

Verwerkersovereenkomst Veilingdienst ARBIT-2018

Inhoud

Artikel 1. Begrippen.....	2
Artikel 2. Voorwerp van deze Verwerkersovereenkomst	3
Artikel 3. Inwerkingtreding en duur	3
Artikel 4. Omvang verwerkingsbevoegdheid Wederpartij	3
Artikel 5. Beveiliging van de Verwerking	4
Artikel 6. Geheimhouding door Personeel van Wederpartij.....	4
Artikel 7. Subverwerker	4
Artikel 8. Bijstand vanwege rechten van Betrokkene.....	4
Artikel 9. Inbreuk in verband met Persoonsgegevens.....	4
Artikel 10. Terugbezorgen of wissen Persoonsgegevens	5
Artikel 11. Informatieverplichting en audit.....	5
Bijlage 1. De Verwerking van Persoonsgegevens	6
Bijlage 2. Passende technische en organisatorische maatregelen.....	8
Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens.....	9

Verwerkersovereenkomst Veilingdienst ARBIT-2018

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 mevrouw A.T.A.J. van Dijk, Directeur-hoofdinspecteur Agentschap Telecom

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, Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening kwalificeert 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 wenselijk 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 artikel 1 van de Algemene Rijksvoorwaarden bij IT-overeenkomsten 2018 (ARBIT-2018). In afwijking daarvan of in aanvulling daarop wordt onder de volgende begrippen in deze Verwerkersovereenkomst verstaan:

- 1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.
- 1.2 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.
- 1.3 Overeenkomst: de overeenkomst tussen Opdrachtgever en Wederpartij Overeenkomst ARBIT-2018 inzake Veilingdienst frequentieverveilingen van [datum], met kenmerk [kenmerk].
- 1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Wederpartij in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

- 1.5 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).
- 1.6 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.
- 1.7 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.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

- 2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Wederpartij in het kader van 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 van Persoonsgegevens.

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 en voor zover Wederpartij alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.
- 3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang verwerkingsbevoegdheid Wederpartij

- 4.1 Wederpartij Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Wederpartij van toepassing zijn.
- 4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Wederpartij in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever daarvan voorafgaand aan de Verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.
- 4.3 Indien Wederpartij op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken, informeert hij Opdrachtgever onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.
- 4.4 Wederpartij heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

Artikel 5. Beveiliging van de Verwerking

- 5.1 In aanvulling op artikel 19 van de ARBIT-2018 en onverminderd artikel 2.3 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 Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming 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-2018.
- 6.2 Wederpartij toont op verzoek van Opdrachtgever aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 17.2 van de ARBIT-2018.

Artikel 7. Subverwerker

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

Wederpartij verleent 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.

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 draagt Wederpartij, naar gelang de keuze van Opdrachtgever, zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle Persoonsgegevens. Wederpartij verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.
- 10.2 **<OPTIONEEL>** Wederpartij [wist of retourneert] de Persoonsgegevens binnen [aantal] [dagen/weken] na afloop van de Overeenkomst, bij gebreke waarvan Wederpartij een boete verschuldigd is van €[bedrag] per dag, met een maximum van €[bedrag].
- 10.3 **<OPTIONEEL>** Persoonsgegevens worden in de door Opdrachtgever aangegeven vorm en op de door Opdrachtgever aangegeven wijze terugbezorgd.

OF

- 10.3 **<OPTIONEEL>** De Persoonsgegevens worden als volgt terugbezorgd: [bestandsformaat] [wijze] [adres].

Artikel 11. Informatieverplichting en audit

- 11.1 Wederpartij stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.
- 11.2 Wederpartij verleent alle benodigde medewerking aan audits.
- 11.3 **<OPTIONEEL>** Opdrachtgever laat eenmaal per [...] een audit uitvoeren door een onafhankelijke partij.

OF

- 11.3 **<OPTIONEEL>** Wederpartij verstrekt met een frequentie van eenmaal per [...], uiterlijk op [datum] aan Opdrachtgever een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de genoemde naleving.

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

Den Haag, [datum]

[Plaats], [datum]

DE MINISTER/STAATSSECRETARIS VAN/VOOR
[naam portefeuille]

[naam Wederpartij]

namens deze,
[functienaam ondertekenaar]

[naam ondertekenaar]

[functie en naam ondertekenaar]

Bijlage 1. De Verwerking van Persoonsgegevens

In deze bijlage moeten in ieder geval onderstaande worden gespecificeerd. Er wordt geadviseerd om contact op te nemen met de interne privacy adviseur bij het invullen van deze bijlage.

Verwerkersverantwoordelijke, inclusief contactgegevens	E: T Sec:
Contactgegevens vertegenwoordiger verwerkersverantwoordelijke	E: T Sec:
Contactgegevens Functionaris Gegevensbescherming	E: T Sec:
Het onderwerp/aard en doel van de verwerking	
Rechtmatige grondslag ¹	Taak algemeen belang/openbaar gezag.
<i>Indien van toepassing: onderbouwing gerechtvaardigd belang</i>	
(Categorieën van) betrokkene(n)	Medewerkers, bezoekers en leveranciers van Agentschap Telecom
(Categorieën van) persoonsgegevens over de betrokkene(n)	Medewerker; Bezoeker; Voornaam, voorletters, achternaam, naam organisatie. Leverancier:
(Categorieën van) ontvangers;	
(Wettelijke) Bewaartermijn van de gegevens	
Bron van de persoonsgegevens	
Rechten van betrokkenen	Betrokkene heeft het recht op: <ul style="list-style-type: none"> • Inzage en rectificatie of wissing van persoonsgegevens of beperking van de betreffende verwerking • Recht bezwaar te maken tegen de verwerking • Recht op gegevensoverdraagbaarheid. • Klacht in te dienen bij een toezichthoudende autoriteit;
Worden de gegevens doorgegeven aan één of meer landen buiten de EU?	Nee
Gebruik gegevens ander doel door verwerkersverantwoordelijke?	
<i>Indien op één van de volgende vragen 'Ja' moet worden beantwoord, is het noodzakelijk om een Privacy Impact Assessment (PIA) uit te voeren. Neem hiervoor contact op met de interne privacy adviseur.</i>	
Is er sprake van geautomatiseerde besluitvorming?	Nee
Is er sprake van verwerking van bijzondere ² categorieën van	

¹ De AVG kent een aantal rechtmatige grondslagen waarop persoonsgegevens mogen worden verwerkt. Zie voor de relevante grondslagen Art. 6 lid 1 van de [AVG](#) (pagina 36). Let op: Voor verwerkingen in het kader van overheidstaken is het verkrijgen van toestemming veelal geen legitieme grondslag. Er bestaat immers een afhankelijkheidsrelatie tussen de verantwoordelijk een de betrokkene(n).

² Denk hierbij aan verwerkingen waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie

persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten?	
Is er sprake van stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten?	
Houdt de soort verwerking, in het bijzonder als het gaat om een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan om andere redenen waarschijnlijk een hoog risico in voor de rechten en vrijheden van personen?	

van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Bijlage 2. Passende technische en organisatorische maatregelen

In deze bijlage moeten de normen en maatregelen die Wederpartij in het kader van de beveiliging van de Verwerking moet hanteren respectievelijk treffen worden gespecificeerd. Hiervoor kan worden verwezen naar documenten waarin normen en maatregelen zijn vastgelegd, zoals in voorkomend geval het programma van eisen of de offerteaanvraag.

Certificaten waarover verwerker beschikt:

Certificaten	Organisatieonderdeel/ dienst waarop certificaat betrekking heeft	Geldigheidsduur certificaat	Verklaring van toepasselijkheid

Kwalificaties waaraan verwerker voldoet:

Verwerker heeft de volgende beveiligingsmaatregelen genomen conform de Baseline Informatiebeveiliging Overheid (BIO) of ISO 27001.

Logische toegangscontrole, gebruik makend van sterke wachtwoorden;
Fysieke maatregelen voor toegangsbeveiliging;
Encryptie (versleuteling) van digitale bestanden met persoonsgegevens;
Organisatorische maatregelen voor toegangsbeveiliging;
Beveiliging van netwerkverbindingen via Transport Layer Security (TLS) technologie;
Geheimhoudingsplicht medewerkers en ingeschakelde derden.

Overige afspraken:

- De verwerker rapporteert minstens jaarlijks over de status van informatiebeveiliging middels een rapportage aan de verantwoordelijke.
- De verwerkingsverantwoordelijke het recht om de gehanteerde beveiligingseisen door een (onafhankelijke) deskundige te laten inspecteren.
- Indien er zich een beveiligingsincident voordoet wat directe impact heeft op de beveiliging van de (persoons)gegevens wordt er door de verwerker direct contact gezocht met de verantwoordelijke. Zie hiervoor ook bijlage 3.

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

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

Informatie die ten minste door Wederpartij moet worden verstrekt

1. Melding inbreuk op de beveiliging

Wederpartij stelt Opdrachtgever onverwijld (niet later dan 24 uur na ontdekking) in kennis van inbreuken op de beveiliging voor zover die nadelige gevolgen (kunnen) hebben voor de bescherming van persoonsgegevens die Wederpartij voor Opdrachtgever verwerkt. De informatieverstrekking dient op een zodanige wijze plaats te vinden dat Opdrachtgever aan de meldplicht van art. 33 AVG kan voldoen.

2. Inhoud van de melding

Wederpartij verstrekt bij de melding aan Opdrachtgever alle feiten en gegevens omtrent de aard en omvang van de inbreuk op de beveiliging. Wederpartij houdt Opdrachtgever ook na de eerste melding op de hoogte van ontwikkelingen met betrekking tot de betreffende inbreuk op de beveiliging en betreft Opdrachtgever actief bij de maatregelen die Wederpartij treft om de gevolgen van de inbreuk op de beveiliging te beperken en herhaling te voorkomen.

3. Meldpunt Dataretentieteam AT

In het geval zich een situatie voordoet zoals beschreven in artikel 9 van deze Verwerkersovereenkomst, neemt Wederpartij conform dat artikel contact op met Opdrachtgever. Wederpartij verstrekt Opdrachtgever een overzicht met daarin de feiten omtrent aard en (mogelijke) omvang van de inbreuk.

Wederpartij meldt telefonisch de inbreuk via telefoonnummer 050 5877130 én via e-mailadres datalek@agentschaptelecom.nl. Dit e-mailadres gebruikt u eveneens voor het nazenden van de aanvullende informatie over de gemelde inbreuk.

4. De Wederpartij meldt aan opdrachtgever

Algemene informatie en contactgegevens:

- 4.1 Naam bedrijf/organisatiebezoek:
- 4.2 (Bezoek)adres:
- 4.3 Postcode:
- 4.4 Plaats:
- 4.5 Kvk nummer:

Door wie wordt de inbreuk gemeld?

- 4.6 Naam contactpersoon:
- 4.7 Functie van de contactpersoon:
- 4.8 E-mailadres van de contactpersoon:
- 4.9 Telefoonnummer van de contactpersoon:
- 4.10 Alternatief telefoonnummer van de contactpersoon:

Met wie kan contact worden opgenomen voor nadere informatie over de melding?

- 4.11 Naam contactpersoon:
- 4.12 Functie van de contactpersoon:
- 4.13 E-mailadres van de contactpersoon:
- 4.14 Telefoonnummer van de contactpersoon:
- 4.15 Alternatief telefoonnummer van de contactpersoon:

Gegevens over de inbreuk

- 4.16 Geef een korte samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.
- 4.17 Hoeveel personen zijn er bij betrokken (minimaal en maximaal).
- 4.18 Omschrijf de groep mensen (betrokkene(n)) van wie persoonsgegevens zijn betrokken bij de inbreuk.
- 4.19 Wanneer vond de inbreuk plaats (datum, tussen

begindatum/einddatum, nog niet bekend).

Wat is de aard van de inbreuk (U kunt meerdere mogelijkheden aankruisen)

- 4.20 Lezen (vertrouwelijkheid),
- 4.21 Kopiëren,
- 4.22 Veranderen (integriteit),
- 4.23 Verwijderen of vernietigen (beschikbaarheid),
- 4.24 Diefstal,
- 4.24 Nog niet bekend.

Om welk type persoonsgegevens gaat het?

- 4.25 Naam, adres, woonplaats,
- 4.26 Telefoonnummers,
- 4.27 E-mailadressen, IP-adressen of andere adressen voor elektronische communicatie,
- 4.28 Toegangs- of identificatiegegevens (inlognaam/wachtwoord/klantnummer),
- 4.29 Financiële gegevens (rekening- of creditkaartnummer),
- 4.30 Burgerservicenummer,
- 4.31 Kopieën van paspoort of andere legitimatiebewijzen,
- 4.32 Geslacht, geboortedatum, leeftijd,
- 4.33 Bijzondere persoonsgegevens (etniciteit, politieke opvattingen, levensbeschouwing, lidmaatschap vakbond, genetische gegevens, biometrische identificatie, gezondheid, seksuele leven of strafrechtelijke gegevens).

Mogelijke gevolgen van de inbreuk op de persoonlijke levenssfeer van de betrokken:

- 4.34 Stigmatisatie of uitsluiting,
- 4.35 Schade aan gezondheid,
- 4.36 Blootstelling aan (identiteits)fraude,
- 4.37 Blootstelling aan spam of phishing,
- 4.38 Anders nl...

Vervolgacties naar aanleiding van de inbreuk

- 4.38 Welke technische en organisatorische maatregelen zijn ondernomen om de inbreuk te verhelpen/te voorkomen? (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?)
- 4.39 Zijn deze maatregelen tijdelijk of is de inbreuk hiermee volledig gedicht?

Technische maatregelen

- 4.40 Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Ja, nee, deels nl. ...)

Internationale aspecten

- 4.41 Heeft de inbreuk betrekking op personen in andere EU-landen of daarbuiten? (Ja, nee, nog niet bekend)

Vervolgmelding

- 4.42 Is naar uw mening deze melding compleet?
- 4.43 Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig,
- 4.44 Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk.

5. Beleidsregels meldplicht datalekken

Opdrachtgever bepaalt - met inachtneming van het bepaalde in de beleidsregels "De meldplicht datalekken in de AVG" van de Autoriteit Persoonsgegevens - of de inbreuk als een datalek aan de Autoriteit Persoonsgegevens wordt gemeld.

6. Medewerking

Partijen verlenen elkaar volledige medewerking bij de melding van een datalek aan de Autoriteit Persoonsgegevens en, indien nodig, aan degene wiens persoonsgegevens het betreft.

7. Aansprakelijkheid

Artikel 26 ARBIT-2018 is van overeenkomstige toepassing op schade als gevolg van een inbreuk op de beveiliging, waaronder mede begrepen een door de Autoriteit Persoonsgegevens aan Opdrachtgever in verband daarmee opgelegde boete.

Bijlage 4: Subverwerker

Subverwerker(s)

Wederpartij maakt bij de uitvoering van de Overeenkomst gebruik van de onderaannemer(s)/derd(n)/subverwerker(s), die in deze bijlage zijn vermeld. Wederpartij zal deze bijlage conform artikel 8 van deze Verwerkersovereenkomst bijwerken, indien er wijzigingen plaatsvinden in de ingeschakelde onderaannemer(s)/derde(n)/subverwerker(s), en deze lijst onverwijld ter beschikking stellen aan de Opdrachtgever.

Partij 1	
Vestigingsplaats:	
Inschrijvingsnummer handelsregister:	
Beschrijving van de werkzaamheden:	
Voorwaarden van Opdrachtgever gesteld aan toestemming:	Zie artikel 7 Subverwerker

Partij 2	
Vestigingsplaats:	
Inschrijvingsnummer handelsregister:	
Beschrijving van de werkzaamheden:	
Voorwaarden van Opdrachtgever gesteld aan toestemming:	Zie artikel 7 Subverwerker