Nederlandse Voedsel- en Warenautoriteit
Ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur

Bijlage 3. Concept Verwerkersovereenkomst inzake 'Bloemen en (groen)attenties'
ARIV-2018

TenderNed-kenmerk: TN 555657
IUC-kenmerk: 202506087

De ondergetekenden:

1.De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag, te dezen vertegenwoordigd door de minister van Landbouw, Visserij, Voedselzekerheid en Natuur, namens deze,
Dhr. L. Rutges – Reukers, Plv. directeur Interne Organisatie van de Nederlandse Voedsel- en Warenautoriteit,
hierna te noemen: Koper

en

2. [volledige naam en rechtsvorm contractant],
[statutair] gevestigd te …,
te dezen vertegenwoordigd door
[naam ondertekenaar]
hierna te noemen: Leverancier,

Hierna gezamenlijk te noemen: Partijen,

OVERWEGENDE DAT:

- voor zover Leverancier Persoonsgegevens Verwerkt ten behoeve van Koper in het kader van de Overeenkomst, kwalificeert Koper als Verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Leverancier als Verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Leverancier 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.

1.3 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 Raamovereenkomst tussen Koper en Leverancier inzake 'Bloemen en (groen)attenties' van [datum], met TenderNed-kenmerk TN 555657 en IUC-kenmerk 202506087.

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

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

1.9 Verordening: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

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

1.11 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.12 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

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

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking door Leverancier 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 Leverancier 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 Leverancier garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat Leverancier 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 Leverancier

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

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

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

5.5 Leverancier informeert Koper 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 Leverancier verleent Koper 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 Leverancier

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 8.1 van de ARIV-2018.

6.2 Leverancier 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 Overeenkomst mag Leverancier alleen met voorafgaande schriftelijke toestemming van Koper een andere Verwerker inschakelen. Deze toestemming, waaraan door Koper nadere voorwaarden kunnen worden verbonden, wordt niet zonder redelijke grond geweigerd.

7.2 Toestemming van Koper laat de eigen verantwoordelijkheid en aansprakelijkheid van Leverancier voor de nakoming van de krachtens de Overeenkomst op hem rustende verplichtingen en de krachtens de belasting-, zorgverzekerings- en sociale verzekeringswetgeving op hem als werkgever rustende verplichtingen, onverlet.

7.3 Wanneer Leverancier met inachtneming van het bepaalde in dit artikel een andere Verwerker inschakelt om ten behoeve van Koper 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 Leverancier Koper bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden.

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

8.3 Leverancier stuurt een verzoek vanuit een Betrokkene zo spoedig mogelijk aan Koper.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Leverancier informeert Koper 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 Leverancier informeert Koper ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf te maken kosten gerelateerd aan de Inbreuk in verband met Persoonsgegevens.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Overeenkomst, of zoveel eerder als overeengekomen, draagt Leverancier er zorg voor dat hij, naar gelang de keuze van Koper, alle Persoonsgegevens wist of terugbezorgt aan Koper en bestaande kopieën verwijdert, tenzij opslag van de Persoonsgegevens op basis van een wettelijk voorschrift verplicht is.
In geval van wissen en/of verwijderen van kopieën door Leverancier informeert hij Koper zodra hij dit heeft gedaan.

10.2 Partijen kunnen voor afzonderlijke of categorieën Persoonsgegevens bewaartermijnen overeenkomen. Na afloop van de overeengekomen bewaartermijn draagt Leverancier 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 Leverancier wist de Persoonsgegevens binnen één week na afloop van de Overeenkomst, of zoveel eerder als overeengekomen.

Artikel 11. Informatieverplichting en audit

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

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

11.3 Leverancier stelt Koper onmiddellijk in kennis indien naar zijn mening een instructie van Koper 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 Koper is te allen tijde bevoegd om naar aanleiding van de op grond van dit artikel verkregen informatie nadere maatregelen voor te stellen. Leverancier is gehouden aan die maatregelen in redelijkheid uitvoering te geven.

Artikel 12. Geschil

12.1 Een partij die meent dat een geschil bestaat, deelt dat schriftelijk mede aan de andere Partij en treedt daarmee in overleg.

12.2 Partijen overleggen binnen twee weken na ontvangst van de in het eerste lid bedoelde mededeling over hun op schrift gestelde zienswijze en oplossingsrichting. De dienstverlening aan Opdrachtgever mag hierdoor niet worden opgeschort.

12.3 Partijen zullen trachten geschillen die mochten ontstaan naar aanleiding van deze overeenkomst eerst minnelijk op te lossen, eventueel door inschakeling van een mediator of door het instellen van een adviescommissie. Indien het geschil niet minnelijk kan worden opgelost, wordt het geschil voorgelegd aan de bevoegde rechter.

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

Den Haag,
datum:

De minister van Landbouw, Visserij,
Voedselzekerheid en Natuur
namens deze en in opdracht van,
Dhr. L. Rutges – Reukers, Plv. directeur Interne
Organisatie van de Nederlandse Voedsel- en Warenautoriteit,

W.A. van Zeil
Teammanager Inkoop Uitvoering Centrum EZ

[Plaats],
datum: …

[naam Opdrachtnemer]

[functie en naam ondertekenaar]

Bijlage 1. De Verwerking van Persoonsgegevens

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

In te vullen door Leverancier (de verwerker)

Naam verwerker inclusief contactgegevens	
Contactgegevens vertegenwoordiger verwerker	
Contactgegevens FG van de verwerker	
Naam en contactgegevens subverwerker	
Worden de gegevens doorgegeven aan een of meer landen buiten de EU?	

In te vullen door Koper (de verwerkingsverantwoordelijke)

Verwerkingsverantwoordelijke	Inspecteur generaal
Contactgegevens vertegenwoordiger verwerkingsverantwoordelijke	privacy@nvwa.nl
Contactgegevens FG van de verwerkingsverantwoordelijke	Functionaris voor Gegevensbescherming Ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur Bureau Bestuursraad Mevr. Carola Overdevest PbFG@minez.nl Postbus 20401 2500 EK Den Haag
Het onderwerp, aard en doel van de Verwerking	De levering van bloemen en (groen)attenties
Het soort Persoonsgegevens	Voornaam (+ voorletters en eventuele titels), achternaam, woonadres, zakelijk adres (locaties NVWA en andere locaties), emailadres, telefoonnummer
Beschrijving categorieën Persoonsgegevens	Overige persoonsgegevens
Beschrijving categorieën Betrokkenen	NVWA medewerkers en NVWA relaties
Beschrijving categorieën Ontvangers van Persoonsgegevens	Opdrachtnemer (medewerkers van de leverancier(s)), medewerkers van de NVWA financiële administratie, medewerkers die bloemen en (groen)attenties bestellen
Locatie Verwerking Persoonsgegevens	

Bijlage 2. Passende technische en organisatorische maatregelen

In deze bijlage moeten de normen en maatregelen die Leverancier 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.

- Binnen de Rijksoverheid geldt de Baseline Informatiebeveiliging Overheid (BIO) als basis voor de inrichting van informatiebeveiliging.
  De beveiliging van Opdrachtnemer dient minstens aan dezelfde eisen te voldoen als de BIOIR2017 dat voorschrijft op de onderdelen: <<in te vullen door opdrachtgever>>.
- Opdrachtnemer richt aanvullende maatregelen in op basis van het risico van de Verwerking, die bijvoorbeeld naar aanleiding van een Privacy Impact Assessment (PIA) zijn vastgesteld. Een overzicht van deze maatregelen is hieronder opgenomen.

In te vullen door Leverancier:

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

Overige kwalificaties:

In te vullen door Koper:

Aanvullende beveiligingseisen:

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

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

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 Leverancier Persoonsgegevens gaat verwerken in het kader van het uitvoeren van de Overeenkomst, heeft Leverancier 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 Koper.

Verlenen van medewerking
Direct nadat u een inbreuk op de beveiliging van door de door de NVWA aan u verstrekte (persoons)gegevens ontdekt of een datalek vermoed, meldt u dit onverwijld schriftelijk (doch uiterlijk binnen 24 uur) aan de CPO (Chief Privacy Officer) van de NVWA via: beveiligingsincidentmelding@nvwa.nl.
Ook vragen wij u uw contactpersoon bij de NVWA op de hoogte te brengen van het (vermoedelijke) datalek. Voor verdere vragen en opmerkingen kunt u contact opnemen met de CPO van de NVWA via: beveiligingsincidentmelding@nvwa.nl.

Aan de hand van deze door u verstrekte informatie wordt door de CPO besloten of er een melding van het datalek moet worden gedaan bij de Autoriteit Persoonsgegevens (AP).

De verantwoordelijkheid voor het melden bij de AP en het informeren van de betrokkenen ligt bij de NVWA. De NVWA beslist verder over de wijze waarop de betrokkene in voorkomende gevallen geïnformeerd moet gaan worden. Het kan zijn dat u betrokken wordt bij het feitelijk informeren van de betrokkene, bijvoorbeeld omdat u beschikt over de daarvoor noodzakelijke persoonsgegevens. Het doel van de meldplicht datalekken is immers gericht op de beperking van schade voor een betrokkene.

Koper zal onder meer de volgende gegevens aan Leverancier 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 Leverancier contact opgenomen met de contactpersoon/het contactpunt datalekken van Koper.

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 email 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 Koper:
Contactgegevens bij datalekken:
E: beveiligingsincidentmelding@nvwa.nl
T: 088 223 3333
Bereikbaarheid: beveiligingsincidentmelding@nvwa.nl

In te vullen door Leverancier:
Contactgegevens bij datalekken:
E: of secundair
T: of secundair
Bereikbaarheid:

Informatie die ten minste door Leverancier 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 soort, categorieën en het aantal Persoonsgegevens en Betrokkene
Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
Maatregelen die Leverancier 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