'Partij' dan wel 'Partijen',

OVERWEGENDE DAT:

- Voor zover opdrachtnemer Persoonsgegevens Verwerkt ten behoeve van opdrachtgever in het kader van de Raamovereenkomst, 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 ARIV-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 ARIV-2018: Algemene Rijksinkoopvoorwaarden 2018.
- 1.2 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.
- 1.2 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 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die opdrachtnemer in het kader van de Raamovereenkomst ten behoeve van opdrachtgever Verwerkt.
- 1.7 Raamovereenkomst: de Raamovereenkomst tussen opdrachtgever en opdrachtnemer Eindejaarsgeschenken van [datum], met kenmerk IUC22-713.
- 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 Raamovereenkomst en is onlosmakelijk verbonden met de Raamovereenkomst.
- 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 voor zover en 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 opdrachtgever 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 Indien en voor zover opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal opdrachtnemer aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.
- 5.4 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de EU/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 zal geen persoonsgegevens doorgeven of laten doorgeven door diens aannemers of onderaannemers naar landen buiten de EU/EER zonder de uitdrukkelijke voorafgaande schriftelijke toestemming van opdrachtgever. Zodra er nieuwe regelgeving is op het gebied van persoonsgegevens, zullen partijen in overleg treden en de Raamovereenkomst op dit punt aanvullen zodat deze Raamovereenkomst niet afwijkt van de geldende regelgeving.
- 5.6 Opdrachtnemer zal zonder de uitdrukkelijke voorafgaande schriftelijke goedkeuring van de opdrachtgever slechts persoonsgegevens verwerken voor zover noodzakelijk is voor het uitvoeren van deze Raamovereenkomst. Opdrachtnemer zal geen Persoonsgegevens verplaatsen of doorgeven aan bedrijven of bedrijfsonderdelen, gevestigd in territoria buiten de EU/EER, of in derde landen, zonder de uitdrukkelijke voorafgaande schriftelijke goedkeuring van opdrachtgever. In het specifieke geval dat opdrachtgever goedkeuring geeft aan verplaatsing van Persoonsgegevens buiten de EU/EER, met inachtneming van het in de vorige volzin gestelde, zal opdrachtnemer de daaraan verbonden verplichtingen uit de Algemene Verordening Gegevensbescherming nakomen, waaronder het aangaan van EU Model Clauses met de verwerkende identiteit buiten de EU.



- 5.7 Opdrachtnemer 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.
- 5.8 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 8.1 van de ARIV-2018.
- 6.2 Opdrachtnemer waarborgt dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 8.2 van de ARIV-2018.

Artikel 7. Subverwerker

- 7.1 Bij het uitvoeren van de Raamovereenkomst mag opdrachtnemer alleen met voorafgaande schriftelijke toestemming van opdrachtgever een andere Verwerker inschakelen. Deze toestemming, waaraan door opdrachtgever nadere voorwaarden kunnen worden verbonden, wordt niet zonder redelijke grond geweigerd.
- 7.2 Toestemming van opdrachtgever laat de eigen verantwoordelijkheid en aansprakelijkheid van opdrachtnemer voor de nakoming van de krachtens de Raamovereenkomst op hem rustende verplichtingen en de krachtens de belasting-, zorgverzekerings- en sociale verzekeringswetgeving op hem als werkgever rustende verplichtingen, onverlet.
- 7.3 Wanneer opdrachtnemer met inachtneming van het bepaalde in dit artikel 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.

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 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 Raamovereenkomst, 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 verwijderd, 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 45 Kalenderdagen na afloop van de leverperiode, of zoveel eerder als overeengekomen, bij gebreke waarvan opdrachtnemer een boete verschuldigd is van € 1.000,- per dag, met een maximum van € 2.500,-. Betaling van de boete laat de verplichting uit dit lid 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,



Verwerkersovereenkomst ARIV-2018

Den Haag, <datum>

<Plaats>, <datum>

DE STAATSSECRETARIS VAN FINANCIEN

<Naam opdrachtnemer>

namens deze,

namens deze,

Directeur Shared Service Organisatie
Centrum voor Facilitaire Dienstverlening (SSO CFD)

<Functie ondertekenaar>

Mevrouw drs. M.N. van Dooren

<Aanhef, initialen en naam ondertekenaar>



Bijlage 1. De Verwerking van Persoonsgegevens

Ten behoeve van de uitgifte van fysieke Eindejaarsvouchers via opdrachtnemer zal opdrachtnemer de NAW-gegevens van alle aangeleverde in- en externe medewerkers van de opdrachtgever per e-mail ontvangen, via een versleuteld Excel-bestand. Opdrachtnemer zal alle aangeleverde NAW-gegevens binnen 45 Kalenderdagen verwijderen en vernietigen.

Na het plaatsen van bestellingen van het eindejaarsgeschenk, zal opdrachtnemer de e-mailgegevens ontvangen van deze bestellers (medewerkers van opdrachtgever). Opdrachtnemer gebruikt de e-mailadressen alleen ten behoeve van het versturen van de bestelbevestiging en voor het versturen van digitale cadeaukaarten en/of het versturen van de track & trace code van de fysiek bestelde eindejaarsgeschenken namens opdrachtgever.

Wanneer bestellers een fysiek eindejaarsgeschenk hebben besteld, zal opdrachtnemer de NAW-gegevens van de bestellers ontvangen. De e-mailadressen en NAW-gegevens worden binnen 45 Kalenderdagen na verzending verwijderd en vernietigd.

Door opdrachtnemer te leveren informatie in een verklaring van de vernietiging aan opdrachtgever:

- Specificatie van de gegevens die vernietigd zijn
- Wanneer de vernietiging is uitgevoerd
- Op grond van welke overeenkomst
- Hoe de gegevens vernietigd zijn
- Eventuele bijzonderheden
- Dagtekening en ondertekening

**Bijlage 2. Passende technische en organisatorische maatregelen**

In deze bijlage zijn de normen en maatregelen die opdrachtnemer in het kader van de beveiliging van de Verwerking moet hanteren respectievelijk gespecificeerd.

1. Voor de informatiebeveiliging van de Persoonsgegevens die opdrachtnemer tijdens de uitvoering van de Opdracht verwerkt, geldt dat opdrachtnemer minimaal maatregelen treft op [basisbeveiligingsniveau 1 van de baseline informatie-beveiliging overheid \(BIO\)](#). Het betreft de volgende standaarden (BIO 10.1.1.2, 13.2.2.4, 13.2.3.3, 18.1.5.1).
2. Opdrachtnemer voor alle webverbindingen van de webwinkel HTTPS en HSTS toepast conform de richtlijnen van het NCSC. Er wordt alleen gebruik gemaakt van standaarden en instellingen die door het NCSC als 'Goed' zijn gekwalificeerd ("ICT-beveiligingsrichtlijnen voor Transport Layer Security"). Met de 'Qualys SSL Labs SSL Server Test' wordt minimaal een A- behaald.
3. Opdrachtnemer voor zijn webwinkel gebruik maakt van een SSL-certificaat*.
4. In het kader van de uitvoering van de te sluiten Raamovereenkomst, garandeert opdrachtnemer de toepassing van passende technische en organisatorische maatregelen, opdat de verwerking aan de vereisten van de Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679) voldoet en de bescherming van de Betrokkene is gewaarborgd.
5. Opdrachtgever en opdrachtnemer geven na ondertekening van de Raamovereenkomst in gezamenlijkheid nader invulling aan de Verwerkers-overeenkomst door de specifieke technische en organisatorische beheersings-maatregelen daarin vast te leggen, voorbeelden hiervan zijn:
 - Pseudonimiseren en versleutelen van persoonsgegevens.
 - Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen.
 - Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.
 - Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.
 - Back-ups en herstelmogelijkheden.
 - Monitoring en logging.
 - Managementrapportages over risicobeheer.
 - Periodiek een audit of hack-test uitvoeren.
 - Controle en sturing op de toegang tot de webwinkel, bevoegdheden, integriteit, gegevensdragers, gebruik en toegang tot gegevens transmissie.
6. Opdrachtnemer gaat akkoord wanneer opdrachtgever besluit om een externe audit of compliance te laten uitvoeren door certificeringinstantie welke wordt aangedragen door opdrachtgever.
7. Indien opdrachtgever het gedurende de looptijd van deze Raamovereenkomst wenselijk acht om aanvullende afspraken rondom de vastlegging en beveiliging van persoonsgegevens te maken, zal opdrachtnemer hier zijn medewerking aan verlenen.
8. Inzake de verwerking van persoonsgegevens is het bepaalde in de Algemene Verordening Gegevensbescherming (AVG) en de ARIV-2018 onverkort van toepassing.
9. Partijen zullen voldoen aan hun verplichtingen onder de van toepassing zijnde wet- en regelgeving ter bescherming van persoonsgegevens (zoals de Algemene Verordening Gegevensbescherming) met betrekking tot alle persoonsgegevens die bij de uitvoering van deze Raamovereenkomst worden verwerkt.

* SSL staat voor Secure Sockets Layer. Een SSL certificaat versleutelt informatie die wordt doorgegeven tussen een website en bezoekers. Het vermindert het risico dat gevoelige informatie, zoals wachtwoorden of bankgegevens, wordt onderschept door onbevoegde partijen.



10. Behalve wanneer opdrachtgever uitdrukkelijk anders bepaalt of voor zover opdrachtnemer hiertoe wettelijk verplicht is, zal opdrachtnemer geen data en of persoonsgegevens aan enige andere partij bekendmaken, anders dan aan medewerkers en betrokken onderaannemers voor wie een dergelijke bekendmaking noodzakelijk is om de gecontracteerde dienstverlening uit te voeren, en uitsluitend in de mate waarin het nodig is voor een daartoe bevoegde partij. Indien opdrachtnemer ten gevolge van een wettelijke verplichting data en of persoonsgegevens aan een andere partij bekend moet maken, zal opdrachtnemer dit (indien toegestaan) van tevoren met opdrachtgever bespreken. Opdrachtnemer zal geen persoonsgegevens gebruiken voor eigen doeleinden anders dan noodzakelijk voor de uitvoering van de Raamovereenkomst.
11. Opdrachtnemer zal naar beste vermogen meewerken aan alle redelijke procedures en processen betreffende de omgang met persoonsgegevens die opdrachtgever aan opdrachtnemer heeft bekendgemaakt.
12. Opdrachtnemer draagt zorg voor alle redelijke technische en organisatorische maatregelen om vernietiging van of schade aan data of persoonsgegevens te voorkomen, inclusief maar niet beperkt tot de betrouwbaarheid van werknemers die toegang hebben tot deze data of persoonsgegevens.
13. De verplichtingen in dit artikel gelden niet alleen voor opdrachtnemer, maar ook voor de eventuele onderaannemer(s)/subverwerker(s). Opdrachtnemer verplicht zich er hierbij toe deze verplichtingen met de onderaannemer(s)/subverwerker(s) vooraf schriftelijk overeen te komen en de naleving ervan te controleren.
Bij het uitvoeren van de Raamovereenkomst mag opdrachtnemer alleen met voorafgaande schriftelijke toestemming van opdrachtgever de onderaannemer(s)/subverwerker(s) inschakelen. Deze toestemming, waaraan door opdrachtgever nadere voorwaarden kunnen worden verbonden, wordt niet zonder redelijke grond geweigerd.

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

In deze bijlage moeten de afspraken over hoe opdrachtnemer opdrachtgever over Inbreuken in verband met Persoonsgegevens gaat informeren worden gespecificeerd.

Departementale procedure

Indien een inbreuk in verband met persoonsgegevens in de zin van artikel 4, lid 12 van de Algemene Verordening Gegevensverwerking heeft plaatsgevonden is opdrachtgever verplicht deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, te melden aan de Autoriteit Persoonsgegevens.

Onder inbreuk in verband met persoonsgegevens wordt in dit schrijven verstaan: 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.

Derhalve gelden de volgende bepalingen als aanvulling op deze overeenkomst:

1. Zodra opdrachtnemer een inbreuk ontdekt of anderszins op de hoogte raakt van een inbreuk, zal opdrachtnemer:
 - a) onmiddellijk alle maatregelen nemen om de tekortkomingen in de beveiliging die hebben geleid tot de inbreuk te corrigeren en de gevolgen daarvan te beperken.
 - b) Opdrachtgever zo snel als redelijkerwijs mogelijk is, maar niet later dan 24 uren na de ontdekking van de inbreuk, informeren over de aard van de inbreuk, de mogelijke impact van de inbreuk op opdrachtgever en/of betrokkene(n), alsmede de maatregelen die opdrachtnemer heeft genomen of zal nemen om de beveiliging te corrigeren en/of de gevolgen te beperken. Voorgaande laat onverlet de verplichtingen die opdrachtnemer heeft op grond van artikel 33 en 34 van de AVG en andere wet- en regelgeving in het kader van de meldplicht datalekken. Opdrachtnemer informeert opdrachtgever door contact op te nemen met Melddesk datalekken Belastingdienst via 088-1588 888.
 - c) Samenwerken met opdrachtgever om de oorzaak van de inbreuk te onderzoeken en alle maatregelen nemen die opdrachtgever nodig acht om een vergelijkbaar incident te voorkomen.
2. Zodra opdrachtnemer een inbreuk ontdekt of anderszins op de hoogte raakt van een inbreuk, verstrekt deze ten minste de volgende informatie aan opdrachtgever:
 - a) De aard van de Inbreuk in verband met Persoonsgegevens; dit omvat mede een overzicht van de feiten omtrent de inbreuk.
 - b) De Persoonsgegevens.
 - c) De categorieën van door de inbreuk getroffen Betrokkenen.
 - d) De waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens.
 - e) De maatregelen die opdrachtnemer heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele gevolgen daarvan.

Opdrachtnemer borgt dat eventuele door hem ingeschakelde onderaannemers bij hen voorkomende inbreuken op de beveiliging op zodanige wijze aan hem melden, dat hij in staat is zijn in deze bijlage neergelegde verplichtingen jegens opdrachtgever na te komen. De melding van een inbreuk in verband met persoonsgegevens van opdrachtnemer aan opdrachtgever dient te worden gestuurd naar melddesk.datalekken.belastingdienst@belastingdienst.nl.



De melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens geschiedt door opdrachtgever.

Indien opdrachtgever een inbreuk in verband met persoonsgegevens met gevolgen voor opdrachtnemer signaleert, zal hij opdrachtnemer hierover zo snel als redelijkerwijs mogelijk is, maar niet later dan 24 uren na signalering inlichten. In deze bijlage moeten de afspraken over hoe opdrachtnemer opdrachtgever over Inbreuken in verband met Persoonsgegevens gaat informeren worden gespecificeerd.

Informatie die ten minste door opdrachtnemer moet worden verstrekt

- Datum en tijdstip van de constatering van de (vermoedelijke) Inbreuk in verband met Persoonsgegevens.
- Aard van de Inbreuk in verband met Persoonsgegevens.
- De Persoonsgegevens en Betrokkene.
- Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens.
- Maatregelen die opdrachtnemer heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.