OVEREENKOMST INZAKE DE VERWERKING VAN PERSOONSGEGEVENS VOOR SAP SUPPORT EN PROFFESIONAL SERVICES

1. ACHTERGROND

1.1 Doel en toepassing. Dit document ("**GVO**") wordt opgenomen in de Overeenkomst en maakt deel uit van een schriftelijke (eventueel in elektronische vorm opgestelde) overeenkomst tussen SAP en de Klant. Deze GVO geldt voor Persoonsgegevens die door de Klant of een Voor De Verwerking Verantwoordelijke worden verstrekt in verband met de uitvoering van de SAP-services ("SAP-service(s)") die worden gespecificeerd in de desbetreffende Overeenkomst, waarvan deze GVO een bijlage is. Deze GVO kan het volgende omvatten:

- **(a)** SAP Support, zoals wordt gedefinieerd in de Softwarelicentie- en -supportovereenkomst; en/of
- **(b)** Professional Services, zoals deze worden beschreven in de serviceovereenkomst tussen SAP en de Klant ("Serviceovereenkomst").

1.2 Structuur. Bijlagen 1 en 2 worden opgenomen in en maken deel uit van deze GVO. Ze stipuleren wat is overeengekomen qua onderwerp, aard en doel van de verwerking, het soort Persoonsgegevens, de gegevenscategorieën, de betrokkenen en de geldende technische en organisatorische maatregelen.

1.3 AVG. SAP en de Klant komen overeen dat elk der partijen de verantwoordelijkheid draagt om de vereisten die uit hoofde van de Algemene Verordening Gegevensbescherming 2016/679 ("**AVG**") voor Voor De Verwerking Verantwoordelijken en Verwerkers gelden te bekijken en door te voeren en dit met name voor wat betreft de Artikelen 28 en 32 tot en met 36 van de AVG, indien en voor zover van toepassing op Persoonsgegevens van de Klant of van Voor De Verwerking Verantwoordelijken die in het kader van de GVO worden verwerkt. Ter illustratie staan in Bijlage 3 de relevante AVG-vereisten en de bijbehorende artikelen van deze GVO.

1.4 Aansturing. In het kader van de GVO treedt SAP op als Verwerker en treden de Klant en de entiteiten aan wie zij toestemming geeft Persoonsgegevens op te nemen in systemen die tijdens de uitvoering van de SAP-service voor SAP toegankelijk zijn op als Voor De Verwerking Verantwoordelijken. De Klant treedt op als enig contactpunt en is volledig verantwoordelijk voor het verkrijgen van alle relevante machtigingen, instemmingen en toestemmingen voor de verwerking van Persoonsgegevens conform deze GVO, inclusief, waar van toepassing, toestemming van Voor De Verwerking Verantwoordelijken voor de inzet van SAP als Verwerker. Indien machtigingen, instemmingen, instructies of toestemmingen door de Klant worden verstrekt, worden deze niet alleen namens de Klant maar ook namens alle eventuele andere Voor De Verwerking Verantwoordelijken verstrekt. Indien SAP de Klant ergens over informeert of van in kennis stelt, wordt dergelijke informatie of een dergelijke kennisgeving geacht te zijn ontvangen door de Voor De Verwerking Verantwoordelijken aan wie de Klant toestemming heeft gegeven Persoonsgegevens op te nemen en is de Klant er verantwoordelijk voor dat dergelijke informatie en kennisgevingen worden doorgestuurd naar de desbetreffende Voor De Verwerking Verantwoordelijken.

2. VEILIGHEID VAN DE VERWERKING

2.1 Passende technische en organisatorische maatregelen. SAP heeft de technische en organisatorische maatregelen geïmplementeerd die in Bijlage 2 worden beschreven en past deze toe. De Klant heeft deze maatregelen beoordeeld en stemt ermee in dat de maatregelen passend zijn gezien de technologische actualiteit, de implementatiekosten en de aard, scope, context en doelstellingen van de verwerking van de Persoonsgegevens.

Bijlage 2 is uitsluitend van toepassing voor zover dergelijke SAP-services op of vanaf SAP-locaties worden uitgevoerd. Indien SAP SAP-services uitvoert op de locatie van de Klant en SAP toegang krijgt tot de systemen en gegevens van de Klant, dient SAP te voldoen aan de redelijke (beheers)technische en fysieke voorwaarden die de Klant stelt om dergelijke gegevens te beschermen en tegen toegang door onbevoegden te beveiligen. Als er toegang wordt verkregen

tot systemen en gegevens van de Klant, is de Klant er verantwoordelijk voor dat SAP-medewerkers gebruikersautorisaties en wachtwoorden krijgen voor toegang tot de systemen en dat deze autorisaties worden ingetrokken en deze toegangsrechten worden beëindigd zodra de Klant dit wenselijk acht. De Klant mag SAP geen toegang geven tot de systemen van Licentienemers of tot persoonsgegevens (van de Klant of van derden), tenzij deze toegang essentieel is voor de uitvoering van SAP-services. De Klant mag geen Persoonsgegevens opslaan in niet-productieomgevingen.

2.2 **Wijzigingen.** SAP past de technische en organisatorische maatregelen die in Bijlage 2 worden beschreven toe voor alle klanten van SAP die dezelfde SAP-service ontvangen. SAP mag de in Bijlage 2 genoemde maatregelen te allen tijde zonder kennisgeving wijzigen, mits er een vergelijkbaar of beter beveiligingsniveau in stand wordt gehouden. Afzonderlijke maatregelen mogen worden vervangen door nieuwe maatregelen die hetzelfde doel dienen zonder het beveiligingsniveau van de Persoonsgegevens te verlagen.

3. VERPLICHTINGEN VAN SAP

3.1 **Instructies van de Klant.** SAP verwerkt Persoonsgegevens uitsluitend conform de gedocumenteerde instructies van de Klant. De Overeenkomst (waaronder deze GVO) bestaat uit dergelijke gedocumenteerde initiële instructies en de Klant kan hiernaast aanvullende instructies verstrekken tijdens de uitvoering van de SAP-service. SAP zal redelijke inspanningen verrichten om eventuele andere instructies van de Klant te volgen, voor zover deze door de Privacywetgeving vereist worden, technisch haalbaar zijn en geen wijzigingen in de uitvoering van de SAP-service noodzakelijk maken. Indien enige van de hiervoor genoemde uitzonderingen van toepassing zijn of indien SAP anderszins niet aan een instructie kan voldoen dan wel van mening is dat een instructie een overtreding van de Privacywetgeving vormt, stelt SAP de Klant hiervan onmiddellijk in kennis (e-mail toegestaan).

3.2 **Verwerking op grond van een wettelijk vereiste.** SAP mag ook Persoonsgegevens verwerken indien dit door relevante wetgeving wordt vereist. SAP dient de Klant in dergelijke gevallen over deze wettelijke eis te informeren voordat de verwerking plaatsvindt, tenzij de desbetreffende wet een dergelijke informatieverstrekking met het oog op zwaarwegende publieke belangen verbiedt.

3.3 **Personeel.** SAP en haar Subverwerkers mogen ten behoeve van de verwerking van Persoonsgegevens uitsluitend toegang verlenen aan bevoegd personeel dat zich tot geheimhouding heeft verbonden. SAP en haar Subverwerkers trainen het personeel dat toegang heeft tot Persoonsgegevens regelmatig op het gebied van de geldende gegevensbeveiligings- en privacymaatregelen.

3.4 **Samenwerking.** Indien de Klant hierom verzoekt, werkt SAP in redelijke mate samen met de Klant en de Voor De Verwerking Verantwoordelijken bij verzoeken van Betrokkenen of toezichthouders inzake de verwerking van Persoonsgegevens door SAP of een eventuele Inbreuk op Persoonsgegevens. SAP dient de Klant zo snel als praktisch gezien mogelijk is in kennis te stellen van een verzoek dat zij van een Betrokkene inzake de verwerking van Persoonsgegevens heeft ontvangen en zal, voor zover van toepassing, niet zonder verdere instructies van de Klant zelf op een dergelijk verzoek reageren. SAP corrigeert of verwijdert eventuele Persoonsgegevens waar zij over beschikt of beperkt haar verwerking van deze gegevens conform de instructies van de Klant en de bepalingen van de Privacywetgeving.

3.5 **Kennisgeving inzake Inbreuk op Persoonsgegevens.** SAP stelt de Klant er zonder onnodig uitstel van in kennis indien zij op de hoogte raakt van een Inbreuk op Persoonsgegevens en verstrekt in de mate van het redelijke alle informatie waarover zij beschikt en waarmee zij de Klant kan helpen aan haar verplichtingen te voldoen bij het melden van de Inbreuk op Persoonsgegevens uit hoofde van de Privacywetgeving. SAP mag dergelijke informatie in fasen beschikbaar stellen naarmate deze beschikbaar komt. Een dergelijke kennisgeving mag niet worden opgevat of geïnterpreteerd als een erkenning van een fout of van aansprakelijkheid van SAP.

3.6 Effectanalyse gegevensbeveiliging. Indien de Klant (of haar Voor De Verwerking Verantwoordelijken) krachtens de Privacywetgeving een effectanalyse voor de gegevensbeveiliging moet (moeten) uitvoeren of van tevoren met een toezichthouder moet (moeten) overleggen, zal SAP op verzoek van de Klant de documenten verstrekken die in algemene zin voor de SAP-service beschikbaar zijn (bijvoorbeeld deze GVO, de Overeenkomst, auditrapporten en certificeringen). Eventuele verdere assistentie dient door de Partijen onderling te worden overeengekomen.

4. GEGEVENSVERWIJDERING

De Klant instrueert SAP hierbij de (eventuele) bij SAP achtergebleven Persoonsgegevens binnen een redelijk tijdsbestek (van niet meer dan zes maanden) conform de Privacywetgeving te verwijderen zodra de Persoonsgegevens niet meer nodig zijn voor de uitvoering van de Overeenkomst, tenzij de geldende wetgeving een langere bewaartermijn voorschrijft.

5. CERTIFICERINGEN EN AUDITS

5.1 Klantaudit. De Klant of een onafhankelijke als auditor optredende derde die redelijkerwijs aanvaardbaar is voor SAP (waarbij het niet mag gaan om als auditor optredende derden die concurrenten van SAP zijn of die onvoldoende gekwalificeerd of onafhankelijk zijn) mag de service- en supportleveringscentra en de IT-beveiligingsmethoden van SAP met betrekking tot de door SAP verwerkte Persoonsgegevens uitsluitend aan een audit onderwerpen indien:

- **(a)** SAP onvoldoende heeft aangetoond dat ze aan de technische en organisatorische maatregelen voldoet, zoals dit wordt aangetoond door certificering voor ISO 27001 of voor andere normen (met een in het certificaat vastgestelde scope); certificeringen zijn beschikbaar op https://www.sap.com/corporate/en/company/quality.html#certificates of, indien een certificering online niet beschikbaar is, op verzoek; of
- **(b)** zich een Inbreuk op Persoonsgegevens heeft voorgedaan; of
- **(c)** er formeel een audit is aangevraagd door de privacytoezichthouder van de Klant; of
- **(d)** verplichte Privacywetgeving de Klant een rechtstreeks auditrecht geeft, met dien verstande dat de Klant slechts eenmaal per periode van twaalf maanden een audit mag uitvoeren, tenzij de verplichte Privacywetgeving frequentere audits verplicht stelt.

5.2 Audit door andere Voor De Verwerking Verantwoordelijke. Elke andere Voor De Verwerking Verantwoordelijke mag de beheeromgeving en beveiligingsmethoden van SAP met betrekking tot door SAP verwerkte Persoonsgegevens uitsluitend aan een audit conform Artikel 5.1 onderwerpen indien een van de in Artikel 5.1 genoemde gevallen van toepassing is op een dergelijke andere Voor De Verwerking Verantwoordelijke. Een dergelijke audit dient via en door de Klant te worden uitgevoerd conform Artikel 5.1, tenzij de audit uit hoofde van de Privacywetgeving door de andere Voor De Verwerking Verantwoordelijke zelf dient te worden uitgevoerd. Indien verschillende Voor De Verwerking Verantwoordelijken waarvan de Persoonsgegevens op basis van de Overeenkomst door SAP worden verwerkt om een audit vragen, dient de Klant alle redelijke inspanningen te doen om de audits te combineren en meerdere audits te vermijden.

5.3 Scope van de audit. De Klant dient ten minste zestig dagen vóór de audit hiervan kennisgeving te doen, tenzij de verplichte Privacywetgeving of een bevoegde privacytoezichthouder een kortere kennisgevingsperiode eist. De frequentie, het tijdsbestek en de scope van de audits dienen door de partijen onderling in redelijkheid en te goeder trouw te worden overeengekomen. Klantaudits dienen voor zover mogelijk tot remote audits te worden beperkt. Indien een audit op locatie verplicht is, mag deze niet langer dan een werkdag duren. Afgezien van dergelijke beperkingen gebruiken de partijen actuele certificeringen en andere auditrapporten om auditherhalingen te voorkomen of tot een minimum te beperken. De Klant dient de resultaten van de audit aan SAP te doen toekomen.

5.4 **Kosten van audits.** De kosten van een audit komen voor rekening van de Klant, tenzij de audit een wezenlijke overtreding door SAP van deze GVO uitwijst. In dat geval komen de kosten van de audit voor rekening van SAP. Indien uit een audit blijkt dat SAP haar verplichtingen uit hoofde van de GVO heeft verzuimd, herstelt SAP dit verzuim onmiddellijk voor eigen rekening.

6. SUBVERWERKERS

6.1 **Toegestaan gebruik.** SAP krijgt een algemene autorisatie om de verwerking van Persoonsgegevens uit te besteden aan Subverwerkers, op voorwaarde dat:

(a) SAP of, namens SAP, SAP SE met de Subverwerker een schriftelijke (eventueel in elektronische vorm opgestelde) overeenkomst aangaat die de bepalingen van deze GVO weerspiegelt voor de verwerking van Persoonsgegevens door de Subverwerker; SAP is aansprakelijk voor inbreuken door de Subverwerker volgens de bepalingen van de Overeenkomst;

(b) SAP, alvorens een Subverwerker te selecteren, de beveiligings-, privacy- en geheimhoudingssituatie bij de Subverwerker evalueert om vast te stellen of de Subverwerker het in deze GVO vereiste beschermingsniveau voor Persoonsgegevens kan bieden;

(c) SAP, in het geval van SAP Support, op https://support.sap.com/en/my-support/subprocessors.html een lijst met Subverwerkers publiceert die op de ingangsdatum van de Overeenkomst geldt of deze lijst op verzoek aan de Klant verstrekt; deze lijst dient de naam, het adres en de rol te omvatten van elke Subverwerker die SAP gebruikt om de SAP-service te leveren ; en

(d) SAP, in het geval van Professional Services, op verzoek van de Klant al vóór aanvang van de desbetreffende SAP-services de lijst beschikbaar stelt of de Subverwerkers identificeert.

6.2 **Nieuwe Subverwerkers.** SAP kan naar eigen goeddunken Subverwerkers inzetten, op voorwaarde dat:

(a) SAP de Klant van tevoren informeert over beoogde toevoegingen aan of vervangingen in de lijst met Subverwerkers en daarbij de naam, het adres en de rol van de nieuwe Subverwerker vermeldt. In het geval van (1) SAP Support gebeurt dit via een post op het SAP Support Portal of via e-mail, zodra de Klant zich op het SAP Portal heeft geregistreerd, en in het geval van (2) Professional Services gebeurt dit via een vergelijkbare post op het SAP Support Portal, via e-mail of in een andere schriftelijke vorm.

(b) De Klant mag bezwaar tegen dergelijke wijzigingen maken, zoals wordt beschreven in Artikel 6.3.

6.3 **Bezwaren tegen nieuwe Subverwerkers.**

(a) SAP Support: indien de Klant uit hoofde van de Privacywetgeving een legitieme reden heeft om bezwaar te maken tegen de verwerking van Persoonsgegevens door de nieuwe Subverwerker, mag de Klant SAP Support beëindigen middels een schriftelijke kennisgeving aan SAP, waarbij een dergelijke kennisgeving uiterlijk dertig dagen na de datum waarop SAP de Klant over de nieuwe Subverwerker informeert dient plaats te vinden. Indien de Klant SAP niet binnen deze periode van dertig dagen van een beëindigingskennisgeving voorziet, wordt de Klant geacht de nieuwe Subverwerker te hebben geaccepteerd. De Klant mag binnen de periode van dertig dagen vanaf de datum waarop SAP de Klant over de nieuwe Subverwerker informeert verzoeken dat de partijen te goeder trouw bij elkaar komen om een oplossing voor het bezwaar te bespreken. Dergelijke besprekingen mogen niet voortduren tot na de periode waarin SAP van een beëindigingskennisgeving dient te worden voorzien en zijn niet van invloed op het recht van SAP om de nieuwe Subverwerker na de periode van dertig dagen te gebruiken.

(b) Professional Services: indien de Klant uit hoofde van de Privacywetgeving een legitieme reden heeft om bezwaar te maken tegen de verwerking van Persoonsgegevens door de nieuwe Subverwerker, mag de Klant tegen de inzet van deze Subverwerker door SAP bezwaar aantekenen door SAP binnen vijf werkdagen na de in Artikel 6.2 genoemde

verstrekking van informatie door SAP schriftelijk van een kennisgeving te voorzien. Indien de Klant bezwaar maakt tegen het gebruik van de Subverwerker, komen de partijen te goeder trouw bij elkaar om een oplossing te bespreken. SAP mag ervoor kiezen om (1) de Subverwerker niet te gebruiken, of (ii) de corrigerende maatregelen te nemen die de Klant in haar bezwaar noemt en de Subverwerker te gebruiken. Indien geen van deze opties redelijkerwijs mogelijk is en de Klant om legitieme redenen bezwaar blijft maken, mag elk der partijen de desbetreffende services beëindigen door hier vijf dagen van tevoren schriftelijk kennisgeving van te doen. Indien die klant niet binnen vijf dagen na ontvangst van de kennisgeving bezwaar maakt, wordt de Klant geacht de Subverwerker te hebben geaccepteerd. Indien er dertig dagen na indiening van het bezwaar geen oplossing voor het bezwaar van de Klant is gevonden en SAP geen beëindigingskennisgeving heeft ontvangen, wordt de Klant geacht de Subverwerker te hebben geaccepteerd.

(c) Elke beëindiging uit hoofde van dit Artikel 6.3 dient volgens elk der partijen vrij van fouten te zijn en valt onder de voorwaarden van de Overeenkomst.

6.4 Dringende vervanging. SAP mag een Subverwerker zonder voorafgaande kennisgeving vervangen indien de reden voor de vervanging redelijkerwijs buiten de macht van SAP ligt en een snelle vervanging om veiligheids- of andere dringende redenen vereist is. In dergelijke gevallen informeert SAP de Klant zo spoedig mogelijk na de aanstelling over de vervangende Subverwerker. Artikel 6.3 is daarbij van toepassing.

7. INTERNATIONALEVERWERKING

7.1 Voorwaarden voor internationale verwerking. SAP heeft het recht, onder andere middels Subverwerkers en voor zover dit door de Privacywetgeving wordt toegestaan, om Persoonsgegevens conform deze GVO te verwerken buiten het land waar de Klant gevestigd is.

7.2 Standaardcontractbepalingen. Indien (i) Persoonsgegevens van een Voor De Verwerking Verantwoordelijke die in de EER of in Zwitserland gevestigd is worden verwerkt buiten de EER, Zwitserland of een land, organisatie of gebied die of dat door de Europese Unie als veilig met een adequaat gegevensbeschermingsniveau wordt aangemerkt uit hoofde van Artikel 45 van de AVG, of indien (ii) Persoonsgegevens van een andere Voor De Verwerking Verantwoordelijke internationaal worden verwerkt en voor een dergelijke internationale verwerking toereikendheidsvoorzieningen worden vereist uit hoofde van de wetgeving van het land waarin de Voor De Verwerking Verantwoordelijke gevestigd is en aan dergelijke toereikendheidsvoorzieningen kan worden voldaan door Standaardcontractbepalingen aan te gaan, vindt het volgende plaats:

(a) SAP en de Klant gaan Standaardcontractbepalingen aan;

(b) De Klant gaat als volgt Standaardcontractbepalingen aan met elke relevante Subverwerker: ofwel (i) de Klant treedt als een onafhankelijke eigenaar van rechten en verplichtingen toe tot de Standaardcontractbepalingen die door SAP of SAP SE en de Subverwerker zijn aangegaan ("Toetredingsmodel") ofwel (ii) de (door SAP vertegenwoordigde) Subverwerker gaat Standaardcontractbepalingen aan met de Klant ("Volmachtmodel"); Het Volmachtmodel is uitsluitend van toepassing indien en voor zover SAP via de lijst met Subverwerkers die in Artikel 6.1(c) of (d) wordt genoemd of via een kennisgeving aan de Klant expliciet heeft bevestigd dat een Subverwerker hiervoor in aanmerking komt; en/of

(c) Andere Voor De Verwerking Verantwoordelijken die door de Klant zijn geautoriseerd om in het kader van de Overeenkomst Persoonsgegevens op te nemen mogen op dezelfde manier als de Klant Standaardcontractbepalingen aangaan met SAP en/of de desbetreffende Subverwerkers conform de Artikelen 7.2 (a) en (b) hierboven. In dergelijke gevallen gaat de Klant namens de andere Voor De Verwerking Verantwoordelijken Standaardcontractbepalingen aan.

7.3 Verhouding tussen de Standaardcontractbepalingen en de Overeenkomst. Niets in de Overeenkomst mag worden opgevat als prevalerend boven strijdige clausules in de Standaardcontractbepalingen. Voor alle duidelijkheid wordt hierbij gesteld dat waar in deze VGO audit- en subverwerkersregels verder worden bepaald in de artikelen 5 en 6, dergelijke bepalingen ook gelden voor de Standaardcontractbepalingen.

7.4 Toepasselijk recht voor de Standaardcontractbepalingen. De Standaardcontractbepalingen vallen onder de wetgeving van het land waar de desbetreffende Voor De Verwerking Verantwoordelijke gevestigd is.

8. DOCUMENTATIE; VERWERKINGSRECORDS

Elk der partijen is verantwoordelijk voor de eigen naleving van de eigen documentatievereisten en dit met name wat betreft het bijhouden van verwerkingsrecords waar dit door de Privacywetgeving wordt vereist. Elk der partijen dient de andere partij in redelijke mate te assisteren bij de naleving van de documentatievereisten, onder andere door de informatie die de andere partij nodig heeft op een redelijkerwijs door de andere partij gevraagde manier (bijvoorbeeld via een elektronisch systeem) te verstrekken, zodat de andere partij aan alle verplichtingen met betrekking tot het bijhouden van verwerkingsrecords kan voldoen.

9. DEFINITIES

Termen die met een hoofdletter beginnen en die niet in dit document worden gedefinieerd, hebben de betekenis die er in de Overeenkomst aan is gegeven.

9.1 "Geautoriseerde Gebruikers" verwijst naar elke persoon aan wie de Klant conform een SAP-softwarelicentie toegangsrechten voor het gebruik van de SAP-service toekent en die een werknemer, agent, aannemer of vertegenwoordiger is van (i) de Klant, (ii) aan de Klant Gelieerde Ondernemingen en/of (iii) Zakenpartners van de Klant of van aan de Klant Gelieerde Ondernemingen (zoals wordt gedefinieerd in de Softwarelicentie- en supportovereenkomst).

9.2 "Voor De Verwerking Verantwoordelijke" verwijst naar de natuurlijke of rechtspersoon, de overheidsinstantie, het bureau of een andere instelling die of dat alleen of gezamenlijk met andere instellingen de doelstellingen en middelen voor de verwerking van Persoonsgegevens bepaalt. Indien de Klant als Verwerker voor een andere Voor De Verwerking Verantwoordelijke optreedt, wordt er voor de doeleinden van deze GVO vanuit gegaan dat het in relatie tot SAP om een aanvullende en onafhankelijke Voor De Verwerking Verantwoordelijke gaat met de respectieve rechten en verplichtingen uit hoofde van deze GVO.

9.3 "Privacywetgeving" verwijst naar de toepasselijke wetgeving die de basisrechten en -vrijheden en het recht op privacy van personen beschermt met betrekking tot de verwerking van Persoonsgegevens in het kader van de Overeenkomst (en omvat, voor zover het om de relatie tussen de partijen inzake de verwerking van Persoonsgegevens door SAP namens de Klant gaat, de AVG als minimumnorm, ongeacht of de Persoonsgegevens onder de AVG vallen).

9.4 "Betrokkene" verwijst naar een geïdentificeerde of identificeerbare natuurlijke persoon volgens de definitie in de Privacywetgeving.

9.5 "Persoonsgegevens" verwijst naar alle informatie over een Betrokkene die uit hoofde van de Privacywetgeving wordt beschermd. Voor de doeleinden van de GVO gaat het hierbij uitsluitend om persoonsgegevens die aan SAP of haar Subverwerkers worden verstrekt of waartoe SAP of haar Subverwerkers toegang krijgen om uit hoofde van de Overeenkomst de SAP-service te leveren.

9.6 "Inbreuk op Persoonsgegevens" verwijst naar het bevestigd (1) onopzettelijk of onwettig vernietigen, verliezen, wijzigen of zonder toestemming openbaar maken van dan wel het zonder toestemming door derden toegang verkrijgen tot Persoonsgegevens of (2) een vergelijkbaar incident waarbij Persoonsgegevens betrokken zijn en dat een Voor De Verwerking Verantwoordelijke in beide gevallen volgens de Privacywetgeving moet melden bij bevoegde privacy-instanties of Betrokkenen.

9.7 **"Professional Services"** verwijst naar implementatieservices, adviesservices en/of services zoals SAP Premium Engagement Support Services, Innovative Business Solutions Development Services en Innovative Business Solutions Development Support Services.

9.8 **"Verwerker"** verwijst naar een natuurlijke of rechtspersoon overheidsinstantie, bureau of andere instelling die of dat namens de Voor De Verwerking Verantwoordelijke Persoonsgegevens verwerkt, ofwel direct als Verwerker van een Voor De Verwerking Verantwoordelijke ofwel indirect als Subverwerker van een Verwerker die Persoonsgegevens namens de Voor De Verwerking Verantwoordelijke verwerkt.

9.9 **"Standaardcontractbepalingen"**, ook wel "Modelcontractbepalingen" genoemd, verwijst naar de (Standaardcontractbepalingen (verwerkers)) of een eropvolgende versie hiervan die door de Europese Commissie worden gepubliceerd (en die automatisch van toepassing zijn).

9.10 **"Subverwerker"** verwijst naar aan SAP Gelieerde Ondernemingen, SAP SE, aan SAP SE Gelieerde Ondernemingen en derden die door SAP, SAP SE of aan SAP SE Gelieerde Ondernemingen ten behoeve van de SAP-service worden ingezet en die Persoonsgegevens verwerken conform deze GVO.

Bijlage 1 bij de GVO en, indien van toepassing, de Standaardcontractbepalingen

Gegevensexporteur
De Gegevensexporteur is een Klant die met SAP een Softwarelicentie- en -supportovereenkomst en/of een Serviceovereenkomst is aangegaan uit hoofde waarvan zij de ontvanger is van de SAP-service die in de desbetreffende Overeenkomst wordt beschreven. Indien de Gegevensexporteur andere Voor De Verwerking Verantwoordelijken toestaat de SAP-service te gebruiken, zijn deze andere Voor De Verwerking Verantwoordelijken ook Gegevensexporteur.

Gegevensimporteur
SAP en haar Subverwerkers leveren de SAP-service zoals deze in de desbetreffende door de Gegevensexporteur aangegane Overeenkomst wordt gedefinieerd en zoals deze de volgende SAP-service omvat:

- In het kader van de Softwarelicentie- en -supportovereenkomst: SAP en/of haar Subverwerkers leveren support wanneer een Klant een supportticket indient omdat de Software niet beschikbaar is of niet naar verwachting werkt. Ze beantwoorden telefoontjes, voeren basisprobleemoplossingen uit en verwerken supporttickets in een trackingsysteem.
- In het kader van de toepasselijke Serviceovereenkomst voor Professional Services: SAP en/of haar Subverwerkers leveren Services op basis van het Orderformulier en het relevante Scopedocument.

Betrokkenen
Tenzij anderszins bepaald door de Gegevensexporteur hebben overgedragen Persoonsgegevens betrekking op de volgende categorieën Betrokkenen: werknemers, aannemers, Zakenpartners of andere personen van wie Persoonsgegevens worden overgedragen of beschikbaar worden gesteld aan dan wel toegankelijk worden gemaakt voor de Gegevensimporteur.

Gegevenscategorieën
Het gaat bij de overgedragen Persoonsgegevens om de volgende gegevenscategorieën:

De Klant bepaalt de gegevens- en/of gegevensveldcategorieën die conform de relevante Overeenkomst via de SAP-service mogen worden overgedragen. Het gaat bij de overgedragen Persoonsgegevens gewoonlijk om de volgende gegevenscategorieën: naam, telefoonnummers, e-mailadres, tijdzone, adresgegevens, systeemtoegangs-/gebruiks-/autorisatiegegevens, bedrijfsnaam, contractgegevens, factuurgegevens en applicatiespecifieke gegevens die door Geautoriseerde Gebruikers worden overgedragen, waarbij het onder andere kan gaan om financiële gegevens zoals bankrekeninggegevens en creditcard-/betaalkaartgegevens.

Bijzondere gegevenscategorieën (indien van toepassing)
Het gaat bij de overgedragen Persoonsgegevens om de volgende bijzondere gegevenscategorieën: zie de eventuele specificatie in de Overeenkomst (inclusief het Orderformulier).

Verwerkingsactiviteiten/-doelen
De overgedragen Persoonsgegevens vallen onder de basisverwerkingsactiviteiten die in de Overeenkomst worden beschreven en waarbij het kan gaan om:

- Het gebruik van Persoonsgegevens voor de levering van de SAP-service
- De opslag van Persoonsgegevens
- De computerverwerking van Persoonsgegevens ten behoeve van gegevensverzending
- De uitvoering van instructies van de Klant conform de Overeenkomst.

Bijlage 2 bij de GVO en, indien van toepassing, de Standaardcontractbepalingen: technische en organisatorische maatregelen

1. TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

De volgende artikelen definiëren SAP's huidige technische en organisatorische maatregelen. SAP mag deze te allen tijde zonder kennisgeving wijzigen, mits er een vergelijkbaar of beter beveiligingsniveau in stand wordt gehouden. Afzonderlijke maatregelen mogen worden vervangen door nieuwe maatregelen die hetzelfde doel dienen zonder het beveiligingsniveau van de Persoonsgegevens te verlagen.

1.1 Fysieke toegangscontrole. Onbevoegde personen krijgen geen fysieke toegang tot terreinen, gebouwen of ruimten waar zich gegevensverwerkingssystemen bevinden die Persoonsgegevens verwerken en/of gebruiken.

Maatregelen:

- SAP beschermt haar voorzieningen en faciliteiten met behulp van passende maatregelen op basis van het SAP-beveiligingsbeleid.
- In het algemeen worden gebouwen beveiligd door middel van toegangscontrolesystemen (bijvoorbeeld toegangssystemen met smartcards).
- Als minimumvereiste geldt dat de buitenste toegangspunten van het gebouw dienen te zijn uitgerust met een gecertificeerd sleutelsysteem dat op een moderne, actieve manier wordt beheerd.
- Gebouwen, specifieke zones en omliggende terreinen kunnen afhankelijk van de beveiligingsclassificatie verder met aanvullende maatregelen worden beveiligd. Het gaat hierbij onder andere om specifieke toegangsprofielen, videobewaking, inbraakalarmsystemen en biometrische toegangscontrolesystemen.
- Toegangsrechten worden individueel en conform de maatregelen voor systeem- en gegevenstoegangscontrole (zie Artikel 1.2 en 1.3 hieronder) aan bevoegde personen toegekend. Dit geldt ook voor bezoekers. Gasten en bezoekers in SAP-gebouwen dienen hun naam te registreren bij de receptie en dienen te worden begeleid door bevoegd SAP-personeel.
- Werknemers van SAP en externe medewerkers dienen op alle SAP-locaties hun ID-kaart te dragen.

Aanvullende maatregelen voor Datacenters:

- Alle Datacenters houden zich aan strenge veiligheidsprocedures, inclusief bewakers, bewakingscamera's, bewegingsdetectoren, toegangscontrolemechanismen en andere maatregelen die tot doel hebben te voorkomen dat apparatuur en faciliteiten van deze Datacenters gecompromitteerd raken. Alleen bevoegde vertegenwoordigers krijgen toegang tot systemen en infrastructuur binnen de faciliteiten van een Datacenter. Fysieke beveiligingsvoorzieningen (bijvoorbeeld bewegingssensoren, camera's enz.) worden regelmatig onderhouden om een deugdelijke werking te waarborgen.
- SAP en alle externe aanbieders van Datacenters loggen de namen van bevoegde personeelsleden die de niet-publieke SAP-ruimten binnen de Datacenters bezoeken en de tijdstippen waarop dit gebeurt.

1.2 Systeemtoegangscontrole. Er dient te worden voorkomen dat gegevensverwerkingssystemen die voor de levering van de SAP-service worden gebruikt door onbevoegden worden gebruikt.

Maatregelen:

- Er worden meerdere autorisatieniveaus gebruikt bij het verschaffen van toegang tot gevoelige systemen, zoals die waarop Persoonsgegevens worden opgeslagen en verwerkt. Autorisaties worden via gedefinieerde processen en conform het SAP-beveiligingsbeleid beheerd.
- Alle medewerkers krijgen toegang tot de SAP-systemen met een unieke ID (gebruikers-ID).
- SAP hanteert procedures om ervoor te zorgen dat aangevraagde autorisatiewijzigingen uitsluitend conform het SAP-beveiligingsbeleid worden geïmplementeerd (er worden bijvoorbeeld geen

rechten verleend zonder autorisatie). Indien medewerkers het bedrijf verlaten, worden hun toegangsrechten ingetrokken.

- SAP heeft een wachtwoordbeleid vastgesteld dat het delen van wachtwoorden verbiedt, bepaalt wat er dient te gebeuren indien een wachtwoord wordt gedeeld en eist dat wachtwoorden regelmatig worden gewijzigd en standaardwachtwoorden worden vervangen. Er worden gepersonaliseerde gebruikers-ID's toegewezen voor verificatiedoeleinden. Alle wachtwoorden dienen aan de gedefinieerde minimumvereisten te voldoen en worden gecodeerd opgeslagen. In het geval van domeinwachtwoorden dwingt het systeem elke zes maanden een wachtwoordwijziging af die aan de vereisten voor complexe wachtwoorden voldoet. Elke computer heeft een screensaver met wachtwoordbeveiliging.
- Het bedrijfsnetwerk wordt door middel van firewalls afgeschermd van het publieke netwerk.
- SAP gebruikt bijgewerkte antivirussoftware op alle toegangspunten tot het bedrijfsnetwerk (voor e-mailaccounts) en op alle bestandsservers en alle werkstations.
- Er is beveiligingspatchbeheer geïmplementeerd om ervoor te zorgen dat relevante beveiligingsupdates regelmatig en periodiek worden doorgevoerd. Volledige externe toegang tot het bedrijfsnetwerk en de kritische infrastructuur van SAP wordt beveiligd met strenge verificatiemaatregelen.

1.3 Gegevenstoegangscontrole. Personen die geautoriseerd zijn om gegevensverwerkingssystemen te gebruiken, krijgen uitsluitend toegang tot de Persoonsgegevens waarvoor ze toegangsrechten hebben en Persoonsgegevens mogen tijdens verwerking, gebruik en opslag niet zonder autorisatie worden gelezen, gekopieerd, gewijzigd of verwijderd.

Maatregelen:

- Persoonsgegevens vergen in het kader van het SAP-beveiligingsbeleid minimaal hetzelfde beveiligingsniveau als "vertrouwelijke" informatie conform de SAP-informatieclassificatienorm.
- Toegang tot Persoonsgegevens wordt uitsluitend verleend voor zover dit strikt noodzakelijk is. Medewerkers krijgen toegang tot de informatie die ze nodig hebben om hun plichten te vervullen. SAP gebruikt autorisatieconcepten die toegangsverleningsprocessen en per account (gebruikers-ID) toegewezen rollen documenteren. Alle Klantgegevens worden beschermd conform het SAP-beveiligingsbeleid.
- Alle productieservers draaien in de Datacenters of in veilige serverruimten. Beveiligingsmaatregelen voor applicaties die Persoonsgegevens verwerken, worden regelmatig gecontroleerd. Hiertoe voert SAP interne en externe beveiligingscontroles en penetratietests uit op haar IT-systemen.
- SAP staat niet toe dat software wordt geïnstalleerd die niet door SAP is goedgekeurd.
- Een SAP-beveiligingsnorm bepaalt hoe gegevens en gegevensdragers worden verwijderd of vernietigd wanneer ze niet langer nodig zijn.

1.4 Gegevensverzendcontrole. Tenzij dit noodzakelijk is voor de levering van de SAP-services conform de relevante Overeenkomst, mogen Persoonsgegevens niet zonder toestemming worden gelezen, gekopieerd, gewijzigd of verwijderd tijdens de verzending. Indien gegevensdragers fysiek worden vervoerd, worden er bij SAP passende maatregelen genomen om de overeengekomen serviceniveaus (bijvoorbeeld codering, containers met loden binnenwerk, enz.) te waarborgen.

Maatregelen:

- Persoonsgegevens die via SAP's interne netwerken worden verzonden, worden conform het SAP-beveiligingsbeleid beschermd.
- Voor gevallen waarin gegevens worden verzonden tussen SAP en de Klant, worden de voor de gegevensverzending vereiste beschermingsmaatregelen hierbij tussen SAP en de Klant overeengekomen en opgenomen in de Overeenkomst. Dit geldt zowel voor de fysieke verzending

van gegevens als voor verzending via een netwerk. De Klant aanvaardt in alle gevallen de verantwoordelijkheid voor elke verzending van gegevens die buiten door SAP gecontroleerde systemen plaatsvindt (bijvoorbeeld in het geval van gegevens die buiten de firewall van het SAP Data Center worden verzonden).

1.5 Gegevensinvoercontrole. Het is mogelijk om met terugwerkende kracht te onderzoeken en vast te stellen of en door wie Persoonsgegevens zijn ingevoerd, gewijzigd of verwijderd in of uit gegevensverwerkingssystemen van SAP.

Maatregelen:

- SAP verleent geautoriseerde medewerkers uitsluitend toegang tot Persoonsgegevens voor zover dit nodig is voor hun werkzaamheden.
- SAP heeft voor zover dit technisch gezien mogelijk is een logsysteem ingevoerd voor de invoer, wijziging, verwijdering of blokkering van Persoonsgegevens binnen de SAP-service door SAP of haar Subverwerkers.

1.6 Taakcontrole. Taakcontrole is vereist om ervoor te zorgen dat persoonsgegevens die namens anderen worden verwerkt strikt volgens de instructies van de Klant worden verwerkt.

Maatregelen:

SAP gebruikt controlemechanismen en processen om de naleving van de contracten tussen SAP en haar klanten, subverwerkers en andere dienstverleners te bewaken.

Persoonsgegevens vergen in het kader van het SAP-beveiligingsbeleid minimaal hetzelfde beveiligingsniveau als "vertrouwelijke" informatie conform de SAP-informatieclassificatienorm.

- Alle medewerkers en contractuele subverwerkers of andere dienstverleners van SAP zijn contractueel verplicht om de vertrouwelijkheid van alle gevoelige informatie, inclusief bedrijfsgeheimen van SAP-klanten en -partners, te respecteren.

  In het geval van SAP Support hebben de klanten van SAP te allen tijde de controle over hun externe supportverbindingen. SAP-medewerkers kunnen zonder medeweten en toestemming van de klant geen toegang krijgen tot een klantsysteem. In het geval van SAP Support voorziet SAP in een speciaal aangewezen beveiligde supportticketvoorziening waarmee SAP een speciale bewaakte veilige zone met toegangscontrole aanbiedt voor de verzending van toegangsgegevens en wachtwoorden. De klanten van SAP hebben te allen tijde de controle over hun externe supportverbindingen. SAP-medewerkers kunnen zonder medeweten en actieve medewerking van de klant geen toegang krijgen tot een on-premise klantsysteem.

1.7 Beschikbaarheidsbewaking. Persoonsgegevens worden beschermd tegen onbedoeld(e) of ongeautoriseerd(e) vernietiging en verlies.

Maatregelen:

- SAP hanteert processen voor periodieke back-up waarmee bedrijfskritische systemen kunnen worden hersteld zoals en wanneer dit noodzakelijk is.
- SAP gebruikt ononderbroken voedingen (bijvoorbeeld UPS, accu's, generatoren, enz.) om ervoor te zorgen dat er altijd stroom beschikbaar is voor de Datacenters.
- SAP heeft bedrijfscontinuïteitsplannen gedefinieerd voor bedrijfskritische processen.
- Noodprocessen en -systemen worden regelmatig getest.

1.8 Gegevensscheidingscontrole. Persoonsgegevens die voor verschillende doeleinden worden verzameld, kunnen gescheiden worden verwerkt.

Maatregelen:

- SAP gebruikt passende technische controlemechanismen om te allen tijde voor scheiding van Klantgegevens te zorgen.
- De Klant (inclusief haar goedgekeurde Voor De Verwerking Verantwoordelijken) heeft middels veilige verificatie en autorisatie altijd uitsluitend toegang tot de eigen Gegevens.

- Indien Persoonsgegevens vereist zijn om een supportincident van de Klant te kunnen verwerken, worden de gegevens aan dit specifieke bericht toegewezen en uitsluitend gebruikt om dit bericht te verwerken. Er wordt geen toegang tot de gegevens verkregen om andere berichten te verwerken. Deze gegevens worden opgeslagen in speciaal hiervoor bestemde supportsystemen.

1.9 Gegevensintegriteitscontrole. Persoonsgegevens blijven intact, volledig en actueel tijdens de verwerkingsactiviteiten.

Maatregelen:

SAP heeft een meerlaagse beschermingsstrategie doorgevoerd om wijzigingen door onbevoegden te voorkomen.

SAP gebruikt met name de volgende zaken om de hierboven genoemde controlemechanismen en maatregelen door te voeren. Voorzieningen:

- Firewalls
- Bewakingscentrum
- Antivirussoftware
- Back-up en herstel
- Externe en interne penetratietests
- Geregelde externe audits ter controle van de beveiligingsmaatregelen

Bijlage 3 bij de GVO

In de volgende tabel worden, uitsluitend ter illustratie, de relevante Artikelen van de AVG en de corresponderende bepalingen van de GVO opgesomd.

Artikel van AVG	Artikel van GVO	Klik op een link om het Artikel te bekijken
28(1)	2 en Bijlage 2	Veiligheid van de verwerking en Bijlage 2, Technische en organisatorische maatregelen.
28(2), 28(3) (d) en 28 (4)	6	SUBVERWERKERS
28 (3) zin 1	1.1. en Bijlage 1, 1.2	Doel en toepassing, Bijlage 1 Structuur.
28(3) (a) en 29	3.1 en 3.2	Instructies van de Klant. Verwerking op grond van een wettelijk vereiste.
28(3) (b)	3.3	Personeel.
28(3) (c) en 32	2 en Bijlage 2	Veiligheid van de verwerking en Bijlage 2, Technische en organisatorische maatregelen.
28(3) (e)	3.4	Samenwerking.
28(3) (f) en 32-36	2 en Bijlage 2, 3.5, 3.6	Veiligheid van de verwerking en Bijlage 2, Technische en organisatorische maatregelen. Kennisgeving inzake Inbreuk op Persoonsgegevens. Effectanalyse gegevensbeveiliging. Indien de Klant (of haar Voor De Verwerking Verantwoordelijken) krachtens de Privacywetgeving een effectanalyse voor de gegevensbeveiliging moet (moeten) uitvoeren of van tevoren met een toezichthouder moet (moeten) overleggen, zal SAP op verzoek van de Klant de documenten verstrekken die in algemene zin voor de SAP-service beschikbaar zijn (bijvoorbeeld deze GVO, de Overeenkomst, auditrapporten en certificeringen). Eventuele verdere assistentie dient door de Partijen onderling te worden overeengekomen.
28(3) (g)	4	Gegevensverwijdering
28(3) (h)	5	CERTIFICERINGEN EN AUDITS
28 (4)	6	SUBVERWERKERS
30	8	Documentatie; verwerkingsrecords
46(2) (c)	7.2	Standaardcontractbepalingen. Indien (i) Persoonsgegevens van een Voor De Verwerking Verantwoordelijke die in de EER of in Zwitserland gevestigd is worden verwerkt buiten de EER, Zwitserland of een land, organisatie of gebied die of dat door de Europese Unie als veilig met een adequaat gegevensbeschermingsniveau wordt aangemerkt uit hoofde van Artikel 45 van de AVG, of indien (ii) Persoonsgegevens van een andere Voor De Verwerking Verantwoordelijke internationaal worden verwerkt en voor een dergelijke internationale verwerking

		toereikendheidsvoorzieningen worden vereist uit hoofde van de wetgeving van het land waarin de Voor De Verwerking Verantwoordelijke gevestigd is en aan dergelijke toereikendheidsvoorzieningen kan worden voldaan door Standaardcontractbepalingen aan te gaan, vindt het volgende plaats:

Bijlage 4
STANDAARDCONTRACTBEPALINGEN (VERWERKERS)[1]

Bijlage 4
STANDAARDCONTRACTBEPALINGEN (VERWERKERS)[2]

De Standaardcontractbepalingen waarnaar in deze GVO wordt verwezen, zijn beschikbaar via de volgende link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087.

Bijlage 4
STANDAARDCONTRACTBEPALINGEN (VERWERKERS)[3]

Voor de toepassing van artikel 26, lid 2, van Richtlijn 95/46/EG (of, na 25 mei 2018, artikel 44 en volgende van Verordening 2016/79), voor de doorgifte van persoonsgegevens aan verwerkers die gevestigd zijn in derde landen die geen passend beschermingsniveau waarborgen

Klant, ook namens andere Voor De Verwerking Verantwoordelijken
(in de Bepalingen hierna de **'gegevensexporteur'**)

en

SAP
(in de Bepalingen hierna de **'gegevensimporteur'**)

elk afzonderlijk 'partij' en gezamenlijk 'de partijen' genoemd,

ZIJN OVEREENGEKOMEN de volgende contractbepalingen, hierna 'de bepalingen' genoemd, vast te stellen teneinde voldoende waarborgen te bieden ten aanzien van de bescherming van de persoonlijke levenssfeer en de fundamentele rechten en vrijheden van personen, bij de doorgifte van de in aanhangsel 1 vermelde persoonsgegevens door de gegevensexporteur aan de gegevensimporteur.

Bepaling 1
Definities

Voor de toepassing van de bepalingen:

(a) gelden voor 'persoonsgegevens', 'bijzondere categorieën gegevens', 'verwerken/verwerking', 'voor de verwerking verantwoordelijke', 'verwerker', 'betrokkene' en 'toezichthoudende autoriteit' dezelfde definities als in Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke

[1] Uit hoofde van het Besluit van 5 februari 2010 van de Europese Commissie (2010/87/EU)

[2] Uit hoofde van het Besluit van 5 februari 2010 van de Europese Commissie (2010/87/EU)

[3] Uit hoofde van het Besluit van 5 februari 2010 van de Europese Commissie (2010/87/EU)

personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens;

(b) wordt onder 'gegevensexporteur' verstaan: de voor de verwerking verantwoordelijke die de persoonsgegevens doorgeeft;

(c) wordt onder 'gegevensimporteur' verstaan: de verwerker die overeenkomt van de gegevensexporteur persoonsgegevens te ontvangen om deze na doorgifte namens de gegevensexporteur te verwerken in overeenstemming met zijn instructies en de voorwaarden van de bepalingen, en die niet onderworpen is aan een regeling van een derde land die passende bescherming biedt in de zin van artikel 25, lid 1, van Richtlijn 95/46/EG;

(d) wordt onder 'subverwerker' verstaan: een verwerker die door de gegevensimporteur of een andere voor de gegevensimporteur werkende subverwerker is gecontracteerd en die overeenkomt van de gegevensimporteur of van een andere voor de gegevensimporteur werkende subverwerker persoonsgegevens te ontvangen, uitsluitend ten behoeve van de verwerkingsactiviteiten die namens de gegevensexporteur worden verricht na de doorgifte, overeenkomstig de instructies van de gegevensexporteur, de voorwaarden van de bepalingen en de voorwaarden van het schriftelijke contract inzake subverwerking;

(e) wordt onder 'toepasselijk recht inzake gegevensbescherming' verstaan: de wettelijke bepalingen ter bescherming van de fundamentele rechten en vrijheden van personen, en met name hun recht op bescherming van de persoonlijke levenssfeer in verband met de verwerking van persoonsgegevens, die in de lidstaat van vestiging van de gegevensexporteur van toepassing zijn op een voor de verwerking verantwoordelijke;

(f) wordt onder 'technische en organisatorische beveiligingsmaatregelen' verstaan: maatregelen die tot doel hebben persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking de doorzending van gegevens in een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking.

Bepaling 2
Bijzonderheden betreffende de doorgifte

De bijzonderheden betreffende de doorgifte, met name, in voorkomend geval, de bijzondere categorieën persoonsgegevens, worden nader omschreven in aanhangsel 1, dat een integrerend deel van de bepalingen vormt.

Bepaling 3
Derdenbeding

1. De betrokkenen kunnen deze bepaling en bepaling 4, onder b) tot en met i), bepaling 5, onder a) tot en met e) en g) tot en met j), bepaling 6, leden 1 en 2, bepaling 7, bepaling 8, lid 2, en de bepalingen 9 tot en met 12 als derde begunstigden tegenover de gegevensexporteur afdwingen.

2. De betrokkenen kunnen deze bepaling, bepaling 5, onder a) tot en met e) en onder g), bepaling 6, bepaling 7, bepaling 8, lid 2, en de bepalingen 9 tot en met 12 tegenover de gegevensimporteur afdwingen in gevallen waarin de gegevensexporteur feitelijk is verdwenen of heeft opgehouden rechtens te bestaan, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur heeft overgenomen en daardoor de

rechten en verplichtingen van de gegevensexporteur op zich neemt; in dit geval kunnen betrokkenen de genoemde bepalingen tegenover deze rechtsopvolger afdwingen.

3. De betrokkenen kunnen deze bepaling, bepaling 5, onder a) tot en met e) en onder g), bepaling 6, bepaling 7, bepaling 8, lid 2, en de bepalingen 9 tot en met 12 tegenover de subverwerker afdwingen in die gevallen waarin zowel de gegevensexporteur als de gegevensimporteur feitelijk is verdwenen, heeft opgehouden rechtens te bestaan of insolvent is geworden, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur heeft overgenomen en daardoor de rechten en verplichtingen van de gegevensexporteur op zich neemt; in dat geval kunnen betrokkenen de genoemde bepalingen tegenover deze rechtsopvolger afdwingen. Deze aansprakelijkheid van de subverwerker jegens derden blijft beperkt tot de verwerkingswerkzaamheden die deze zelf heeft uitgevoerd krachtens de bepalingen.

4. De partijen verzetten zich er niet tegen dat de betrokkenen door een vereniging of andere instelling worden vertegenwoordigd, indien de betrokkenen dit uitdrukkelijk wensen en dit in het nationale recht is toegestaan.

Bepaling 4

Verplichtingen van de gegevensexporteur

De gegevensexporteur stemt ermee in en garandeert dat:

(a) de verwerking van de persoonsgegevens, met inbegrip van de doorgifte zelf, is geschied en zal blijven geschieden in overeenstemming met alle relevante bepalingen van het toepasselijke recht inzake gegevensbescherming (en, waar van toepassing, is gemeld aan de betrokken autoriteiten van de lidstaat waar de gegevensexporteur is gevestigd), en dat zij niet in strijd is met de toepasselijke bepalingen van die staat;

(b) hij de gegevensimporteur instructie heeft gegeven, en gedurende de verwerking van de persoonsgegevens zal geven, de persoonsgegevens uitsluitend namens de gegevensexporteur en in overeenstemming met het toepasselijke recht inzake gegevensbescherming en de bepalingen te verwerken;

(c) de gegevensimporteur voldoende waarborgen zal bieden ten aanzien van de technische en organisatorische beveiligingsmaatregelen die in aanhangsel 2 bij dit contract worden omschreven;

(d) deze beveiligingsmaatregelen, na een beoordeling van de vereisten van het toepasselijke recht inzake gegevensbescherming, geschikt zijn bevonden om persoonsgegevens te beschermen tegen vernietiging, hetzij bij ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking doorzending van gegevens via een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking, en deze maatregelen gezien de aan de verwerking en de aard van de te beschermen gegevens verbonden risico's een passend beveiligingsniveau waarborgen, gelet op de stand van de techniek en de kosten van de tenuitvoerlegging;

(e) hij op de naleving van deze beveiligingsmaatregelen zal toezien;

(f) wanneer de doorgifte bijzondere categorieën gegevens betreft, de betrokkene ervan in kennis is gesteld, of vóór of zo spoedig mogelijk na de doorgifte ervan in kennis zal worden

gesteld, dat zijn gegevens kunnen worden doorgegeven naar een derde land dat geen passende bescherming biedt als bedoeld in Richtlijn 95/46/EG;

(g) hij overeenkomstig bepaling 5, onder b), en bepaling 8, lid 3, ontvangen kennisgevingen van de gegevensimporteur of een subverwerker aan de toezichthoudende autoriteit zal doorzenden, wanneer hij (dat wil zeggen de gegevensexporteur) besluit de doorgifte voort te zetten of de opschorting op te heffen;

(h) hij op verzoek een afschrift van de bepalingen ter beschikking van de betrokkene zal stellen, met uitzondering van aanhangsel 2, alsmede een beknopte beschrijving van de beveiligingsmaatregelen en een afschrift van elk contract voor subverwerkingsdiensten dat overeenkomstig de bepalingen dient te worden opgesteld; indien de bepalingen of het contract commerciële informatie bevatten, mag de gegevensexporteur deze commerciële informatie verwijderen;

(i) in geval van subverwerking de verwerkingsactiviteiten worden uitgevoerd overeenkomstig bepaling 11 door een subverwerker die ten minste hetzelfde beschermingsniveau voor de persoonsgegevens en de rechten van de betrokkenen waarborgt als de gegevensimporteur overeenkomstig deze bepalingen; en

(j) hij zal toezien op de naleving van bepaling 4, onder a) tot en met i).

Bepaling 5

Verplichtingen van de gegevensimporteur

De gegevensimporteur stemt ermee in en garandeert dat:

(a) hij de persoonsgegevens uitsluitend namens de gegevensexporteur en in overeenstemming met diens instructies en met de bepalingen verwerkt; indien hij om welke reden dan ook daartoe niet in staat is, stemt hij ermee in de gegevensexporteur onverwijld daarvan in kennis te stellen, in welk geval de gegevensexporteur de gegevensdoorgifte mag opschorten en/of het contract mag beëindigen;

(b) hij geen reden heeft aan te nemen dat de op hem toepasselijke wetgeving hem belet de van de gegevensexporteur ontvangen instructies en zijn verplichtingen krachtens het contract na te komen, en dat hij in geval van een wijziging in deze wetgeving die in aanzienlijke mate afbreuk dreigt te doen aan de in de bepalingen opgenomen waarborgen en verplichtingen, de gegevensexporteur, zodra hij de wijziging kent, onverwijld daarvan in kennis stelt, in welk geval de gegevensexporteur de gegevensdoorgifte mag opschorten en/of het contract mag beëindigen;

(c) hij de in aanhangsel 2 omschreven technische en organisatorische beveiligingsmaatregelen vóór de verwerking van de doorgegeven persoonsgegevens heeft getroffen;

(d) hij de gegevensexporteur onverwijld ervan in kennis stelt wanneer:

(i) een wetshandhavingsinstantie een juridisch bindend verzoek om verstrekking van persoonsgegevens heeft gedaan, tenzij deze kennisgeving anderszins is verboden, zoals een strafrechtelijk verbod dat ten doel heeft de vertrouwelijkheid van een wetshandhavingsonderzoek te bewaren;

(ii) iemand per ongeluk of op ongeoorloofde wijze toegang tot de gegevens heeft gehad;

(iii) hij van de betrokkenen rechtstreeks een verzoek heeft ontvangen, waarop hij niet ingaat, tenzij hem dit anderszins is toegestaan;

(e) hij alle vragen van de gegevensexporteur betreffende de door hem uitgevoerde verwerking van de doorgegeven persoonsgegevens zo spoedig mogelijk naar behoren beantwoordt en het advies van de toezichthoudende autoriteit volgt bij de verwerking van de doorgegeven gegevens;

(f) hij op verzoek van de gegevensexporteur zijn verwerkingsvoorzieningen beschikbaar stelt voor controle van de onder deze bepalingen vallende verwerkingsactiviteiten, welke wordt uitgevoerd door de gegevensexporteur of door een controleorgaan waarvan de leden onafhankelijk zijn, over de vereiste beroepskwalificaties beschikken, tot geheimhouding verplicht zijn en door de gegevensexporteur worden aangewezen, waar van toepassing in overleg met de toezichthoudende autoriteit;

(g) hij, wanneer de betrokkene geen afschrift van de gegevensexporteur kan verkrijgen, hem op verzoek een afschrift van de bepalingen alsmede eventuele subverwerkingscontracten ter beschikking stelt, met uitzondering van aanhangsel 2 dat door een beknopte beschrijving van de beveiligingsmaatregelen wordt vervangen; indien de bepalingen of contracten commerciële informatie bevatten, mag de gegevensimporteur deze commerciële informatie verwijderen;

(h) hij, wanneer subverwerking plaatsvindt, de gegevensexporteur tevoren heeft ingelicht en diens schriftelijke toestemming heeft verkregen;

(i) de verwerkingsdiensten van de subverwerker overeenkomstig bepaling 11 zullen worden uitgevoerd;

(j) hij van elk subverwerkingscontract dat hij in het kader van de bepalingen aangaat, onverwijld een afschrift doet toekomen aan de gegevensexporteur.

Bepaling 6

Aansprakelijkheid

1. De partijen komen overeen dat elke betrokkene die ten gevolge van een schending van de verplichtingen bedoeld in bepaling 3 of bepaling 11 door een partij of een subverwerker schade heeft geleden, het recht heeft van de gegevensexporteur vergoeding voor de geleden schade te ontvangen.

2. Wanneer de betrokkene geen vordering tot schadevergoeding wegens niet-nakoming door de gegevensimporteur of diens subverwerker van een van de in bepaling 3 of bepaling 11 bedoelde verplichtingen, als bedoeld in lid 1, tegen de gegevensexporteur kan instellen doordat de gegevensexporteur feitelijk is verdwenen, heeft opgehouden rechtens te bestaan of insolvent is geworden, stemt de gegevensimporteur ermee in dat de betrokkene een vordering kan instellen tegen de gegevensimporteur alsof hij de gegevensexporteur was, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur heeft overgenomen, in welk geval de betrokkene zijn rechten tegenover die rechtsopvolger kan doen gelden.

De gegevensimporteur kan zich niet aan zijn aansprakelijkheid onttrekken door zich te beroepen op niet-nakoming van verplichtingen door de subverwerker.

3. Wanneer de betrokkene de in lid 1 of 2 bedoelde vordering wegens niet-nakoming door de subverwerker van een van de in bepaling 3 of bepaling 11 bedoelde verplichtingen niet tegen de gegevensexporteur of de gegevensimporteur kan instellen doordat zowel de gegevensexporteur als de gegevensimporteur feitelijk is verdwenen, heeft opgehouden rechtens te bestaan of insolvent is geworden, stemt de subverwerker ermee in dat de betrokkene een vordering kan instellen tegen de subverwerker, met betrekking tot diens eigen verwerkingsactiviteiten krachtens de bepalingen, alsof deze de gegevensexporteur of de gegevensimporteur was, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur of de gegevensimporteur heeft overgenomen, in welk geval de betrokkene zijn rechten tegenover die rechtsopvolger kan doen gelden. De aansprakelijkheid van de subverwerker blijft beperkt tot de verwerkingsactiviteiten die deze zelf heeft uitgevoerd krachtens de bepalingen.

Bepaling 7

Bemiddeling en rechtsmacht

1. De gegevensimporteur stemt ermee in dat, indien de betrokkene tegen hem rechten ten behoeve van derden en/of vorderingen tot schadevergoeding krachtens de bepalingen inroept, de gegevensimporteur de beslissing van de betrokkene aanvaardt:

(a) om het geschil te onderwerpen aan bemiddeling door een onafhankelijke persoon of, waar van toepassing, door de toezichthoudende autoriteit;

(b) om het geschil voor te leggen aan een rechterlijke instantie in de lidstaat waar de gegevensexporteur is gevestigd.

2. De partijen komen overeen dat de door de betrokkene gemaakte keuze geen afbreuk doet aan diens materiële of formele rechten om op grond van andere bepalingen van nationaal of internationaal recht verhaal te zoeken.

Bepaling 8

Samenwerking met de toezichthoudende autoriteiten

1. De gegevensexporteur stemt ermee in een afschrift van dit contract bij de toezichthoudende autoriteit neer te leggen, indien deze daarom verzoekt of indien dit krachtens het toepasselijke recht inzake gegevensbescherming vereist is.

2. De partijen komen overeen dat de toezichthoudende autoriteit bevoegd is bij de gegevensimporteur en eventuele subverwerkers een controle te verrichten die dezelfde reikwijdte heeft en aan dezelfde voorwaarden is onderworpen als die welke krachtens het toepasselijke recht inzake gegevensbescherming voor haar controle van de gegevensexporteur zouden gelden.

3. Indien er wetgeving bestaat die op de gegevensimporteur of een subverwerker van toepassing is en die de uitvoering van controles als in lid 2 bedoeld op de gegevensimporteur of een subverwerker verbiedt, stelt de gegevensimporteur de gegevensexporteur daarvan onverwijld in kennis. In een dergelijk geval mag de gegevensexporteur de in bepaling 5, onder b), bedoelde maatregelen nemen.

Bepaling 9

Toepasselijk recht

Op de bepalingen is het recht van de lidstaat van vestiging van de gegevensexporteur van toepassing.

Bepaling 10

Wijziging van het contract

De partijen verbinden zich ertoe de bepalingen niet te wijzigen. Dit vormt voor de partijen geen beletsel om indien nodig bepalingen toe te voegen betreffende met de transactie verband houdende vraagstukken, mits deze niet met de modelcontractbepalingen in strijd zijn.

Bepaling 11

Subverwerking

1. De gegevensimporteur besteedt de verwerkingsactiviteiten die hij overeenkomstig de bepalingen namens de gegevensexporteur uitvoert, niet uit zonder de voorafgaande schriftelijke toestemming van de gegevensexporteur. Indien de gegevensimporteur met toestemming van de gegevensexporteur zijn verplichtingen uit hoofde van de bepalingen uitbesteedt, dient hij met de subverwerker een schriftelijk contract te sluiten waarbij aan de subverwerker dezelfde verplichtingen worden opgelegd als die waaraan de gegevensimporteur uit hoofde van de bepalingen moet voldoen. Indien de subverwerker niet voldoet aan zijn verplichtingen tot gegevensbescherming uit hoofde van dat schriftelijke contract, blijft de gegevensimporteur jegens de gegevensexporteur volledig aansprakelijk voor de uitvoering van de verplichtingen van de subverwerker uit hoofde van dat contract.

2. In het tevoren tussen de gegevensimporteur en de subverwerker te sluiten schriftelijke contract dient tevens een derdenbeding te zijn opgenomen zoals vervat in bepaling 3, dat voorziet in gevallen dat de betrokkene geen vordering tot schadevergoeding als bedoeld in bepaling 6, lid 1, kan instellen tegen de gegevensexporteur of de gegevensimporteur omdat deze feitelijk zijn verdwenen, hebben opgehouden rechtens te bestaan of insolvent zijn geworden, en er geen rechtsopvolger is die contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur of de gegevensimporteur heeft overgenomen. Deze aansprakelijkheid van de subverwerker jegens derden blijft beperkt tot de verwerkingswerkzaamheden die deze zelf heeft uitgevoerd krachtens de bepalingen.

3. Op de in lid 1 bedoelde bepalingen betreffende de gegevensbeschermingsaspecten van de subverwerking uit hoofde van het in lid 1 bedoelde contract is het recht van de lidstaat van vestiging van de gegevensexporteur van toepassing.

4. De gegevensexporteur houdt een lijst bij van subverwerkingscontracten die krachtens de bepalingen zijn gesloten en door de gegevensimporteur overeenkomstig bepaling 5, onder j), zijn aangemeld, en werkt deze ten minste eenmaal per jaar bij. Deze lijst wordt ter beschikking gesteld van de toezichthoudende autoriteit voor gegevensbescherming die op de gegevensexporteur toezicht houdt.

Bepaling 12

Verplichting na de beëindiging van de verwerking van persoonsgegevens

1. De partijen komen overeen dat de gegevensimporteur en de subverwerker na het beëindigen van de verlening van de gegevensverwerkingsdiensten alle doorgegeven persoonsgegevens en kopieën daarvan aan de gegevensexporteur terugbezorgen of, indien de gegevensexporteur dat verkiest, alle persoonsgegevens vernietigen en aan de gegevensexporteur verklaren dat de vernietiging heeft plaatsgevonden, tenzij de op de gegevensimporteur toepasselijke wetgeving hem verbiedt alle of een gedeelte van de doorgegeven persoonsgegevens terug te bezorgen of te vernietigen. In dat geval garandeert de gegevensimporteur dat hij de vertrouwelijkheid van de doorgegeven persoonsgegevens zal respecteren en dat hij de doorgegeven gegevens niet verder actief zal verwerken.

2. De gegevensimporteur en de subverwerker garanderen dat zij op verzoek van de gegevensexporteur en/of de toezichthoudende autoriteit hun verwerkingsvoorzieningen voor een controle van de in lid 1 bedoelde maatregelen beschikbaar zullen stellen.