KANTAR

Algemene Inkoopvoorwaarden van Kantar Netherlands B.V.

1. DEFINITIES

1.1. In deze Overeenkomst hebben de hierna genoemde begrippen de volgende betekenis

1.1.1. **"AVG"** betekent de 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 intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming).

1.1.2. **"Beleid van de Leverancier"** betekent al het beleid of alle gedragscodes die op de leveranciers van The Kantar Group Limited en diens directe of indirecte dochterondernemingen van toepassing zijn, zoals van tijd tot tijd door de Opdrachtgever aan de Leverancier gemeld of beschikbaar op een door de Opdrachtgever voor diens leveranciers van tijd tot tijd toegankelijk gemaakt extranet van de Opdrachtgever (dat op verzoek beschikbaar zal worden gesteld), inclusief, maar niet beperkt tot de Kantar Gedragscode hierbij gevoegd als Bijlage 1 en al het toepasselijk beleid van Kantar met betrekking tot anti-omkoping.

1.1.3. **"Diensten"** betekent de diensten zoals gespecificeerd in de Inkooporder of de verwijzing naar het Inkoopordernummer waarin de diensten in enige vorm van schriftelijke communicatie worden gespecificeerd.

1.1.4. **"Gelieerde onderneming"** betekent elke entiteit die, direct of indirect via een of meer tussenpersonen, de controle heeft over, of onder gemeenschappelijke controle staat, en in het geval van de Klant van tijd tot tijd handelt als Kantar, maar met uitzondering van Europanel.

1.1.5. **"Gegevens van Opdrachtgever"** betekent alle gegevens (inclusief persoonsgegevens m.b.t. personeel, opdrachtgevers/klanten of leveranciers van de Opdrachtgever of diens klanten), documenten, tekst, tekeningen, diagrammen, specificaties, afbeeldingen (samen met een database waarvan deze samengesteld zijn) geleverd of beschikbaar gesteld aan de Leverancier door of namens de Opdrachtgever of diens klanten, of waarvoor de Leverancier ingevolge deze Overeenkomst verplicht is om deze te genereren, verwerken, op te slaan of te verzenden.

1.1.6. **"Gegevensbeschermingswetgeving"** betekent de Europese Richtlijn inzake Gegevensbescherming (95/46/EC) en de Europese Richtlijn betreffende Privacy en Elektronische Communicatie (zoals van tijd tot tijd gewijzigd) en wetgeving om die Richtlijnen in ieder land uit te voeren en vanaf 25 mei 2018, de EU Richtlijn inzake Gegevensbescherming en de AVG.

1.1.7. **"Inkooporder"** betekent de inkooporder die aan deze Algemene Inkoopvoorwaarden is gehecht of iedere andere schriftelijke communicatie waarin naar het Inkoopordernummer wordt verwezen en waarop deze Algemene Inkoopvoorwaarden van toepassing zijn.

1.1.8. **"Intellectuele Eigendomsrechten"** betekent alle octrooien, rechten op uitvindingen, auteursrechten en naburige rechten, morele rechten, databankrechten, topografierechten voor halfgeleiders, gebruiksmodellen, rechten op ontwerpen, handelsmerken, dienstmerken, handels- of merknamen, domeinnamen, recht op goodwill, rechten op geheime of vertrouwelijke informatie en andere vergelijkbare of gelijkwaardige rechten of vormen van bescherming die nu of in de toekomst overal in de wereld bestaan.

1.1.9. **"Leverancier"** betekent de entiteit zoals geïdentificeerd in de Inkooporder.

1.1.10. **"Opdrachtgever"** betekent de Kantar gelieerde genoemd op de Inkooporder.

1.1.11. **"Overeenkomst"** betekent de Inkooporder samen met deze Algemene Inkoopvoorwaarden.

1.1.12. **"Personeel van Leverancier"** betekent al het personeel dat vereist is om de Diensten uit te voeren.

1.1.13. **"Persoonsgegevens"** heeft de betekenis zoals gegeven in Bijlage 3.

1.1.14. **"Te Leveren Prestatie"** betekent alle goederen, items, apparatuur en materiaal die als onderdeel van de Diensten worden geleverd.

1.1.15. **"Vergoedingen"** betekent het totaalbedrag vermeldt op de Inkooporder dat door de Opdrachtgever betaald zal worden.

1.1.16. **"Vertrouwelijke Informatie"** betekent alle informatie met betrekking tot directeuren, functionarissen en medewerkers van de Kantar Groep, begrotingen, prijzen, orderportefeuilles, methodieken, vragenlijsten, accounts, financiën, moeder- en dochtervennootschappen, gegevens van Opdrachtgever en opdrachtgevers en klanten van de Opdrachtgever en/of een lid van de Kantar Groep

1.1.17. **"Zeggenschap"** betekent (a) het bezit, direct of indirect, van de bevoegdheid om het management of het beleid van een dergelijke entiteit te sturen, hetzij door eigendom van stemrechtverlenende effecten, door een contract met betrekking tot stemrechten, of anderszins, of (b) eigendom, direct of indirect, van meer dan vijftig procent (50%) van de uitstaande stemrechtverlenende effecten of ander eigendomsbelang van een dergelijke entiteit.

2. DE DIENSTEN

2.1. Deze Algemene Inkoopvoorwaarden zijn van toepassing op de Diensten.

2.2. De Inkooporder wordt geacht aanvaard te zijn bij aanvang van de Diensten. De Leverancier verstrekt de Diensten vanaf de datum zoals gespecificeerd op de Inkooporder. De Leverancier verstrekt de Diensten aan de Opdrachtgever in overeenstemming met de verzoeken die de Opdrachtgever van tijd tot tijd doet, het Beleid van de Leverancier, best practices in de industrie en de voorwaarden van deze Overeenkomst. De tijdsplanning van de levering van de Diensten is van wezenlijk belang.

2.3. De Leverancier garandeert dat al het Personeel van Leverancier:

2.3.1. voldoet aan al het Beleid van de Leverancier, zoals van tijd tot tijd bijgewerkt;

2.3.2. deugdelijk gekwalificeerd en opgeleid is teneinde de Diensten te verstrekken;

2.3.3. deugdelijk gescreend is in overeenstemming met specifieke instructies van de Opdrachtgever en geen strafrechtelijke veroordelingen heeft; en

2.3.4. bevoegd is om te werken in het gebied waar de Diensten verstrekt worden.

2.4. De Leverancier garandeert, verbindt zich ertoe en verklaart dat hij voortdurend aan het volgende voldoet:

2.4.1. de Leverancier heeft volledige capaciteit en bevoegdheid om zijn verplichtingen ingevolge deze Overeenkomst aan te gaan en na te komen;

2.4.2. de Leverancier voldoet aan alle toepasselijke wetgeving, regelgeving en gedragscodes;

2.4.3. de Leverancier zal niets doen of nalaten met betrekking tot de nakoming van zijn verplichtingen ingevolge deze Overeenkomst dat een negatief effect heeft of kan hebben op de reputatie van de Opdrachtgever of diens cliënt; en

2.4.4. de Te Leveren Prestaties zijn in alle opzichten compleet, nauwkeurig, maken geen inbreuk en zijn conform deze Overeenkomst.

3. VERGOEDINGEN

3.1. De Leverancier is alleen gerechtigd om de Opdrachtgever te factureren nadat de Diensten naar redelijke tevredenheid van de Opdrachtgever zijn voltooid. De Opdrachtgever betaalt de Vergoedingen voor de Kosten op de volgende betalingscyclus van de Opdrachtgever nadat er zestig (60) dagen verstreken zijn na het einde van de maand waarin een geldige factuur waarop het juiste Inkoopordernummer vermeld staat ontvangen is. In het geval dat de Koper de Diensten namens een cliënt van de Leverancier koopt, is de Opdrachtgever niet verplicht om de Leverancier te betalen totdat de Opdrachtgever betaling van de cliënt ontvangen heeft. De Vergoedingen zijn exclusief omzetbelasting of vergelijkbare belastingen. De Opdrachtgever is gerechtigd om bedragen van de Vergoedingen af te trekken of in te houden indien dit door de wet is vereist.

3.2. De Leverancier is gerechtigd om rente in rekening te brengen over het onbetwiste bedrag, tegen een rentevoet van 2% boven de rentevoet op de basisherfinancieringstransacties van de Europese Centrale Bank per jaar.

4. BEËINDIGING

4.1. De Opdrachtgever is op ieder moment gerechtigd om deze Overeenkomst geheel of gedeeltelijk (met een proportionele vermindering van Vergoedingen) te beëindigen:

4.1.1. zonder opgave van reden met een schriftelijke kennisgeving aan de Leverancier van dertig (30) dagen; of

4.1.2. onmiddellijk indien de Leverancier een wezenlijke inbreuk maakt op de Overeenkomst die niet binnen 14 dagen nadat de Opdrachtgever de Leverancier vraagt om de inbreuk te herstellen verholpen is; of

4.1.3. onmiddellijk in het geval van een bevel of beslissing tot vereffening van de Leverancier of indien er voor de Leverancier een curator of bewindvoerder is aangesteld voor een deel van zijn activa, of indien er omstandigheden ontstaan op grond waarvan de rechtbank of een crediteur gerechtigd is om een curator of beheerder aan te stellen of indien de rechtbank tot de vereffening of bewindsvoering beveelt, of een regeling treft met crediteuren, of indien de Leverancier niet in staat is om zijn opeisbare schulden te voldoen.

4.2. Na afloop of beëindiging van deze Overeenkomst of een deel van de Diensten zal de Leverancier alle Vertrouwelijke Informatie aan de Opdrachtgever overhandigen en contact onderhouden met de Opdrachtgever en/of derde zodat er een soepele overdracht plaatsvindt.

4.3. De afloop of beëindiging van deze Overeenkomst doet geen afbreuk aan de rechten die tot de datum van de beëindiging zijn opgebouwd of andere bepalingen die uitdrukkelijk of impliciet van kracht blijven na de beëindiging.

5. AUDIT

5.1. De Leverancier houdt in verband met de Diensten tijdens deze Overeenkomst en gedurende 6 jaar daarna op zijn hoofdvestiging een juiste en nauwkeurige boekhouding bij (inclusief maar niet beperkt tot urenstaten, claims administratie, facturen, onkosten, kosten, kredietnota's) in overeenstemming met algemeen geaccepteerde regels voor het bewaren van boekhouding en documenten. De Leverancier staat de Opdrachtgever en/of zijn cliënt toe om dergelijke administratie na een redelijke schriftelijke kennisgeving te inspecteren om vast te stellen of deze Overeenkomst (inclusief, maar niet beperkt tot, de beperkingen neergelegd in Artikel 10) nageleefd wordt.

5.2. Indien de Opdrachtgever naar aanleiding van een audit ontdekt dat er in verband met de Diensten teveel is betaald of dat er sprake is van enige andere niet-naleving van de voorwaarden van deze Overeenkomst zal de Leverancier dergelijke niet-naleving onmiddellijk op zijn eigen kosten herstellen en de Opdrachtgever het volledig teveel betaalde bedrag en de kosten van de betreffende audit terugbetalen.

6. AANSPRAKELIJKHEID EN VRIJWARING

6.1. Niets in deze Overeenkomst kan de aansprakelijkheid van enige partij met betrekking tot de volgende vorderingen beperken of uitsluiten:

6.1.1. wegens dood of letselschade veroorzaakt door nalatigheid van dergelijke partij; of

6.1.2. als gevolg van fraude, inclusief bedrieglijke voorstellingen door dergelijke partij; of

6.1.3. waarvoor de aansprakelijkheid anderszins niet rechtmatig beperkt of uitgesloten kan worden; of

6.1.4. wegens een vrijwaring die door de Leverancier onder deze Overeenkomst aan de Opdrachtgever verstrekt is; of

6.1.5. vorderingen voor een inbreuk door de Leverancier van Artikelen 8 t/m 10 of 12.1; of

6.1.6. wegens een opzettelijke of bewuste niet-nakoming door de Leverancier.

6.2. Met inachtneming van Artikel 6.1, is de Opdrachtgever niet aansprakelijk voor indirecte, speciale of gevolgschade, of voor winstderving (direct of indirect), verlies van goodwill, zakelijke verliezen, inkomstenverlies of verlies van verwachte besparingen.

6.3. De Leverancier vrijwaart de Opdrachtgever jegens alle verliezen, kosten, aansprakelijkheden, schade, onkosten, vorderingen en procedures opgelopen en/of geleden door de Opdrachtgever als gevolg van of in verband met:

6.3.1. een inbreuk op deze Overeenkomst; of

6.3.2. een verlies of schade aan eigendommen van de Opdrachtgever tijdens de verstrekking van de Diensten; of

6.3.3. een onzorgvuldige handeling of nalaten door de Leverancier, Personeel van Leverancier en/of onderaannemers of hun medewerkers in verband met deze Overeenkomst; of

6.3.4. een vordering dat er met het gebruik van de Te Leveren Prestatie en/of Diensten een inbreuk gemaakt wordt op de Intellectuele Eigendomsrechten van een derde.

6.4. Met inachtneming van Artikel 6.1 en 6.2, is de totale aansprakelijkheid van de Opdrachtgever ontstaan uit of met betrekking tot deze Overeenkomst (op grond van de overeenkomst, onrechtmatige daad, inclusief nalatigheid, of anderszins) niet meer dan het bedrag aan Vergoedingen dat door de Opdrachtgever ingevolge deze Overeenkomst aan de Leverancier betaald of betaalbaar is in de twaalf (12) maanden voorafgaand aan de gebeurtenis waardoor dergelijke aansprakelijkheid ontstond.

6.5. Met inachtneming van Artikel 6.1 en 6.2, is de totale aansprakelijkheid van de Leverancier ontstaan uit of met betrekking tot deze Overeenkomst (op grond van de overeenkomst, onrechtmatige daad, inclusief nalatigheid, of anderszins) niet meer dan € 10.000.000 (tien miljoen Euro) per vordering.

7. VERZEKERING

7.1. De Leverancier sluit bij een gerenommeerde derde verzekeringsbedrijf een verzekering af om de verplichtingen en aansprakelijkheden ingevolge deze Overeenkomst te dekken en:

7.1.1. met betrekking tot zijn openbare aansprakelijkheid, voor een minimumbedrag van € 1.000.000 voor één gebeurtenis en onbeperkt in de relevante verzekeringsperiode;

7.1.2. met betrekking tot zijn werkgeversaansprakelijkheid, voor een minimumbedrag van € 5.000.000 voor één gebeurtenis en onbeperkt in de relevante verzekeringsperiode;

7.1.3. met betrekking tot zijn beroepsaansprakelijkheid, voor een minimumbedrag van € 1,000,000 voor één gebeurtenis en onbeperkt in de relevante verzekeringsperiode.

7.2. De Opdrachtgever wordt in dergelijke polis aangewezen als extra verzekerde en de polis bevat een vrijwaringsclausule voor opdrachtgevers. Een dergelijke verzekering zal niet tot een bijdrage oproepen en kan geen secundaire verzekering zijn ten opzichte van een andere verzekering die beschikbaar is voor de Opdrachtgever. De Opdrachtgever is niet aansprakelijk voor de betaling van enig eigen risico en dergelijk eigen risico is niet lager dan € 50.000.

7.3. De Leverancier sluit een extra verzekeringsdekking af als deze op enig moment redelijkerwijs nodig geacht wordt door de Opdrachtgever.

8. GEGEVENSBESCHERMING

8.1. Indien de Leverancier voor de verstrekking van de Diensten namens de Opdrachtgever persoonsgegevens moet verwerken zal de Leverancier voldoen aan het zevende beginsel in de Gegevensbeschermingswetgeving en:

8.1.1. voldoen aan de Gegevensbeschermingswetgeving;

8.1.2. alleen handelen op aanwijzingen van de Opdrachtgever als verwerkingsverantwoordelijke;

8.1.3. voldoen aan Bijlage 2 (Informatiebeveiliging Addendum);

8.1.4. voldoen aan Bijlage 3 (Gegevensbescherming).

8.2. De Leverancier vrijwaart de Opdrachtgever jegens alle verliezen, aansprakelijkheden, vorderingen, onkosten, schade en kosten geleden of opgelopen door de Opdrachtgever als gevolg van een tekortkoming van de Leverancier om zich te houden aan Gegevensbeschermingswetgeving, dit Artikel 8 en de bepalingen van Bijlage 3.

8.3. De Leverancier zal voldoen aan de specifieke voorwaarden vereist door AVG met betrekking tot de Diensten waarvoor de verwerking van Persoonsgegevens is vereist zoals beschreven in Bijlage 3.

8.4. De Leverancier garandeert dat hij maatregelen heeft getroffen waarvan de ISO/IEC 27001 Informatiebeveiligingsnorm of enige vergelijkbare norm zoals die op enig moment geldt, deel uitmaakt

9. INTELLECTUELE EIGENDOMSRECHTEN

9.1. Onder voorbehoud van 9.3, is de Opdrachtgever eigenaar van de Intellectuele Eigendomsrechten t.a.v. de Te Leveren Prestatie en de Leverancier draagt hierbij onherroepelijk en onvoorwaardelijk de volledige eigendom van alle Intellectuele Eigendomsrechten van de Te Leveren Prestaties aan de Opdrachtgever over ten tijde van de creatie daarvan. De Leverancier doet absoluut en onherroepelijk afstand en zal bewerkstelligen dat zijn personeel absoluut en onherroepelijk afstand doen ten gunste van de Opdrachtgever van hun morele rechten (indien van toepassing) met betrekking tot dergelijke Te Leveren Prestaties.

9.2. Niets in deze Overeenkomst is bedoeld om de eigendom van de Leverancier aan te tasten op de materialen gebruikt of ontwikkeld door de Leverancier onafhankelijk van de Diensten of de generieke methodes, middelen, technologie of processen die door de Leverancier worden gebruikt (maar hierdoor niet worden ontwikkeld) bij het uitvoeren van de Diensten (gezamenlijk te noemen: **"Bestaande Materialen van Leverancier"**). Indien de Bestaande Materialen van Leverancier (of een deel daarvan) verwerkt worden in de Te Leveren Prestaties, of indien deze vereist zijn om de Diensten te gebruiken of te benutten, verleent de Leverancier hierbij een eeuwigdurende, wereldwijde, onherroepelijke, niet-exclusieve, loyaltyvrije licentie aan de Opdrachtgever om de Bestaande Materialen van Leverancier te gebruiken teneinde de Opdrachtgever in staat te stellen om alle voordelen van de Diensten te genieten.

9.3. De Leverancier garandeert en verklaart dat hij het recht heeft om alle Intellectuele Eigendomsrechten die onder deze Overeenkomst zijn toegekend of overgedragen over te dragen of in licentie te geven en dat de toewijzing en de voorwaarden van de overdracht of licentie geen inbreuk maakt op de Intellectuele Eigendomsrechten van een derde.

9.4. De Leverancier zal op grond van deze Overeenkomst geen rechten of eigendomsrechten op of belangen verkrijgen in enige Intellectuele Eigendomsrechten die eigendom zijn van of aan de Opdrachtgever in licentie zijn gegeven door een derde en de Leverancier erkent dat dergelijke Intellectuele Eigendomsrechten het eigendom blijven van de Opdrachtgever en/of zijn licentiegevers.

10. GEEN OMKOPING

10.1. De Leverancier zal voldoen aan de Amerikaanse Wet op Corrupte Praktijken, (de Foreign Corrupt Practices Act), 15 U.S.C. §78dd-2 (hierna te noemen: de **"FCPA"**) en de Engelse Omkopingswetgeving (de UK Bribery Act 2010) (hierna te noemen: de **"UKBA"**) en zal ervoor zorgen dat zijn groepsvennootschappen, medewerkers en diens directeuren, werknemers, vertegenwoordigers en tussenpersonen of een derde die een dienst uitvoert voor de Opdrachtgever (hierna eenieder te noemen: een **"Verwante Persoon"**) de FCPA en de UKBA naleeft.

10.2. De Leverancier zal niet direct of indirect verzoeken, akkoord gaan met het ontvangen of accepteren van een financiële of andere genoegdoening in strijd met zijn/haar wettige plicht of om hem/haar ertoe te bewegen om zijn/haar invloed uit te oefenen of om een handeling of beslissing te bewerkstelligen of beïnvloeden (inclusief de ondeugdelijke uitvoering van een positie) om zaken voor de Opdrachtgever te verkrijgen of te behouden en zal bewerkstelligen dat iedere Verwante Persoon dit evenmin doet. De Leverancier stelt de Opdrachtgever onmiddellijk schriftelijk in kennis als hij op de hoogte raakt van een overtreding van de FCPA, UKBA of dit Artikel 10.

11. MATERIALEN OPRACHTGEVER EN KLANT

11.1. Eigendomsrechten op eigendommen van de Opdrachtgever of een klant van de Opdrachtgever die voor de uitvoering van de Diensten aan de Leverancier zijn verstrekt blijven toebehoren aan de Opdrachtgever of zijn klant (naargelang van toepassing).

11.2. Met inachtneming van een redelijke voorafgaande kennisgeving, zijn de Opdrachtgever of zijn klant gerechtigd om hun eigendom te allen tijde weer in bezit te nemen van de Leverancier.

11.3. De Leverancier houdt alle eigendommen van de Opdrachtgever of een klant van de Opdrachtgever in zijn bezit veilig en zal zich niet van dergelijk bezit ontdoen of hiervan afstand doen zonder de schriftelijke goedkeuring van de Opdrachtgever en zijn klant, behalve indien dit vereist is voor de levering van de Diensten.

11.4. De Leverancier doet hierbij afstand van enig retentierecht of ander recht dat hij anders misschien zou hebben op enig eigendom van de Opdrachtgever of een klant van de Opdrachtgever en houdt dit eigendom vrij van retentierechten en andere lasten.

11.5. De Leverancier gebruikt het eigendom van de Opdrachtgever of een klant van de Opdrachtgever alleen in verband met de levering van de Diensten waarop deze betrekking heeft.

12. MODERNE SLAVERNIJWET

12.1. De Leverancier garandeert dat:

12.1.1. noch de Leverancier, noch zijn functionarissen, medewerkers, vertegenwoordigers of onderaannemers:

a. een overtreding hebben gepleegd ingevolge de Moderne Slavernijwet (Modern Slavery Act) van 2015 (een **"MSA-overtreding"**);

b. in kennis zijn gesteld dat zij onderwerp zijn van een onderzoek met betrekking tot een beweerdelijke MSA-overtreding of vervolging ingevolge de Moderne Slavernijwet van 2015;

c. bekend zijn met enige omstandigheid binnen hun toeleveringsketen dat reden kan zijn voor een onderzoek met betrekking tot een beweerdelijke MSA-overtreding of vervolging ingevolge de Moderne Slavernijwet van 2015;

12.1.2. hij zal voldoen aan de Moderne Slavernijwet van 2015;

12.1.3. hij de Opdrachtgever onmiddellijk schriftelijk zal informeren als het op de hoogte raakt of reden heeft om aan te nemen dat een van zijn functionarissen, medewerkers, vertegenwoordigers of onderaannemers een verplichting van de Leverancier ingevolge dit artikel 12 heeft geschonden of mogelijk heeft geschonden.

13. ALGEMEEN

13.1. De Leverancier zal tijdens deze Overeenkomst en gedurende een periode van 5 jaar daarna alle Vertrouwelijke Informatie vertrouwelijk houden en zal dergelijke Vertrouwelijke Informatie niet gebruiken of aan een derde bekendmaken, tenzij dit strikt noodzakelijk is om de Diensten te leveren of indien vereist door de wet.

13.2. Het is een partij niet toegestaan om zonder de voorafgaande schriftelijke goedkeuring van de andere partij op enige wijze zijn rechten of verplichtingen ingevolge deze Overeenkomst te cederen, uit te besteden of op enige manier over te dragen. Het is de Klant echter wel toegestaan om zijn rechten (direct of indirect) aan een gelieerde onderneming.

13.3. Iedere bepaling van deze Overeenkomst is scheidbaar en staat los van andere bepalingen. De ongeldigheid of niet-afdwingbaarheid van een specifieke bepaling tast de andere bepalingen van deze Overeenkomst niet aan.

13.4. Ieder nalaten om een recht of rechtsmiddel ingevolge deze Overeenkomst, de wet of in billijkheid uit te oefenen of een vertraging in de uitoefening daarvan betekent niet dat er afstand is gedaan van de rechten of rechtsmiddelen of andere rechten of rechtsmiddelen.

13.5. Niets in deze Overeenkomst mag worden geïnterpreteerd als het oprichten of impliceren van enig partnerschap of agentschapsrelatie tussen de partijen.

13.6. Deze Overeenkomst vormt de gehele overeenkomst en overeenstemming tussen de partijen met betrekking tot de hierin behandelde onderwerpen en vervangt alle voorgaande overeenkomsten tussen de partijen met betrekking tot dergelijke zaken. Deze Overeenkomst kan slechts schriftelijk worden aangepast met de instemming van de Opdrachtgever en de Leverancier.

13.7. Geen enkele persoon die geen partij is bij deze Overeenkomst heeft enig rechten krachtens de Engelse Contracten (Recht van Derden) Wet uit 1999 (Contracts (Rights of Third Parties) Act 1999).

13.8. Iedere kennisgeving die ingevolge deze Overeenkomst gegeven dient te worden geschiedt schriftelijk en heeft

alleen geldig plaatsgevonden indien deze verzonden is naar het adres zoals vermeldt op de Inkooporder, per gewone post, per aangetekende post of speciale verzending.

13.9. Deze Overeenkomst en alle niet-contractuele verplichtingen worden beheerst door Engels recht en de partijen gaan ermee akkoord dat zij eventuele geschillen zullen voorleggen aan de niet-exclusieve bevoegdheid van de Engelse rechtbanken. De Engelstalige versie van deze Overeenkomst en enige kennisgeving of ander document met betrekking tot deze Overeenkomst, prevaleren in geval van een conflict.

BIJLAGE 1
KANTAR GEDRAGSCODE

Kantar en zijn bedrijven zijn op veel gebieden en in veel landen over de hele wereld actief. In alle gevallen respecteren we de nationale wetten, en waar relevant, alle andere wetten met een internationaal bereik, zoals de UK Bribery Act (Britse anti-omkoopwet), de US Foreign Corrupt Practices Act (Amerikaanse wet tegen buitenlandse corruptiepraktijken) en de UK Modern Slavery Act (Britse wet tegen moderne slavernij), en industriële gedragscodes. We streven ernaar ethisch te handelen in alle aspecten van ons bedrijf en de hoogste normen van eerlijkheid en integriteit te handhaven.

We verwachten en eisen van al onze zakelijke partners, inclusief onze leveranciers, dat ze in dezelfde mate streven naar ethisch gedrag en vragen u daarom om uw instemming met onze zakelijke gedragscode (in de eerste kolom), zoals gewijzigd voor niet-Kantar-entiteiten (in de tweede kolom), te bevestigen.

We verwachten van al onze leveranciers dat ze passende maatregelen hanteren op de naleving van enerzijds deze normen en anderzijds op de van toepassing zijnde lokale en internationale wetgeving.

We verwachten van onze leveranciers dat ze zich zichtbaar aan de principes van deze code houden en dat ze een doorlopend proces van risicobeheer hebben op het gebied van milieu, gezondheid en veiligheid, en arbeid en ethiek, dat samenhangt met de activiteiten van de leveranciers.

Leveranciers moeten werknemers aanmoedigen om bezorgdheid te melden zonder angst voor bedreiging of represailles te hoeven hebben. Leveranciers moeten hiertoe zo nodig passende maatregelen treffen.

Leveranciers dienen gelijkwaardige normen voor deze Code in te voeren voor hun eigen toeleveringsketen.

Kantar's Code	**Wat Kantar verwacht van haar leveranciers**
Wij, personeel en management van alle bedrijven in de Kantar Groep (**"de Groep"**), erkennen onze verplichtingen ten opzichte van iedereen die belang heeft bij het laten slagen van onze onderneming, inclusief aandeelhouders, klanten, bedrijfsleiding en toeleveranciers;	U bevestigt dat u onze verplichtingen erkent en dat u met uw handelen deze verplichtingen niet zult schaden.
Informatie over ons bedrijf zal helder en nauwkeurig gecommuniceerd worden, op een niet-discriminatoire manier en in overeenstemming met alle lokale regelgeving;	U bevestigt dat u informatie over de Kantar Groep op de wijze zoals hiernaast beschreven zult behandelen.
Wij selecteren en bevorderen onze mensen op basis van hun kwalificaties en verdiensten, zonder te discrimineren op basis van ras, religie, herkomst, huidskleur, geslacht, seksuele geaardheid, genderidentiteit of -expressie, leeftijd of handicap;	U bevestigt dat u een gelijkwaardig beleid voert binnen uw organisatie.
Wij zijn ervan overtuigd dat een werkplek veilig en beschaafd moet zijn; wij tolereren geen seksuele intimidatie, discriminatie of kwetsend gedrag van welke aard dan ook, inclusief het aanhoudend vernederen van individuen door woorden of daden, het vertonen of verspreiden van beledigende materialen, of het gebruik of het bezit van wapens in panden van Kantar of klanten;	U bevestigt dat u binnen uw organisatie en uw toeleveringsketen een gelijkwaardig beleid hanteert en dat u onze werkplek en mensen conform dat beleid respecteert. Vooral: • Werkgelegenheid moet vrij worden gekozen; gedwongen of gebonden arbeid of enige andere vorm van moderne slavernij mag niet worden gebruikt; • Werknemers mogen niet worden verplicht om paspoorten of door de overheid uitgegeven identiteitsbewijzen in te leveren als voorwaarde voor tewerkstelling; • Kinderarbeid mag niet worden gebruikt; • De aan werknemers betaalde vergoedingen moeten voldoen aan alle toepasselijke loonwetten; • Werkweken mogen het door de lokale wetgeving vastgestelde maximum niet overschrijden; • Er is geen onmenselijke behandeling van werknemers, waaronder seksuele intimidatie, seksueel misbruik, lijfstraffen, fysieke dwang of verbaal geweld;

	• Kantar verwacht van zijn leveranciers dat zij veilige werkomstandigheden voor alle werknemers creëren en bevorderen; • Blootstelling van werknemers aan fysieke gevaren moet waar mogelijk worden geëlimineerd of, indien dat niet mogelijk is, worden beheerst; • Leveranciers moeten over adequate procedures beschikken om noodsituaties aan te pakken die werknemers kunnen treffen; en • Systemen moeten aanwezig zijn om arbeidsongevallen en ziekte te beheren, op te sporen en te rapporteren.
Het gebruik, bezit of de distributie van illegale drugs, of personeel dat onder invloed van alcohol of drugs op het werk verschijnt, wordt door ons niet getolereerd;	U bevestigt dat u een gelijkwaardig beleid voert in uw organisatie en dat u onze werkplek en werknemers zoals beschreven zult behandelen.
Wij zullen alle informatie met betrekking tot de activiteiten van de Groep of hun klanten vertrouwelijk behandelen. In het bijzonder is "handelen met voorkennis" uitdrukkelijk verboden en vertrouwelijke informatie mag niet voor persoonlijk gewin worden gebruikt;	U bevestigt dat u instemt met ons informatiebeschermingsbeleid.
Wij zetten ons in voor de bescherming van gegevens van consumenten, klanten en werknemers in overeenstemming met nationale wetgeving en branche codes;	U bevestigt dat u in uw organisatie vergelijkbare maatregelen heeft getroffen die alle informatie van en met betrekking tot onze bedrijfsvoering en die van onze zakenpartners dekken.
Wij zullen geen werk verrichten dat voor zover ons bekend stellingen, suggesties of beelden bevat die in strijd zijn met het openbaar fatsoen en wij zullen de impact van ons werk op minderheidsgroeperingen grondig beoordelen, of dit nu minderheden zijn op basis van ras, religie, land van herkomst, huidskleur, geslacht, seksuele geaardheid, genderidentiteit of -expressie, leeftijd of handicap;	Voor zover van toepassing bevestigt u dat u vergelijkbare standaarden hanteert voor uw werk.
Wij zullen geen werk uitvoeren dat erop gericht of ontwikkeld is om te misleiden, inclusief met betrekking tot sociale, milieu- en mensenrechtenkwesties;	Voor zover van toepassing bevestigt u dat u vergelijkbare standaarden hanteert voor uw werk.
Wij zullen het risico op reputatieschade voor de Groep door klanten of opdrachten beoordelen voordat de activiteiten worden opgestart. Hieronder valt ook reputatieschade door samenwerking met klanten die deelnemen aan activiteiten die inbreuk maken op de mensenrechten;	Dit heeft alleen betrekking op leden van de Kantar Groep.
Wij zullen noch voor persoonlijk noch voor familiaal gewin direct of indirect betrokken zijn bij activiteiten die concurreren met bedrijven binnen de Groep of met onze verplichtingen ten opzichte van deze bedrijven;	Dit heeft alleen betrekking op leden van de Kantar Groep.
Wij zullen geen steekpenningen geven, aanbieden of accepteren, of dit nu in contanten of anderszins is, aan of van derden, inclusief maar niet beperkt tot overheidsbeambten, klanten en makelaars of hun vertegenwoordigers. Wij zullen er gezamenlijk voor zorgen dat alle medewerkers dit beleid begrijpen door middel van training, communicatie en door het geven van voorbeelden;	Dit is direct op u van toepassing.
Wij zullen geen persoonlijke zaken aanbieden ter stimulering van een zakelijke relatie. Dit is niet bedoeld om geschikt amusement of incidentele giften van beperkte waarde te verbieden tenzij de klant een beleid voert waarbinnen dit verboden is;	Dit is direct op u van toepassing.

Wij zullen voor persoonlijk gewin geen goederen of diensten accepteren voor meer dan de nominale waarde van toeleveranciers, mogelijke leveranciers of andere derde partijen;	Dit is direct op u van toepassing.
Wij zullen geen persoonlijke of familiale belangenverstrengelingen toestaan binnen onze bedrijven of met onze toeleveranciers of andere derde partijen met wie we zaken doen;	U zou een gelijkwaardig beleid moeten voeren binnen uw organisatie.
Er mogen geen zakelijke bijdragen voor minder dan de marktwaarde van welke aard dan ook, inclusief het leveren van diensten of materialen, gedaan worden aan politici, politieke partijen of actiecomités, zonder de voorafgaande schriftelijke goedkeuring van de Raad van Bestuur van Kantar; en	U zou uw eigen beleid moeten hebben met betrekking tot dergelijke bijdragen, inclusief passende autorisatieprocedures.
Wij zullen blijven streven naar een positieve bijdrage aan de samenleving en het milieu door: hoge normen voor marketingethiek te handhaven; binnen ons bedrijf, onze toeleveringsketen en onze klanten de mensenrechten te respecteren; respect voor het milieu; ondersteuning van maatschappelijke organisaties; ondersteuning van de ontwikkeling van medewerkers; en het beheren van aanzienlijke duurzaamheidsrisico's in onze toeleveringsketen. Ons duurzaamheidsbeleid en de verklaring inzake het mensenrechtenbeleid geven meer informatie over onze verplichtingen op deze gebieden.	U zou een gelijkwaardig beleid moeten hebben in uw organisatie. Vooral: • Leveranciers moeten voldoen aan de vereisten van de Britse Modern Slavery Act; • Leveranciers moeten alle relevante milieuvergunningen verkrijgen, inclusief voor afval en emissies; • Leveranciers moeten ernaar streven om verontreiniging te voorkomen door het implementeren van maatregelen in hun faciliteiten en processen, en door het recyclen, hergebruiken en vervangen van materialen.

We bevestigen dat we ons houden aan de Kantar Code of Business Conduct, zoals van toepassing op onze organisatie. Als we ons bewust worden van inbreuken, met name met betrekking tot omkoping of ongepaste geschenken of diensten aan of van uw organisatie of een andere derde partij, of met betrekking tot andere zaken die de reputatie van Kantar rechtstreeks of door associatie kunnen schaden, zullen we u onmiddellijk informeren.

Handtekening:

Naam:

Positie:

Organisatie:

Datum:

BIJLAGE 2
Addendum Informatiebeveiliging

1. Inleiding.
Deze Bijlage Beveiligingseisen (deze "Bijlage") stelt de basisvereisten voor de informatiebeveiliging van Leverancier vast die nodig zijn om de vertrouwelijkheid, beschikbaarheid en integriteit van de Vertrouwelijke Informatie van Opdrachtgever en de Vertrouwelijke Informatie van de klant van Opdrachtgever te waarborgen. Leverancier voldoet tijdens de levering van de diensten door Leverancier ingevolge deze Overeenkomst aan deze vereisten.

2. Terminologie.

2.1. De volgende termen zoals gebruikt in deze Bijlage (met één hoofdletter of allemaal kleine letters) hebben de volgende betekenis. Elke andere term met een hoofdletter die in deze bijlage gebruikt maar niet gedefinieerd wordt heeft de betekenis zoals bepaald in de Overeenkomst.

2.2. **Aannemer** betekent een onderaannemer, onafhankelijk aannemer, serviceprovider of agent van Leverancier die Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever opslaat, verwerkt, behandelt of hiertoe toegang heeft.

2.3. **Gevoelige informatie van Opdrachtgever** betekent alle Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever, waaronder Persoonsgegevens (e-mail, naam, enz.), gezondheidsinformatie, financiële informatie of beleggingsinformatie.

2.4. **Encryptie** betekent de omkeerbare transformatie van gegevens van het origineel (niet-versleutelde tekst) naar een gecodeerde opmaak (gecodeerde tekst) als mechanisme om de vertrouwelijkheid, integriteit en/of authenticiteit te beschermen. Voor de versleuteling is een encryptie-algoritme en één of meerdere encryptiesleutels vereist.

2.5. **Opslaan** betekent het opslaan, archiveren, een back-up maken en/of vergelijkbare taken uitvoeren.

3. Veiligheidscontrole.

3.1. Leverancier geeft Opdrachtgever het recht om het beveiligingsprogramma van Leverancier jaarlijks te controleren gedurende de periode dat Leverancier Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever verwerkt, opslaat of hiertoe anderszins toegang heeft. Leverancier zal tijdig (maar in geen geval later dan dertig (30) dagen na een verzoek van Opdrachtgever om dergelijke controle uit te voeren) dergelijke controle plannen op een wederzijds aanvaardbare datum.

3.2. Leverancier geeft Opdrachtgever toegang tot het beleid, de procedures en andere relevante documentatie van Leverancier, evenals tot het personeel van Leverancier indien dit redelijkerwijs nodig is om dergelijke controles uit te voeren. Leverancier zal binnen dertig (30) dagen na voltooiing van dergelijke controle een verbeterplan bij Opdrachtgever indienen waarin elk probleem tijdig en in overeenstemming met een verbeterschema zoals overeengekomen door de partijen wordt opgelost.

4. Specifieke Beveiligingseisen.

4.1. Beveiligingsbeleid

Leverancier houdt een uitgebreid beveiligingsbeleid en procedures in stand die ten minste het volgende dekken:

4.1.1. de verplichtingen van Leverancier t.a.v. informatiebeveiliging;

4.1.2. de classificatie, labeling en behandeling van informatie. Dergelijk beleid en procedures met betrekking de behandeling van informatie dient de toegestane methodes voor de verzending, opslag en vernietiging te beschrijven en dergelijke methodes mogen niet minder bescherming bieden dan zoals neergelegd in de hieronder uiteengezette Opdrachtgever Richtlijnen Informatiebescherming Leverancier;

4.1.3. acceptabel gebruik van de bedrijfsmiddelen van Leverancier, waaronder computersystemen, netwerken en berichtgeving;

4.1.4. beheer van informatiebeveiligingsincidenten, inclusief kennisgevingen m.b.t. datalekken en procedures voor de verzameling van bewijs;

4.1.5. authenticatieregels voor de opmaak, inhoud en gebruik van wachtwoorden voor eindgebruikers, beheerders en systemen;

4.1.6. toegangscontroles, inclusief periodieke evaluaties van toegangsrechten;

4.1.7. disciplinaire maatregelen voor Leverancier Personeel dat heeft nagelaten om te voldoen aan dergelijk beleid en procedures; en

4.1.8. de onderwerpen die beschreven zijn in de rest van dit Onderdeel 4, op een wijze die overeenstemt met dergelijke onderwerpen zoals beschreven in dit Onderdeel 4.

De leverancier moet Kantar binnen 30 dagen op de hoogte stellen van fundamentele wijzigingen in zijn beleid.

4.2. Verantwoordelijkheid voor het Informatiebeveiligingsprogramma van Leverancier

Leverancier draagt de verantwoordelijkheid voor de informatiebeveiligingsverplichting en wijst personeel aan om het informatiebeveiligingsprogramma van Leverancier in stand te houden en om informatiebeveiliging en informatierisicobeheer uit te voeren.

4.3. **Audits, Beoordelingen en Toezicht op het Informatiebeveiligingsprogramma van Leverancier**
Leverancier dient het Informatiebeveiligingsprogramma van Leverancier regelmatig aan een toezicht te onderwerpen en te controleren zodat de juiste veiligheidsmaatregelen zijn getroffen om de risico's voor Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever te beperken.

4.4. **Bedrijfsmiddelen en Informatiebeheer**
Leverancier zal:

4.4.1. een overzicht bijhouden van alle Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever die Leverancier verwerkt of opslaat;

4.4.2. een overzicht bijhouden van de fysieke IT-activa en software die Leverancier gebruikt bij de uitvoering van zijn activiteiten ingevolge deze Overeenkomst; en

4.4.3. de Opdrachtgever Richtlijnen Informatiebescherming Leverancier (hieronder uiteengezet) volgen bij het behandelen, verwerken en opslaan van de Vertrouwelijke Informatie van Opdrachtgever en de Vertrouwelijke Informatie van de klant van Opdrachtgever.

4.5. **Fysieke en omgevingsbeveiliging**
Leverancier zal:

4.5.1. toegang beperken tot de ruimtes van Leverancier waar Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever is opgeslagen of verwerkt of hiertoe toegang wordt verkregen waarbij uitsluitend personeel van Leverancier dat hiertoe bevoegd is toegang krijgt;

4.5.2. redelijke beste praktijken implementeren voor infrastructuursystemen, inclusief brandblus-, koel-, energie- en noodsystemen en de veiligheid van medewerkers;

4.5.3. fysieke toegangscontroles verzorgen voor alle ruimtes waar Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever wordt opgeslagen of verwerkt of hiertoe toegang wordt verkregen die in verhouding staan tot de gevoeligheid van de Vertrouwelijke Informatie van Opdrachtgever en de Vertrouwelijke Informatie van de klant van Opdrachtgever;

4.5.4. de ruimtes waar Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever wordt behandeld, opgeslagen en/of verwerkt regelmatig controleren.

4.6. **Personeel gerelateerde Kwesties**
Leverancier zal:

4.6.1. Een criminele achtergrondcontrole uitvoeren voor al het personeel van Leverancier (inclusief Aannemers), daar waar toegestaan door de wet, dat toegang heeft tot de Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever, voor zover toegestaan door toepasselijke wetgeving; dergelijke achtergrondcontroles dienen te worden uitgevoerd voordat dergelijk individu toegang heeft tot de Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever en Leverancier zal een individu zonder adequate achtergrondcontrole niet toestaan om toegang te krijgen tot Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever;

4.6.2. nieuw personeel (inclusief Aannemers) trainen t.a.v. het acceptabel gebruik en behandeling van de vertrouwelijke informatie van Leverancier en vertrouwelijke informatie van andere bedrijven die aan Leverancier is toevertrouwd (zoals Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever);

4.6.3. veiligheidscursussen en training bieden voor zijn personeel (inclusief Aannemers) en een register bijhouden van de medewerkers die dergelijke cursussen voltooid hebben; en

4.6.4. een formele gebruikersregistratie en uitschrijving procedure implementeren voor het toewijzen en intrekken van toegang tot de informatiesystemen en diensten van Leverancier; en na beëindiging van de contractuele relatie met personeel van Leverancier (inclusief Aannemers) zal Leverancier de toegang van die persoon tot Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever zo spoedig mogelijk (maar in ieder geval niet later dan twee (2) werkdagen na de beëindiging) intrekken.

4.7. **Communicatie en Activiteiten**
Leverancier zal:

4.7.1. regelmatig back-ups uitvoeren die genoegzaam zijn om de diensten binnen de overeengekomen hersteltijd (of indien er geen specifieke hersteltijd overeengekomen is tussen partijen, binnen een commercieel redelijke tijd) voor Opdrachtgever te herstellen;

4.7.2. alle media voor de back-up waarop Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever staat versleutelen overeenkomstig de hieronder uiteengezette Opdrachtgever Richtlijnen Informatiebescherming Leverancier;

4.7.3. geen Vertrouwelijke Informatie van Opdrachtgever of Vertrouwelijke Informatie van de klant van Opdrachtgever buiten de ruimtes van Leverancier opslaan of dit kopiëren zonder de voorafgaande schriftelijke goedkeuring van Opdrachtgever;

4.7.4. geen Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever aan een derde verzenden, overdragen of verstrekken, of een derde toegang verstrekken tot Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever zonder dat hiervoor voorafgaand schriftelijke goedkeuring is verkregen van Opdrachtgever;

4.7.5. indien een van de activiteiten zoals omschreven in leden (4.7.3) en (4.7.4) door Opdrachtgever zijn goedgekeurd zal Leverancier een overzicht bijhouden van de derden en/of locaties buiten de ruimtes van Leverancier waar Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever wordt opgeslagen of gekopieerd, de derden die Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever ontvangen of hiertoe toegang verkrijgen, het doel van het opslaan, kopiëren, verstrekken of toegang geven tot dergelijke Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever, de wijze waarop dergelijke Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever verzonden of anderszins aan dergelijke derde is verstrekt, de methode of het protocol (indien van toepassing) voor de verzending en versleuteling/bescherming die bij de verzending of anderszins verstrekking van dergelijke Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever gebruikt is, een beschrijving van de Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever die verzonden of anderszins is verstrekt aan dergelijke derde, de naam van de medewerker van Opdrachtgever die e.e.a. goedgekeurd heeft en de datum waarop dergelijke goedkeuring is verkregen;

4.7.6. bij het wissen of vernietigen van de Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever, procedures voor de vernietiging van data hanteren die voldoen aan de Norm voor Veilige Data Opschoning van het Britse Ministerie van Defensie (Department of Defense Standard for Secure Data Sanitization DOD 5220.22M), of deze overtreffen. Leverancier zal alle Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever onmiddellijk wissen of vernietigen na een schriftelijk verzoek van Opdrachtgever;

4.7.7. de Opdrachtgever Richtlijnen Informatiebescherming Leverancier (zoals hieronder uiteengezet) volgen, inclusief die betrekking hebben op de versleuteling, bij het verzenden of vervoeren van de Vertrouwelijke Informatie van Opdrachtgever en de Vertrouwelijke Informatie van de klant van Opdrachtgever;

4.7.8. versleuteling van de harde schijf gebruiken voor alle mobiele apparaten waarop enige Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever is opgeslagen of door het personeel van Leverancier wordt gebruikt om toegang te krijgen tot Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever. Dergelijke versleuteling dient in overeenstemming te zijn met de hieronder uiteengezette Opdrachtgever Richtlijnen Informatiebescherming Leverancier;

4.7.9. up-to-date malwaredetectie en preventie handhaven op de servers van Leverancier en/of platforms van de eindgebruiker waarmee Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever verzonden, benaderd, verwerkt of opgeslagen wordt of hiertoe toegang wordt verkregen;

4.7.10. een verharde internet perimeter en beveiligde infrastructuur handhaven met gebruik van firewall, antivirus, anti-malware, inbraakdetectiesystemen en andere beveiligingstechnologie die commercieel redelijk is; en

4.7.11. regulier patchmanagement en systeemonderhoud implementeren voor alle systeem van Leverancier die Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever verzenden, verwerken of opslaan of hiertoe toegang verkrijgen.

4.8. **Toegangscontrole**
Leverancier zal:

4.8.1. de beste praktijken voor gebruikersauthenticatie handhaven; indien er voor de authenticatie van personen of geautomatiseerde processen gebruikgemaakt wordt van wachtwoorden om toegang te krijgen tot de Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever dienen dergelijke wachtwoorden te voldoen aan de huidige beste praktijken voor het gebruik, aanmaken, opslag en bescherming van wachtwoorden. (Raadpleeg de Opdrachtgever Richtlijnen Informatiebescherming Leverancier hieronder);

4.8.2. ervoor zorgen dat gebruikers-ID's uniek zijn en niet gedeeld worden en verwijderd binnen 48 uur na beëindiging van een gebruiker bij de leverancier;

4.8.3. toegangsrechten toewijzen op basis van de gevoeligheid van de Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever, de functie-eisen van het individu en "need-to-

know" voor de specifieke Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever;

4.8.4. de toegangsrechten voor het personeel van Leverancier (inclusief Aannemers) ten minste ieder jaar controleren om ervoor te zorgen dat de "need-to-know"-beperkingen up-to-date zijn;

4.8.5. regelmatig rapporten beoordelen van de toegang door een gebruiker tot de faciliteiten van Leverancier waarop Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever staat; en

4.8.6. geen Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever onbeheerd achterlaten op desktops, printers of elders op een onveilige wijze binnen de faciliteiten van Leverancier.

4.9. **Applicatieontwikkeling; Kwetsbaarheidsscans en Penetratietesten**
Leverancier zal:

4.9.1. een veilige ontwikkelingsmethode implementeren waarin de beveiliging gedurende de gehele levenscyclus van de ontwikkeling is verwerkt;

4.9.2. veilige coderingsstandaarden ontwikkelen en afdwingen;

4.9.3. de veiligheid van codering controleren met gebruik van geautomatiseerde scanning-tools voor alle extern gerichte applicaties en voor software ontwikkeld door Leverancier (of een Aannemer) en geleverd aan Opdrachtgever;

4.9.4. ten minste één keer per kwartaal kwetsbaarheidsscans uitvoeren voor alle extern gerichte applicaties die Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever ontvangen, verwerken of opslaan of hiertoe toegang verkrijgen; Leverancier zal op verzoek van Opdrachtgever schriftelijk bevestigen dat Leverancier dergelijke kwetsbaarheidsscans heeft uitgevoerd;

4.9.5. een extern bedrijf gebruiken om ten minste één keer per jaar penetratietesten uit te laten voeren voor alle extern gerichte applicaties die Gevoelige Informatie van Opdrachtgever ontvangen, verwerken of opslaan of hiertoe toegang verkrijgen; dergelijke penetratietesten worden uitgevoerd door een leverancier van Leverancier die door Opdrachtgever is goedgekeurd; Leverancier zal op verzoek van Opdrachtgever schriftelijk bevestigen dat Leverancier dergelijke penetratietesten heeft uitgevoerd; en Leverancier zal alle wezenlijke kwesties die tijdens dergelijke penetratietesten uitgevoerd door of namens Leverancier zijn ontdekt binnen dertig (30) dagen herstellen, of, indien dergelijke kwesties niet binnen die periode van dertig (30) dagen kunnen worden hersteld, binnen een periode zoals onderling overeengekomen tussen Leverancier en Opdrachtgever.

4.10. **Aannemers**
Leverancier zal:

4.10.1. redelijke stappen nemen om Aannemers te selecteren en aan te houden die in staat zijn om veiligheidsmaatregelen in stand te houden om Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever in stand te houden in overeenstemming met toepasselijke wet- en regelgeving en op een dergelijke wijze die niet minder bescherming biedt dan de vereisten zoals uiteengezet in deze Overeenkomst, inclusief deze Bijlage. Leverancier zal met iedere Aannemer een overeenkomst sluiten op grond waarvan dergelijke Aannemer contractueel gehouden is om dergelijke veiligheidsmaatregelen te implementeren en in stand te houden;

4.10.2. een Aannemer geen Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever verstrekken of een Aannemer toestaan hiertoe toegang te krijgen of dit verwerken, op te slaan, te bekijken of op andere wijze mee om te gaan zonder de voorafgaande schriftelijke toestemming van Opdrachtgever;

4.10.3. verantwoordelijk zijn jegens Opdrachtgever voor alle handelingen en nalaten van een Aannemer, inclusief een nalaten van een Aannemer om te voldoen aan de bepalingen van deze Overeenkomst, inclusief deze Bijlage; en

4.10.4. regelmatig iedere Aannemer te beoordelen, inclusief een beoordeling van het beleid en de praktijken t.a.v. informatiebeveiliging van de Aannemer.

5. Beheer van Informatiebeveiligingsincidenten

5.1. Leverancier zal:

5.1.1. een proces voor het beheer van informatiebeveiligingsincidenten instellen, testen en behouden, waaronder processen voor het behoud van bewijsmateriaal, het informeren van en werken met wetshandhavingsinstanties, overheidsinstanties en in voorkomende gevallen vergelijkbare partijen en het uitvoeren van forensische analyses;

5.1.2. een Opdrachtgever schriftelijk informeren over een informatiebeveiligingsinbreuk waarbij Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever betrokken is, inclusief enige daadwerkelijke of vermoedelijke onbevoegde toegang tot Vertrouwelijke Informatie van

Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever of een informatiebeveiligingsincident waarbij de systemen, hardware, installaties, apparaten of bedrijfscomputers van de Aannemer betrokken waren of waarbij anderszins personeel van een Aannemer betrokken was; Leverancier zal een dergelijk incident onmiddellijk melden, maar in ieder geval niet later dan vierentwintig (24) uur na het moment waarop Leverancier voor het eerst gewaar wordt van een dergelijk incident. Leverancier zal Opdrachtgever hierna regelmatig updates versturen m.b.t. het onderzoek en beperking van een dergelijk incident. Leverancier staat Opdrachtgever of door Opdrachtgever aangewezen partijen toe om deel te nemen aan alle aspecten van het onderzoek. Leverancier is verantwoordelijk voor alle kosten gemaakt door een partij in verband met dergelijke incidenten, waaronder, maar niet beperkt tot, de kennisgeving aan getroffen betrokkenen, gerechtelijk onderzoek, kredietbewaking voor betrokkenen en andere corrigerende en juridische maatregelen; en

5.1.3. voor elk dergelijk incident, niet later dan tien (10) dagen na afsluiting van het incident door Leverancier een definitieve schriftelijke kennisgeving verstrekken aan Opdrachtgever, inclusief gedetailleerde informatie met betrekking tot de hoofdoorzaak van een dergelijk incident en plannen om een soortgelijk incident in de toekomst te voorkomen.

6. Bedrijfscontinuïteitsbeheer

6.1. Leverancier zal:

6.1.1. een uitgebreid bedrijfscontinuïteitsplan ("BCP") opstellen en behouden dat voorziet in het herstel van zowel de technologie als de bedrijfsactiviteiten in het geval van een ongepland incident;

6.1.2. zijn BCP ten minste ieder jaar testen of beoordelen op een wijze zoals hij naar eigen goeddunken deugdelijk acht.

7. Naleving

7.1. Leverancier zal:

7.1.1. voldoen aan de hieronder uiteengezette Opdrachtgever Richtlijnen Informatiebescherming Leverancier;

7.1.2. beleid en praktijken in onderlinge overeenstemming vaststellen en behouden voor het bewaren van documenten en vernietiging van data van toepassing op Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever en op andere informatie geproduceerd in de loop van of anderszins gerelateerd aan de activiteiten van Leverancier ingevolge deze Overeenkomst;

7.1.3. een ethische code vaststellen en medewerkers verplichten om deze code jaarlijks te bekijken en hiermee akkoord te gaan (mits en voor zover toegestaan door de wet).

8. Opvolgen risicobeheer-acties

8.1. Indien Opdrachtgever eerder een veiligheidscontrole heeft uitgevoerd m.b.t. Leverancier en/of één of meerdere van zijn faciliteiten (of van zijn Aannemers, indien van toepassing), en als resultaat van een dergelijke veiligheidsbeoordeling werden punten van zorg geïdentificeerd door de Opdrachtgever, zal Leverancier

8.1.1. indien hij dit niet reeds heeft gedaan, redelijke samenwerking verlenen aan Opdrachtgever om tijdig in onderlinge overeenstemming een risicobeheerplan op te stellen en dergelijke tot bezorgdheid stemmend onderdelen te herstellen en

8.1.2. de acties zoals gespecificeerd in het risicobeheerplan uiterlijk op de overeenkomstige datum zoals vermeld in het risicobeheerplan te implementeren

8.2. Het risicobeheerplan voor de meest recente veiligheidsbeoordeling wordt hieronder uiteengezet, of, als het onderstaande plan blanco is, zal worden uiteengezet in een ander document dat is opgesteld en goedgekeurd door de partijen

RISICOBEHEERPLAN		
Niveau van zorg	Actieplan	Datum
HOOG		
MEDIUM		
LAAG		

9. Identiteitsdiefstal

Indien Leverancier Persoonsgegevens verwerkt, behandelt of hiertoe toegang heeft zal Leverancier Opdrachtgever tijdig in kennis stellen als medewerkers van Leverancier tijdens de activiteiten van Leverancier ingevolge deze Overeenkomst op de hoogte zijn geraakt van een mogelijke identiteitsdiefstal m.b.t. een individu waarop dergelijke Persoonsgegevens betrekking hebben.

10. Updates

Opdrachtgever kan dit Addendum Informatiebeveiliging te allen tijde herzien met inachtneming van een schriftelijke kennisgeving van dertig (30) dagen aan Leverancier. Indien Leverancier van oordeel is dat hij niet kan voldoen aan dergelijke herzieningen zal Leverancier Opdrachtgever schriftelijk binnen deze periode van dertig (30) dagen informeren waarbij de specifieke onderdelen worden genoemd waaraan Leverancier niet kan voldoen. Opdrachtgever behoudt zich in een dergelijk geval het recht voor om enige of alle diensten of projecten met Leverancier te beëindigen zonder aansprakelijkheid of boete als gevolg van dergelijke beëindiging.

Aanhangsel 1
Opdrachtgever Richtlijnen Informatiebescherming Leverancier

Opdrachtgever Informatie Classificatie en Behandeling Matrix

Zonder dat de verplichtingen van Leverancier zoals uiteengezet in deze Overeenkomst (inclusief deze Bijlage) worden beperkt, geeft onderstaande tabel een samenvatting van bepaalde specifieke vereisten die van toepassing zijn bij het verzenden (of overdragen), opslaan of vernietigen van Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever, inclusief Gevoelige Informatie van Opdrachtgever.

Informatieclassificatie	Voorbeelden	Verzending	Opslag	Vernietiging
Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever, anders dan Gevoelige Informatie van Opdrachtgever	Bedrijfsstrategieën en plannen; Auditrapporten; Marketinginformatie voordat deze gepubliceerd wordt; Eigen software van Opdrachtgever; Technische specificaties of architecturen.	Elektronisch: Versleuteld indien deze via openbare netwerken wordt verzonden of buiten de ruimtes van Leverancier wordt overgedragen op draagbare media of apparaten of andere elektronische media; Afdruk: Via koerier versturen (inclusief bezorging de volgende dag) of per aangetekende post met een traceernummer.	Beperk toegang uitsluitend tot bevoegd personeel; voer ieder kwartaal controles van toegangsrechten uit. Bij voorkeur versleuteling indien in opslag.	Elektronisch: Gebruik DOD 5220.22M of vergelijkbare procedures. Afdruk: Versnipperen
Gevoelige Informatie van Opdrachtgever	Persoonlijke data (inclusief naam, e-mail, telefoon, postadres, BSN of rekeningnummer) Persoonlijke financiële informatie Persoonlijke gezondheidsinformatie	Hetzelfde als hierboven	Beperk toegang uitsluitend tot bevoegd personeel; voer ieder kwartaal controles van toegangsrechten uit. Versleuteling bij opslag is vereist.	Hetzelfde als hierboven

Versleuteling

Hieronder zijn de huidige encryptie-algoritmes uiteengezet waaraan Opdrachtgever de voorkeur geeft alsmede de huidige aanvullende acceptabele encryptie-algoritmes. Leverancier zal één van de gewenste encryptie-algoritmes gebruiken voor het versleutelen van Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever tenzij dit redelijkerwijs niet haalbaar is, in welk geval Leverancier één van de aanvullende acceptabele encryptie-algoritmes zal gebruiken voor het versleutelen van Vertrouwelijke Informatie van Opdrachtgever en Vertrouwelijke Informatie van de klant van Opdrachtgever.

Voorkeur Encryptie Algoritmes		
Doel	**Algoritmes**	**Minimale sleutellengte (bits)**
Sleuteluitwisseling	RSA Diffie-Hellman	bij voorkeur 2048, indien niet mogelijk dan 1024
Gegevensbescherming	AES in CBC modus 3DES in CBC EDE3 modus	bij voorkeur 256, indien niet mogelijk dan 128 168
Hash	SHA-256	n.v.t.
HMAC	HMAC SHA-256	256
Digitale Handtekening	RSA met SHA-256 DSA met SHA-256	bij voorkeur 2048, indien niet mogelijk dan 1024

Aanvullende Acceptabele Encryptie Algoritmes		
Doel	**Algoritmes**	**Minimale sleutellengte (bits)**
Gegevens- bescherming	AES in CTR modus RC4 RC5 in CBC modus Blowfish in CBC modus CAST-128 in CBC modus IDEA in CBC modus	bij voorkeur 2048, indien niet mogelijk dan 128
Hash	bij voorkeur SHA-2, indien niet mogelijk dan SHA-1 MD5 dient nooit gebruikt te worden tenzij er een uitzondering voor technologie nodig is.	n.v.t.
HMAC	bij voorkeur HMAC SHA-2, indien niet mogelijk dan SHA-1 MD5 dient nooit gebruikt te worden tenzij er een uitzondering voor technologie nodig is.	160 128
Digitale Handtekening	ECC met SHA-256, SHA-2 Bij voorkeur RSA met SHA-2, indien niet mogelijk dan SHA-1, Bij voorkeur DSA met SHA-2, indien niet mogelijk dan SHA-1	160 min bij voorkeur 2048, indien niet mogelijk dan 1024

Richtlijnen voor authenticatie d.m.v. een wachtwoord

Alle wachtwoorden die door Leverancier (of een Aannemer) beheerd of gecontroleerd worden dienen aan de volgende richtlijnen te voldoen:

Gebied	**Richtlijn**
Minimale wachtwoord lengte	8 tekens
Wachtwoord complexiteit	2 van de 4 teken types (hoofdletter, kleine letter, cijfer, speciaal), niet gemakkelijk te verbinden aan een individu of proces, komt niet voor in een woordenboek en is geen patroon. Het wordt sterk aanbevolen dat wachtwoorden 3 van de 4 lettertypes bevatten
Maximale levensduur wachtwoord	Maximaal 90 dagen
Minimale wachtwoord historie	1 dag
Bescherming tijdens transport	Verplicht. Wachtwoorden moeten tijdens transport versleuteld zijn.
Bescherming tijdens opslag	Verplicht. Wachtwoorden moeten gehasht zijn met gebruik van een goedgekeurd hash-algoritme (zie tabel hierboven).

KANTAR

Bijlage 3
Gegevensbescherming

1. DEFINITIES

1.1. In deze Bijlage 3 hebben de termen die hierin worden gebruikt maar niet anderszins in deze Overeenkomst worden gedefinieerd de betekenis zoals toegekend in de EU Richtlijn inzake Gegevensbescherming (AVG / GDPR).

1.1.1. betekent **Gedekte Persoonsgegevens** alle Persoonsgegevens die door de Leverancier tijdens het verstrekken van de Diensten of de uitvoering van zijn andere verplichtingen ingevolge deze Overeenkomst worden verwerkt;

1.1.2. betekent **Veiligheidsmaatregelen voor Gegevens** de administratieve, technische en fysieke Veiligheidsmaatregelen die beschermen tegen bedreigingen of risico's voor de integriteit en veiligheid van de onbevoegde of onopzettelijke vernietiging, verlies, wijziging of gebruik van en de onbevoegde toegang tot Gedekte Persoonsgegeven en die voldoen aan de beste praktijken in de industrie;

1.1.3. betekent **Modelvoorwaarden** de standaard contractuele bepalingen zoals goedgekeurd door het besluit van de Europese Commissie van 5 februari 2010 (2010/87/EU) met betrekking tot standaard contractuele bepalingen voor de overdracht van persoonsgegevens aan verwerkers gevestigd in derde landen (maar exclusief de contractuele bepalingen die door de Europese Commissie in dat besluit als optioneel bestempeld zijn), zoals van tijd tot tijd door de Europese Commissie aangepast of vervangen;

1.1.4. **"Subverwerker"** betekent elke derde partij die door de Leverancier is aangesteld om in het kader van de Overeenkomst In-Scope Persoonsgegevens namens de Klant te Verwerken;

1.1.5. De termen **"Verwerkingsverantwoordelijke", "Betrokkene", "Lidstaat", "Persoonsgegevens", "Verwerking", "Verwerker"** en **"Toezichthoudende autoriteit"** hebben dezelfde betekenis als in de AVG, en hun verwante termen zullen dienovereenkomstig worden uitgelegd; een verwijzing naar het overdragen van gegevens uit een land of gebied omvat, zonder beperking, toegang op afstand tot die gegevens van buiten dat land of gebied;

1.1.6. zijn de verwijzingen naar Toepasselijk Recht in Artikel 2.4 beperkt tot wetgeving van de Europese Unie of de Lidstaat waaraan de Leverancier onderworpen is, voor zover die Bepalingen van toepassing zijn met betrekking tot de Gedekte Persoonsgegevens waarvan de verwerking onderworpen is aan wetgeving van de Europese Unie of Lidstaat.

2. VERPLICHTINGEN

2.1. Elke Leverancier en Opdrachtgever zal te allen tijde voldoen aan zijn verplichtingen ingevolge alle Gegevensbeschermingswetgeving en al het toepasselijk Beleid van Leverancier in verband met deze Overeenkomst.

2.2. De Leverancier is niet gerechtigd om de Gedekte Persoonsgegevens voor enig ander doel te gebruiken dan om de Diensten te verlenen en zijn andere verplichtingen ingevolge deze Overeenkomst uit te voeren.

2.3. Rollen van de partijen. De partijen erkennen en komen overeen dat met betrekking tot de Verwerking van Gedekte Persoonsgegevens, Opdrachtgever de Verwerkingsverantwoordelijke is, Leverancier de Verwerker en alleen Subverwerkers mag inschakelen in overeenstemming met de vereiste uiteengezet in artikel 2.8.2(b) hieronder.

2.4. De Leverancier zal:

2.4.1. Gedekte Persoonsgegevens alleen in overeenstemming met de schriftelijke aanwijzingen van Opdrachtgever verwerken;

2.4.2. Opdrachtgever tijdig inlichten indien hij gewaar wordt van fouten of onnauwkeurigheden in Gedekte Persoonsgegevens;

2.4.3. ervoor zorgen dat, tenzij anderszins schriftelijk geïnstrueerd door Opdrachtgever of vereist door Gegevensbeschermingswetgeving, kopieën van Gedekte Persoonsgegevens in het bezit of onder het beheer van de Leverancier, een onderaannemer of personeel van Leverancier permanent worden vernietigd als ze niet langer nodig zijn voor de uitvoering van de verplichtingen van de Leverancier ingevolge deze Overeenkomst;

2.4.4. ervoor zorgen dat Gedekte Persoonsgegevens alleen toegankelijk zijn voor personeel van Leverancier dat:

a. toegang tot de gegevens nodig heeft om zijn rol uit te voeren bij de uitvoering van de verplichtingen van Leverancier ingevolge deze Overeenkomst;

b. deugdelijke training heeft ontvangen t.a.v. de vereisten van Gegevensbeschermingswetgeving van toepassing op de verwerking, zorg voor en behandeling van de gegevens; en

c. onderworpen is aan contractuele of wettelijke geheimhoudingsverplichtingen met betrekking tot de Gedekte Persoonsgegevens; en

2.4.5. met inachtneming van Artikel 2.15, de Opdrachtgever dergelijke samenwerking, hulp en informatie verlenen en alle documenten ondertekenen waarvan redelijkerwijs mag worden gevraagd om te helpen bij het voldoen aan hun verplichtingen ingevolge Gegevensbeschermingswetgeving voor zover deze betrekking hebben op Gedekte Persoonsgegevens en meewerken en voldoen aan de aanwijzingen of besluiten van enige bevoegde toezichthoudende autoriteit met betrekking tot dergelijke gegevens en om, in elk geval, binnen die tijd de

Opdrachtgever bij te staan te voldoen aan tijdslimieten opgelegd door Gegevensbeschermings-wetgeving of door de toezichthoudende autoriteit.

2.5. Met betrekking tot Gedekte Persoonsgegevens waarvan de verwerking onderworpen is aan wetgeving van de Europese Unie of een Lidstaat, zal de Leverancier:

2.5.1. dergelijke gegevens niet van een land of gebied overdragen, en zal ervoor zorgen dat een onderaannemer deze niet overdragen, en zal tevens van een Opdrachtgever niet verlangen dat deze een dergelijke overdracht bewerkstelligt, behalve:

a. tussen lidstaten van de Europese Unie, the Europese Economisch Ruimte;

b. op de schriftelijke instructie van Opdrachtgever, welke alsdan onderhevig is aan aanvullende redelijke beperkingen gesteld door Opdrachtgever; en te allen tijde met betrekking tot een soort overdracht, die tijdig aangegaan is (of verplicht is in geval van een overdracht door or aan een onderaannemer die de aannemer tijdig aangaat) een overeenkomst met de leverancier op Modelvoorwaarden aangepast maar voltooid op een dergelijke wijze zoals redelijkerwijs gestipuleerd door de Klant, of een dergelijk formulier die de Partijen schriftelijk overeengekomen zijn.

2.6. Met betrekking tot de Gedekte Persoonsgegevens die niet onder Artikel 2.5 vallen, maar waarvan de verwerking onderworpen is aan Gegevensbeschermingswetgeving die het volgende verbiedt of beperkt:

2.6.1. de overdracht van die Gedekte Persoonsgegevens aan een land of gebied of

2.6.2. de verwerking van die Gedekte Persoonsgegevens in een land of gebied, zal de Leverancier die Gedekte Persoonsgegevens niet overdragen of verwerken in strijd met dergelijk verbod of beperking.

2.7. De Leverancier zal:

2.7.1. te allen tijde beschikken over (en de functionaris voor gegevensbescherming van Opdrachtgever schriftelijk geïnformeerd houden over de identiteit van) Leverancierspersoneel die verantwoordelijk is voor het assisteren van Opdrachtgever bij het beantwoorden van vragen ontvangen van betrokkenen of een bevoegde gegevensbeschermingsautoriteit of privacy autoriteit;

2.7.2. ervoor zorgen dat Leverancierspersoneel waarnaar in Artikel 2.7.1 wordt verwezen altijd prompt en redelijkerwijs reageert op vragen zoals bedoeld in dat Artikel, waarbij volledig rekening wordt gehouden met de relevante vereisten van Gegevensbeschermingswetgeving wat betreft een tijdig antwoord; en

2.7.3. geen stappen nemen met betrekking tot een vraag zoals bedoeld in Artikel 2.7.1, behalve op schriftelijke instructies van de toepasselijke Opdrachtgever.

2.8. De Leverancier zal:

2.8.1. geen Gedekte Persoonsgegevens aan een derde openbaren of overdragen, behalve in het geval van een openbaarmaking of overdracht:

a. op schriftelijke instructies van de Opdrachtgever in overeenstemming met Artikel 2.5; of

b. voorzover vereist door Gegevensbeschermingswetgeving of een andere bepaling van deze Overeenkomst;

2.8.2. met betrekking tot de verwerking van Gedekte Persoonsgegevens door een onderaannemer:

a. voldoen aan de bepalingen van Artikel 13.2 (Overdracht, Onderaanneming);

b. ervoor zorgen dat verwerking door de subverwerker wordt uitgevoerd ingevolge een schriftelijk contract waarmee aan de subverwerker dezelfde verplichtingen worden opgelegd als opgelegd aan de Leverancier ingevolge deze Bijlage 3 (Gegevensbescherming: AVG);

c. bewerkstelligen dat de subverwerker die verplichtingen vervult en naleeft; en

d. indien de Opdrachtgever hierom vraagt, bewerkstelligen dat de subverwerker een schriftelijk contract aangaat met de Opdrachtgever, waarmee dezelfde verplichtingen aan de subverwerker worden opgelegd als opgelegd aan de Leverancier ingevolge deze Bijlage 3 (Gegevensbescherming: AVG).

2.9. De Leverancier:

2.9.1. zal Veiligheidsmaatregelen voor Gegevens vaststellen, implementeren en behouden, inclusief, als onderdeel van de Veiligheidsmaatregelen voor Gegevens, veiligheidsprocedures en praktijken om onbevoegde of onopzettelijke toegang tot of vernietiging, verlies, modificatie, gebruik of publicatie van Gedekte Persoonsgegevens te voorkomen;

2.9.2. garandeert Opdrachtgever dat de Leverancier schriftelijke veiligheidsbeleid, procedures en praktijken heeft die voldoen aan de gegevensbeveiligingsverplichtingen van de Leverancier ingevolge Gegevensbeschermingswetgeving;

2.9.3. zal op iedere faciliteit van waaruit de Leverancier de Diensten verleent de Veiligheidsmaatregelen voor Gegevens in stand houden en afdwingen, evenals met betrekking tot alle netwerken waar Gedekte Persoonsgegevens worden verwerkt; en

2.9.4. zal de Veiligheidsmaatregelen voor Gegevens van tijd tot tijd beoordelen en herzien in overeenstemming met heersende praktijken in de industrie en zoals redelijkerwijs verzocht door Opdrachtgever (en zal op verzoek prompt

Opdrachtgever schriftelijk informeren over dergelijke aangepaste Veiligheidsmaatregelen voor Gegevens).

2.10. In het geval van onbevoegde of onopzettelijke toegang tot of gebruik of openbaarmaking van Gedekte Persoonsgegevens, of indien de Leverancier redelijkerwijs gelooft dat een dergelijke toegang, gebruik of openbaarmaking heeft plaatsgevonden of het risico bestaat dat het zal plaatsvinden (inclusief, zonder beperking, het verlies van of de onmogelijkheid om media, apparaat, of installatie waarop Gedekte Persoonsgegevens opgeslagen staan of kunnen staan) zal de Leverancier:

2.10.1. de Opdrachtgever zonder vertraging informeren, in ieder geval binnen vierentwintig (24) uur, waarbij redelijke details worden verstrekt van de impact op de Opdrachtgever van de toegang, het gebruik of de openbaarmaking en de door de Leverancier genomen of te nemen corrigerende maatregelen;

2.10.2. met inachtneming van Artikel 2.15, onmiddellijk alle nodige en passende corrigerende maatregelen treffen om de onderliggende oorzaak van de toegang, het gebruik of de openbaarmaking te verhelpen;

2.10.3. alle maatregelen nemen met betrekking tot de toegang, het gebruik of de openbaarmaking die wordt vereist door Gegevensbeschermingswetgeving, inclusief, zonder beperking, op verzoek van de Opdrachtgever, het verstrekken van kennisgevingen aan betrokkenen wiens persoonsgegevens mogelijk zijn getroffen, ongeacht of een dergelijke kennisgeving vereist is door Gegevensbeschermingswetgeving; en

2.10.4. indien de toegang, het gebruik of de openbaarmaking zou kunnen leiden tot toegang tot financiële informatie van een betrokkene of tot een redelijk risico op identiteitsdiefstal of fraude, zal de Leverancier gedurende een redelijke periode (maar niet minder dan één (1) jaar), kredietbewakingsdiensten verstrekken voor dergelijke betrokkenen.

2.11. Naast eventuele auditrechten binnen de Overeenkomst en op verzoek van de Opdrachtgever en met inachtneming van de redelijke discretie van de Opdrachtgever, staat de Leverancier de Opdrachtgever (hetzij door hemzelf of namens zijn klanten) of een door de Opdrachtgever geïnstrueerde onafhankelijke auditor toe om de gegevens van de Leverancier te auditeren en te beoordelen, en de goedgekeurde Subverwerker, het informatiebeveiligingsprogramma, de gegevensverwerkingsfaciliteiten en het nalevingsprogramma voor gegevensbescherming om de naleving van dit Bijlage 3 (Gegevensbescherming), de Wetgeving inzake gegevensbescherming en de verplichtingen van de Opdrachtgever of de eigen klanten van de Opdrachtgever ("Gegevensbescherming en veiligheidsaudit").

2.12. Een dergelijke gegevensbeschermings- en beveiligingsaudit kan tests omvatten die bedoeld zijn om inbreuk te maken op het informatiebeveiligingsprogramma van de leverancier of de goedgekeurde subverwerker en de bijbehorende beveiligingsmaatregelen (inclusief tests voor beveiligingspenetratie) en moeten worden uitgevoerd met niet minder dan tien (10) dagen voorafgaande schriftelijke merk op.

2.13. Indien de Opdrachtgever redelijkerwijs van mening is dat de resultaten van een gegevensbeschermings- en beveiligingsaudit een zwak punt in de door de leverancier of de goedgekeurde subverwerker genomen veiligheidsmaatregelen aan het licht brengt, zal de leverancier deze zwakte evalueren en binnen een termijn van door de Opdrachtgever overeengekomen termijnen.

2.14. De Leverancier erkent dat een regelgevende instantie of diens agent van tijd tot tijd de Leverancier of een goedgekeurde Subverwerker kan auditen, en dat een dergelijke audit niet onderworpen zal zijn aan een van de beperkingen uiteengezet in deze Clausules 2.11 tot 2.14.

2.15. Opdrachtgever:

2.15.1. is zelf verantwoordelijk voor het instrueren van de Leverancier om dergelijke stappen te nemen in de verwerking van persoonsgegevens namens Opdrachtgever, die redelijkerwijs nodig zijn voor de uitvoering van de verplichtingen van de Leverancier ingevolge deze Overeenkomst; en

2.15.2. machtigt de Leverancier, voor zover toegestaan door Gegevensbeschermingswetgeving, om soortgelijke instructies namens Opdrachtgever aan de onderaannemers te verstrekken.

2.16. De kosten en onkosten die de Leverancier maakt bij de voldoening aan Artikelen 2.4.5, 2.10.2, 2.10.3 en 2.10.4 worden gedragen:

2.16.1. door de Leverancier in de gevallen dat de actie genomen dient te worden door de Leverancier als gevolg van een niet-nakoming van deze Overeenkomst of een nalatigheid, opzettelijk of frauduleus handelen of nalaten door de Leverancier, inclusief het nalaten om te voldoen aan de AVG, een onderaannemer of Personeel van Leverancier; en

2.16.2. door Opdrachtgever in andere gevallen.

2.17. Leverancier zal te allen tijde op verzoek van Opdrachtgever alle Persoonsgegevens waarvan Opdrachtgever de enige Verwerkingsverantwoordelijke is en die door Leverancier namens Opdrachtgever in het kader van de Overeenkomst worden Verwerkt, aan Opdrachtgever retourneren en/of op verzoek van Opdrachtgever verwijderen uit zijn systemen, met uitzondering van back-upkopieën die de Leverancier of zijn Gelieerde Ondernemingen moeten bewaren om te voldoen aan de toepasselijke wet- of regelgevingsvereisten, op voorwaarde dat dergelijke kopieën vertrouwelijk en veilig worden bewaard in overeenstemming met Bijlage 3 (Gegevensbescherming).

Ondertekend voor en namens de leverancier

Ondertekend .....

Naam .....

Functie .....

Bedrijfsnaam .....

Datum .....