GEGEVENSVERWERKINGSOVEREENKOMST

Deze Gegevensverwerkingsovereenkomst (de 'Overeenkomst') wordt gesloten tussen Siemens Product Lifecycle Management Software Inc., ook bekend als Siemens Industry Software (hierna in dit document 'SISW' genoemd) en de klant die heeft aangegeven de voorwaarden van deze Overeenkomst te accepteren ('Klant'). SISW behoudt zich het recht voor om haar gelieerde bedrijven te gebruiken voor het verkrijgen van haar rechten en het vervullen van haar verplichtingen onder deze Overeenkomst. Daarom kan de hier gebruikte term 'SISW' ook verwijzen naar gelieerde bedrijven die direct of indirect het eigendom zijn of onder controle staan van het uiteindelijke moederbedrijf van Siemens Product Lifecycle Management Software Inc. en die door Siemens Product Lifecycle Management Software Inc. geautoriseerd zijn om SISW clouddiensten (de 'Cloud Service') te distribueren.

De Klant is als enige verantwoordelijk voor het bepalen van het type gegevens en de personen die betrokken zijn bij de verwerking en zal ervoor zorgen dat de verwerking via de Cloud Service legitiem is. De Klant is ook verantwoordelijk voor eventuele correctie, verwijdering of blokkering van persoonsgegevens met behulp van de functionaliteiten van de Cloud Service. De Klant mag zijn gegevens, inclusief persoonsgegevens, exporteren en verwijderen met behulp van de functionaliteiten van de Cloud Service. Na beëindiging van deze Gegevensverwerkingsovereenkomst heeft de Klant 30 dagen om een schriftelijk verzoek in te dienen bij SISW om de Klantgegevens beschikbaar te stellen aan de Klant om deze te downloaden. Na afloop van de periode die door SISW in antwoord op een dergelijk verzoek is ingesteld, worden eventuele achtergebleven gegevens van de Klant verwijderd en zijn deze niet langer beschikbaar voor de Klant. SISW en de Klant komen overeen dat, binnen het kader van de Cloud Service, het recht van de Klant om instructies uit te vaardigen uitsluitend wordt uitgeoefend middels de functionaliteiten van de Cloud Service. Voor aanvullende instructies met betrekking tot de gegevens van de Klant is een afzonderlijke schriftelijke overeenkomst tussen SISW en de Klant vereist, inclusief overeenstemming over eventuele extra vergoedingen die de Klant moet betalen voor het uitvoeren van dergelijke instructies. De Klant verbindt zich ertoe om geen beschermde gezondheidsinformatie (PHI) te uploaden of te bewaren in de Cloud Service, tenzij SISW en de Klant een afzonderlijke schriftelijke overeenkomst hebben gesloten waarin het opslaan van PHI in de Cloud Service expliciet wordt toegestaan.

Bij het leveren van de Cloud Service zal SISW zich, met betrekking tot het productiesysteem, houden aan de technische en organisatorische maatregelen die worden beschreven in Appendix 2 bij Exhibit A van deze Gegevensverwerkingsovereenkomst. Niet-productieystemen die gerelateerd zijn aan de Cloud Service kunnen al of niet voldoen aan de in Appendix 2 bij Exhibit A beschreven maatregelen. Bovendien kan SISW technische en organisatorische maatregelen die betrekking hebben op het productiesysteem periodiek wijzigen, op voorwaarde dat dergelijke wijzigingen geen nadelige gevolgen hebben voor het beschermingsniveau dat dergelijke maatregelen daadwerkelijk bieden. SISW zal verhinderen dat zijn medewerkers zonder toelating persoonsgegevens kunnen verzamelen, verwerken of gebruiken en zal alleen werknemers inzetten voor de verwerking van persoonsgegevens van de Klant die specifiek geïnformeerd zijn over het voldoen aan de vereisten voor het beschermen van de privacy van persoonsgegevens.

SISW heeft het recht om onderaannemers in te schakelen bij het uitvoeren van de Cloud Service. In zoverre toegang van onderaannemers tot persoonsgegevens van de Klant niet kan worden uitgesloten, zal SISW de Klant op diens verzoek een lijst verstrekken van de desbetreffende onderaannemers en hun respectievelijke locaties en zal SISW deze lijst indien nodig bijwerken voordat een nieuwe onderaannemer toegang krijgt tot de persoonsgegevens van de Klant. Indien de Klant redelijke bezwaren heeft tegen een nieuwe onderaannemer, zal de Klant SISW op de hoogte stellen van dit bezwaar en indien SISW vasthoudt aan het inschakelen van de nieuwe onderaannemer is de Klant gerechtigd om de Gegevensverwerkingsovereenkomst te beëindigen. Indien de inschakeling van een onderaannemer grensoverschrijdend verkeer van persoonsgegevens tot gevolg heeft, zal SISW zich inzetten om te zorgen dat de onderaannemer een gepast niveau van gegevensbescherming hanteert voor de persoonsgegevens.

SISW zal regelmatig controleren of de van toepassing zijnde technische en organisatorische maatregelen nageleefd worden en zal, na redelijk verzoek van de Klant, bevestigen dat men zich houdt aan de van toepassing zijnde technische en organisatorische maatregelen. Indien de Klant redenen heeft om aan te nemen dat een bevestiging door SISW onjuist is, heeft de Klant het recht om bevestigd te zien dat de technische en organisatorische maatregelen worden nageleefd door, na redelijke voorafgaande kennisgeving, een audit bij SISW te plannen. Een dergelijke audit wordt uitgevoerd op kosten van de Klant.

SISW en de Klant komen overeen dat elke overdracht van persoonsgegevens van de Klant vanuit landen in de Europese Unie naar landen buiten de EU waarvan de EU meent dat de persoonsgegevens niet voldoende worden beschermd, zullen worden uitgevoerd conform de voorzieningen van de EU modelcontractbepalingen die zijn vastgelegd in Exhibit A en die hiervan volledig deel uitmaken. In geval van een conflict tussen de voorwaarden van deze Gegevensverwerkingsovereenkomst en de

voorwaarden van de modelcontractbepalingen, hebben de voorzieningen in de modelcontractbepalingen voorrang. De modelcontractbepalingen vallen onder de wetten van de EU-lidstaat waarin de gegevensexporteur (zoals gedefinieerd in Exhibit A) gevestigd is.

Exhibit A
EU modelcontractbepalingen

Ten behoeve van Artikel 26(2) van Richtlijn 95/46/EC voor de overdracht van persoonsgegevens aan verwerkers die gevestigd zijn in derde landen die geen toereikende mate van gegevensbescherming waarborgen

door en tussen

Klant en/of een gerelateerd bedrijf van Klant dat gevestigd is in de EU

(hierna de '**gegevensexporteur**' genoemd)

en

Siemens Product Lifecycle Management Software Inc., ook bekend als Siemens Industry Software, inclusief alle gerelateerde bedrijven die direct of indirect het eigendom zijn van of onder controle staan van het uiteindelijke moederbedrijf Siemens Product Lifecycle Management Software Inc. en die door Siemens Product Lifecycle Management Software Inc. zijn geautoriseerd om namens hen gegevens te verwerken

(hierna de '**gegevensimporteur**' genoemd)

elk een 'partij'; samen 'de partijen',

HEBBEN OVEREENSTEMMING BEREIKT over de volgende Contractuele bepalingen (de Bepalingen) teneinde voldoende waarborgen te creëren met betrekking tot de bescherming van de privacy en fundamentele rechten en vrijheden van individuele personen voor de overdracht door de gegevensexporteur aan de gegevensimporteur van de in Appendix 1 gespecificeerde persoonsgegevens.

Artikel 1. Definities

In het kader van de Bepalingen:

(a) zullen 'persoonsgegevens', 'bijzondere categorieën gegevens', 'proces/verwerking', 'voor de verwerking verantwoordelijke', 'verwerker', 'betrokkene' en 'toezichthoudende autoriteit' dezelfde betekenis hebben als in de Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens;

(b) 'de gegevensexporteur' betekent de voor de verwerking verantwoordelijke die de persoonsgegevens overdraagt;

(c) 'de gegevensimporteur' betekent de verwerker die bereid is de persoonsgegevens te ontvangen van de gegevensexporteur, welke bedoeld zijn voor verwerking namens deze na de overdracht conform de instructies en de voorwaarden van de Bepalingen en die niet afhankelijk is van een systeem van een derde land dat onvoldoende bescherming waarborgt volgens de strekking van Artikel 25(1) van Richtlijn 95/46/EC;

(d) 'de onderaannemer' betekent elke verwerker die is aangesteld door de gegevensimporteur of door een andere onderaannemer van de gegevensimporteur die bereid is om van de gegevensimporteur of enige andere onderaannemer van de gegevensimporteur persoonsgegevens te ontvangen, welke uitsluitend bedoeld zijn voor het uitvoeren van verwerkingsactiviteiten namens de gegevensexporteur na de overdracht conform de instructies, de voorwaarden van de Bepalingen en de voorwaarden van het schriftelijke onderaannemingscontract;

(e) 'de van toepassing zijnde wet op de gegevensbescherming' betekent de wetgeving die de fundamentele rechten en vrijheden van natuurlijke personen beschermt en met name in verband met de verwerking van persoonsgegevens met betrekking tot een voor de verwerking verantwoordelijke in de Lidstaat waarin de gegevensexporteur gevestigd is;

(f) 'technische en organisatorische beveiligingsmaatregelen' betekent maatregelen die tot doel hebben persoonsgegevens te beschermen tegen onbedoelde of onwettige vernietiging, verlies door ongelukken, wijziging, ongeautoriseerde bekendmaking of toegang, met name waar de verwerking verzending van gegevens via een netwerk inhoudt, en tegen alle andere onwettige vormen van verwerking.

Artikel 2. Details van de overdracht

De details van de overdracht en met name, waar van toepassing, de speciale categorieën persoonsgegevens worden gespecificeerd in Appendix 1, die een integraal onderdeel vormt van de Bepalingen.

Artikel 3. Derdenbeding

1. De betrokkene kan bij de gegevensexporteur deze Bepaling, Bepaling 4(b) t/m (i), Bepaling 5(a) t/m (e) en (g) t/m (j), Bepaling 6(1) en (2), Bepaling 7, Bepaling 8(2) en Bepalingen 9 t/m 12 afdwingen als derde begunstigde.

2. De betrokkene kan bij de gegevensexporteur deze Bepaling, Bepaling 5(a) t/m (e) en (g), Bepaling 6, Bepaling 7, Bepaling 8(2) en Bepalingen 9 t/m 12 afdwingen , in gevallen waarbij de gegevensexporteur feitelijk is verdwenen of voor de wet is opgehouden te bestaan, tenzij enige opvolgende entiteit alle wettelijke verplichtingen van de gegevensexporteur contractueel of van rechtswege op zich heeft genomen, ten gevolge waarvan deze de rechten en verplichtingen van de gegevensexporteur overneemt, in welk geval de betrokkene de bepalingen bij de nieuwe entiteit kan afdwingen.

3. De betrokkene kan bij de onderaannemer deze Bepaling, Bepaling 5(a) t/m (e) en (g), Bepaling 6, Bepaling 7, Bepaling 8(2) en Bepalingen 9 t/m 12 afdwingen, in gevallen waarbij zowel de gegevensexporteur als de gegevensimporteur feitelijk is verdwenen of voor de wet is opgehouden te bestaan of insolvent is geworden, tenzij enige opvolgende entiteit alle wettelijke verplichtingen van de gegevensexporteur contractueel of van rechtswege op zich heeft genomen, ten gevolge waarvan deze de rechten en verplichtingen van de gegevensexporteur overneemt, in welk geval de betrokkene de bepalingen bij de nieuwe entiteit kan afdwingen. De aansprakelijkheid jegens derde van de onderaannemer zal beperkt zijn tot diens eigen verwerkingsactiviteiten krachtens de Bepalingen.

4. De partijen maken geen bezwaar wanneer een betrokkene wordt vertegenwoordigd door een associatie of een andere rechtspersoon indien de betrokkene dat expliciet wenst en indien dit toegestaan is onder de nationale wetgeving.

Artikel 4. Verplichtingen van de gegevensexporteur

De gegevensexporteur verklaart en garandeert:

(a) dat de verwerking, met inbegrip van de overdracht zelf, van de persoonsgegevens is en zal worden uitgevoerd overeenkomstig de relevante voorzieningen van de van toepassing zijnde wet op de gegevensbescherming (en, waar van toepassing, is medegedeeld aan de betreffende autoriteiten van de Lidstaat waar de gegevensexporteur gevestigd is) en niet in strijd is met de relevante voorzieningen van die Lidstaat;

(b) dat hij de gegevensimporteur heeft geïnstrueerd en tijdens de duur van de verwerkingsservice voor de persoonsgegevens zal blijven instrueren om de overgedragen persoonsgegevens uitsluitend te verwerken

namens de gegevensexporteur en conform de van toepassing zijnde wet op de gegevensbescherming en de Bepalingen;

(c) dat de gegevensimporteur voldoende garanties zal geven inzake de technische en organisatorische beveiligingsmaatregelen die gespecificeerd zijn in Appendix 2 bij dit contract;

(d) dat na evaluatie van de vereisten van de van toepassing zijnde wet op de gegevensbescherming, de beveiligingsmaatregelen passend zijn om persoonsgegevens te beschermen tegen onbedoelde of onwettige vernietiging, verlies door ongelukken, wijziging, ongeautoriseerde bekendmaking of toegang, met name waar de verwerking het verzenden van gegevens via een netwerk inhoudt, en tegen alle andere onwettige vormen van verwerking, en dat deze maatregelen een passende bescherming bieden tegen de risico's die optreden door de verwerking en het karakter van de gegevens die moeten worden beschermd, rekening houdend met de status en de kosten van hun implementatie;

(e) dat hij waarborgt dat de juiste beveiligingsmaatregelen worden genomen;

(f) dat, indien bijzondere categorieën gegevens worden overgebracht de betrokkene is geïnformeerd en zal worden geïnformeerd voor, of zo spoedig mogelijk na, de overdracht dat de gegevens kunnen worden overgebracht naar een derde land dat onvoldoende bescherming waarborgt volgens de strekking van Richtlijn 95/46/Ec;

(g) dat elke van de gegevensimporteur of een onderaannemer ontvangen melding met betrekking tot Bepaling 5(b) en Bepaling 8(3) zal worden doorgegeven aan de toezichthoudende autoriteit als de gegevensexporteur besluit om de overdracht voort te zetten of de opschorting te beëindigen;

(h) op verzoek aan de betrokkene een kopie beschikbaar te stellen van de Bepalingen, met uitzondering van Appendix 2, en een overzicht van de beveiligingsmaatregelen, alsmede een kopie van elk contract voor het onderaanbesteden van diensten dat moet worden opgesteld conform de Bepalingen, tenzij de Bepalingen of het contract commerciële informatie bevatten, in welk geval de betreffende commerciële informatie kan worden verwijderd;

(i) dat, in geval van onderaanbesteding, de verwerkingsactiviteit wordt uitgevoerd conform Bepaling 11 door een onderaannemer die tenminste hetzelfde niveau van bescherming voor de persoonsgegevens en dezelfde rechten van de betrokkene biedt als de gegevensimporteur krachtens de Bepalingen; en

(j) dat hij waarborgt dat zal worden voldaan aan Bepaling 4(a) t/m (i).

Artikel 5. Verplichtingen van de gegevensimporteur

De gegevensimporteur verklaart en garandeert:

(a) de persoonsgegevens alleen namens de gegevensexporteur te verwerken en conform de instructies en de Bepalingen; als hij om enige reden een dergelijke waarborg niet kan geven zal hij de gegevensexporteur onmiddellijk informeren over zijn onvermogen om aan de instructies en de Bepalingen te voldoen, in welk geval de gegevensexporteur het recht heeft om de gegevensoverdracht op te schorten en/of het contract te beëindigen;

(b) dat hij geen redenen heeft om aan te nemen dat van toepassing zijnde wetgeving hem verhindert om de van de gegevensexporteur ontvangen instructies uit te voeren en aan zijn verplichtingen onder het contract te voldoen en dat, in geval van een wijziging in de wetgeving die een nadelig effect zou kunnen hebben op de garanties en verplichtingen die het gevolg zijn van de Bepalingen, hij de gegevensexporteur onmiddellijk op de hoogte zal

stellen van de wijziging, in welk geval de gegevensexporteur het recht heeft om de gegevensoverdracht op te schorten en/of het contract te beëindigen;

(c) dat hij de in Appendix 2 gespecificeerde technische en organisatorische beveiligingsmaatregelen heeft geïmplementeerd voordat de overgebrachte persoonsgegevens worden verwerkt;

(d) dat hij de gegevensexporteur onverwijld op de hoogte zal stellen van:

(i) enig wettelijk bindend verzoek om bekendmaking van de persoonsgegevens door een wetshandhavende autoriteit, tenzij anderszins verboden, zoals een verbodsbepaling onder het strafrecht om de vertrouwelijkheid van een strafrechtelijk onderzoek te waarborgen,
(ii) elke onbedoelde of ongeautoriseerde toegang en
(iii) elk verzoek dat rechtstreeks van de betrokkenen ontvangen is, zonder te reageren op dat verzoek, tenzij hij anderszins geautoriseerd is om dat te doen;

(e) onmiddellijk en passend te reageren op alle informatieverzoeken van de gegevensexporteur in verband met de verwerking van de persoonsgegevens die worden overgebracht en het advies van de toezichthoudende autoriteit inzake de verwerking van de overgebrachte gegevens op te volgen;

(f) op verzoek van de gegevensexporteur zijn gegevenswerkingsfaciliteiten open te stellen voor een audit naar de verwerkingsactiviteiten die onder de Bepalingen vallen, welk onderzoek zal worden uitgevoerd door de gegevensexporteur of door een uit onafhankelijke leden samengesteld inspectie-orgaan dat de vereiste professionele kwalificaties heeft en dat gebonden is aan geheimhoudingsplicht en dat door de gegevensexporteur is geselecteerd, waar nodig in overleg met de toezichthoudende autoriteit;

(g) op verzoek aan de betrokkene een kopie van de Bepalingen ter beschikking te stellen, tenzij de Bepalingen of het contract commerciële informatie bevatten, in welk geval de betreffende commerciële informatie kan worden verwijderd, met uitzondering van Appendix 2 die zal worden vervangen door een samenvatting van de beveiligingsmaatregelen in die gevallen waar de betrokkene geen kopie van de gegevensexporteur kan verkrijgen;

(h) dat in geval van onderaanneming hij de gegevensexporteur van tevoren op de hoogte heeft gesteld en diens schriftelijke toestemming heeft verkregen;

(i) dat de verwerkingsservices van de onderaannemer worden uitgevoerd conform Bepaling 11;

(j) om direct een kopie van een onderaannemersovereenkomst die wordt gesloten onder de Bepalingen aan de gegevensexporteur toe te zenden.

Artikel 6. Aansprakelijkheid

1. De partijen komen overheen dat elke betrokkene die schade heeft geleden ten gevolge van een inbreuk op de in Bepaling 3 of in Bepaling 11 vastgelegde verplichtingen door enige partij of onderaannemer, recht heeft op een vergoeding voor de geleden schade door de gegevensexporteur.

2. Indien een betrokkene niet in staat is om tegen de gegevensexporteur een claim voor schadevergoeding in te dienen conform paragraaf 1, voortkomend uit een inbreuk door de gegevensimporteur of diens onderaannemer op enige van hun verplichtingen zoals vastgelegd in Bepaling 3 of in Bepaling 11, omdat de gegevensimporteur feitelijk is verdwenen of voor de wet is opgehouden te bestaan of insolvent is geworden, stemt de gegevensimporteur ermee in dat de betrokkene een claim kan indienen tegen de gegevensimporteur alsof deze de gegevensexporteur was, tenzij

enige opvolgende entiteit alle wettelijke verplichtingen van de gegevensexporteur contractueel of van rechtswege op zich heeft genomen, in welk geval de betrokkene zijn claim tegen die entiteit kan indienen.

De gegevensimporteur mag zich niet beroepen op een inbreuk op zijn verplichtingen door een onderaannemer om zijn eigen aansprakelijkheid af te wijzen.

3. Indien een betrokkene niet in staat is om tegen de gegevensexporteur of de gegevensimporteur een claim in te dienen conform paragraaf 1 en 2, voortkomend uit een inbreuk door de onderaannemer op enige van diens verplichtingen zoals vastgelegd in Bepaling 3 of in Bepaling 11, omdat zowel de gegevensimporteur als de gegevensimporteur feitelijk zijn verdwenen of voor de wet zijn opgehouden te bestaan of insolvent zijn geworden, stemt de onderaannemer ermee in dat de betrokkene een claim kan indienen tegen de onderaannemer ten aanzien van diens eigen verwerkingsactiviteiten onder de Bepalingen alsof deze de gegevensexporteur of de gegevensimporteur was, tenzij enige opvolgende entiteit alle wettelijke verplichtingen van de gegevensexporteur of de gegevensimporteur contractueel of van rechtswege op zich heeft genomen, in welk geval de betrokkene zijn claim tegen die entiteit kan indienen. De aansprakelijkheid van de onderaannemer zal beperkt zijn tot diens eigen verwerkingsactiviteiten onder de Bepalingen.

Artikel 7. Bemiddeling en jurisdictie

1. De gegevensimporteur stemt ermee in dat als de betrokkene tegen hem een beroep doet op rechten als derde begunstigde en/of een schadevergoeding eist voor schade onder de Bepalingen, de gegevensimporteur de beslissing van de betrokkene zal accepteren:

   (a) o.m in het geschil te laten bemiddelen door een onafhankelijk persoon of, waar van toepassing, door de toezichthoudende autoriteit;

   (b) om het geschil voor te leggen aan de rechtbank van de Lidstaat waarin de gegevensexporteur is gevestigd.

2. De partijen komen overeen dat de door de betrokkene gemaakte keuze geen afbreuk doet aan diens materiële of procedurele rechten op schadevergoeding krachtens andere voorzieningen in de nationale of internationale wetgeving.

Artikel 8. Samenwerking met toezichthoudende autoriteiten

1. De gegevensexporteur stemt ermee in om een kopie van het contract te deponeren bij de toezichthoudende autoriteit als deze daarom verzoekt of als dat verplicht is onder de van toepassing zijnde wet op de gegevensbescherming.

2. De partijen komen overeen dat de toezichthoudende autoriteit het recht heeft om een onderzoek in te stellen naar de gegevensimporteur en elke onderaannemer, dat dezelfde reikwijdte heeft en waarvoor dezelfde voorwaarden gelden als voor een eventuele audit van de gegevensexporteur onder de van toepassing zijnde wet op de gegevensbescherming.

3. De gegevensimporteur zal de gegevensexporteur onverwijld informeren over het bestaan van wetgeving die op deze of op een onderaannemer van toepassing is die het uitvoeren van een audit van de gegevensimporteur of enige onderaannemer, krachtens paragraaf 2 verhindert. In een dergelijk geval zal de gegevensexporteur gerechtigd zijn om de maatregelen te nemen die voorzien zijn in Bepaling 5 (b).

Artikel 9. Toepasselijk recht

De Bepalingen vallen onder de wet van de Lidstaat waarin de gegevensexporteur gevestigd is.

Artikel 10. Aanpassing van het contract

De partijen verplichten zich om de Bepalingen niet aan te passen of te wijzigen. Dit belet de partijen niet om indien nodig Bepalingen toe te voegen over gerelateerde onderwerpen, mits deze niet strijdig zijn met een eerdere Bepaling.

Artikel 11. Onderaannemers

1. De gegevensimporteur zal geen van zijn verwerkingsactiviteiten die worden uitgevoerd namens de gegevensexporteur onder de Bepalingen zonder voorafgaande schriftelijke toestemming van de gegevensexporteur onderaanbesteden. Wanneer de gegevensimporteur zijn verplichtingen onder de Bepalingen met toestemming van de gegevensexporteur onderaanbesteedt, zal deze dit alleen doen via een schriftelijke overeenkomst met de onderaannemer die aan de onderaannemer dezelfde verplichtingen oplegt als welke gelden voor de gegevensimporteur onder de Bepalingen. Wanneer de onderaannemer zijn verplichting tot gegevensbescherming onder een dergelijke schriftelijke overeenkomst niet nakomt, blijft de gegevensimporteur volledig aansprakelijk tegenover de gegevensexporteur voor het nakomen van de verplichtingen van de onderaannemer onder de desbetreffende overeenkomst.

2. Het eerdere schriftelijke contract tussen de gegevensimporteur en de onderaannemer zal ook een Bepaling voor een derde begunstigde bevatten zoals vastgelegd in Bepaling 3, voor gevallen waarin de betrokkene niet in staat is om tegen de gegevensexporteur of de gegevensimporteur een schadevergoedingsclaim in te dienen conform paragraaf 1 van Bepaling 6, omdat deze feitelijk zijn verdwenen of voor de wet zijn opgehouden te bestaan of insolvent zijn geworden en geen opvolgende entiteit alle wettelijke verplichtingen van de gegevensexporteur of de gegevensimporteur contractueel of van rechtswege heeft overgenomen. De aansprakelijkheid jegens derde van de onderaannemer zal beperkt zijn tot diens eigen verwerkingsactiviteiten krachtens de Bepalingen.

3. De voorzieningen inzake gegevensbeschermingsaspecten voor onderaanbesteding van het contract waarnaar in paragraaf 1 wordt verwezen vallen onder de wetgeving van de Lidstaat waarin de gegevensexporteur gevestigd is.

4. De gegevensexporteur zal een lijst bijhouden van de onderaannemingsovereenkomsten die zijn afgesloten onder de Bepalingen en die gemeld zijn door de gegevensimporteur conform Bepaling 5 (j) en deze lijst zal tenminste eenmaal per jaar worden bijgewerkt. De lijst zal beschikbaar zijn voor de autoriteit van de gegevensexporteur die toezicht houdt op gegevensbescherming.

Artikel 12. Verplichting na beëindiging van de services voor het verwerken van persoonsgegevens

1. De partijen komen overheen dat de gegevensimporteur en de onderaannemer na beëindiging van de levering van gegevensverwerkingsservices, naar inzicht van de gegevensexporteur, alle overgebrachte persoonsgegevens en de kopieën daarvan zullen retourneren aan de gegevensexporteur of alle persoonsgegevens zullen vernietigen en aan de gegevensexporteur zullen certificeren dat dit is gebeurd, tenzij de gegevensimporteur door geldende wetgeving wordt verhinderd om alle of een gedeelte van de overgebrachte persoonsgegevens te retourneren of te vernietigen. In dat geval garandeert de gegevensimporteur dat hij de vertrouwelijkheid van de overgebrachte persoonsgegevens zal waarborgen en dat hij de overgebrachte persoonsgegevens niet langer actief zal verwerken.

2. De gegevensimporteur en de onderaannemer garanderen dat zij op verzoek van de gegevensexporteur en/of de toezichthoudende autoriteit de gegevenswerkingsfaciliteit open zullen stellen voor een controle op de in paragraaf 1 beschreven maatregelen.

APPENDIX 1 BIJ DE MODELCONTRACTBEPALINGEN

Gegevensexporteur
De gegevensexporteur is (gaarne in korte bewoordingen de voor de overdracht relevante activiteiten specificeren):

Klant is abonnee van een Cloud Service die wordt geleverd door SISW, welke door de Klant geautoriseerde eindgebruikers toestaat om Klantgegevens in te voeren, te wijzigen, te gebruiken, te verwijderen, te downloaden en anderszins te verwerken, waaronder ook persoonsgegevens kunnen zijn zoals beschreven in de Overeenkomst en de relevante documentatie voor de Cloud Service.

Gegevensimporteur
De gegevensimporteur is (gaarne in korte bewoordingen de voor de overdracht relevante activiteiten specificeren):

Siemens Product Lifecycle Management Software Inc. levert, zelf en/of via zijn onderaannemers, de Cloud Service die het volgende inhoudt: onderhouden van de computerinfrastructuur in de Verenigde Staten en de Europese Unie waarop de Cloud Service wordt uitgevoerd, opslaan op de infrastructuur van de Klantgegevens die door de Klant naar de Cloud Service worden geüpload, bewaken van de beschikbaarheid en de goede werking van de Cloud Service en de infrastructuur en waarborgen van de veiligheid van de infrastructuur zoals vastgelegd in de Overeenkomst en de relevante documentatie voor de Cloud Service.

Betrokkenen
De persoonsgegevens die worden overgebracht hebben betrekking op de volgende categorieën betrokkenen (gaarne specificeren):

Tenzij expliciet schriftelijk gespecificeerd door de gegevensexporteur, kunnen betrokkenen onder meer zijn: eindgebruikers die door de Klant geautoriseerd zijn om de Cloud Service te gebruiken en andere personeelsleden van de Klant van wie persoonsgegevens zijn opgeslagen in de Cloud Service.

Gegevenscategorieën
De persoonsgegevens die worden overgebracht behoren tot de volgende gegevenscategorieën (gaarne specificeren):

Specifieke gegevenscategorieën die worden opgeslagen in de Cloud Service kunnen wezenlijk worden geconfigureerd door de Klant, hoewel bepaalde gangbare gegevenscategorieën die worden opgeslagen in de Cloud Service bijvoorbeeld (maar niet uitsluitend) kunnen zijn: naam, e-mailadres, bedrijfsnaam, telefoonnummer, werklocatie, nationaliteit of staatsburgerschap en informatie over de toegang tot en het gebruik van de Cloud Service. Afhankelijk van de configuratie van de Cloud Service door de Klant kunnen diverse andere gegevenscategorieën vertegenwoordigd zijn in de Klantgegevens.

Bijzondere categorieën gegevens (indien van toepassing)
De persoonsgegevens die worden overgebracht bevatten de volgende bijzondere categorieën gegevens (gaarne specificeren):

Over eventuele bijzondere categorieën gegevens die in de Cloud Service worden opgeslagen moet overeenstemming worden bereikt tussen de partijen in de Overeenkomst of in een Order of deze moeten worden vastgelegd in een Statement of Work voor het leveren van professionele services aan de Klant als onderdeel van diens implementatie van de Cloud Service.

Verwerkingsactiviteiten
Op de overgebrachte persoonsgegevens worden de volgende elementaire verwerkingsactiviteiten uitgevoerd (gaarne specificeren):

De persoonsgegevens kunnen worden verwerkt als onderdeel van de normale werking van de Cloud Service, afhankelijk van de configuratie van de Klant, via opslag en/of archivering op de computerinfrastructuur die wordt onderhouden door de gegevensexporteur, in single-tenant of multi-tenant omgevingen, gebruikt of overgebracht overeenkomstig de instructies die aan de Cloud Service worden gegeven door een eindgebruiker die door de Klant is geautoriseerd om de Cloud Service te gebruiken en in het kader van onderhoudsactiviteiten voor de Cloud Service die worden uitgevoerd door de gegevensexporteur.

APPENDIX 2 BIJ DE MODELCONTRACTBEPALINGEN

Bepaalde Cloud Service diensten worden geleverd onder afwijkende voorwaarden, die indien van toepassing vastgelegd worden in een Order. Anderszins voert de gegevensimporteur de hieronder beschreven technische en organisatorische maatregelen met betrekking tot de in het Systeem opgeslagen persoonsgegevens uit conform Bepalingen 4(d) en 5(c) van de Bepalingen.

Beschrijving van de technische en organisatorische beveiligingsmaatregelen die door de gegevensimporteur worden geïmplementeerd overeenkomstig Bepaling 4(d) en 5(c):

1. Controle op de fysieke toegang. Ongeautoriseerde personen hebben geen fysieke toegang tot de gebouwen of ruimtes waar de gegevensverwerkingssystemen die de persoonsgegevens verwerken en/of gebruiken zich bevinden.

   Maatregelen: Alle datacenters hanteren strikte beveiligingsprocedures en dwingen deze af met behulp van beveiligingspersoneel, bewakingsapparatuur, bewegingsdetectoren, toegangscontrolemechanismen en andere maatregelen om te voorkomen dat apparatuur en datacenterfaciliteiten gevaar lopen. Alleen geautoriseerde vertegenwoordigers hebben toegang tot systemen en infrastructuur in de datacenterfaciliteiten. Om een goede werking te waarborgen vindt regelmatig onderhoud van fysieke beveiligingsapparatuur (zoals bewegingssensoren, camera's en dergelijke) plaats. De volgende fysieke beveiligingsmaatregelen worden tot in detail geïmplementeerd in alle datacenters:

   a. In het algemeen worden gebouwen beveiligd met toegangscontrolesystemen (smart-cardsysteem).
   b. Autorisatiegegevens, zoals elektronische toegangbadges (uniek voor elke werknemer, leverancier of onderaannemer) en pincodes worden verstrekt aan geautoriseerd personeel om fysiek toegang te verkrijgen tot de datacenterfaciliteiten.
   c. Fysieke toegang tot de datacenters binnen de systeemgrens wordt gecontroleerd door een elektronisch toegangscontrolesysteem, dat bestaat uit kaartlezers en pinapparaten voor het betreden van gebouwen en ruimtes en alleen kaartlezers voor het verlaten van gebouwen en ruimtes.
   d. Afhankelijk van de veiligheidsclassificatie worden gebouwen, individuele gebieden en omliggende terreinen verder beveiligd met extra maatregelen. Dit kunnen bijvoorbeeld specifieke toegangsprofielen, videobewaking, inbraakalarmsystemen en biometrische toegangscontrolesystemen zijn.
   e. Toegangsrechten worden op individuele basis verleend aan geautoriseerde personeelsleden, volgens de hieronder beschreven maatregelen voor controle op systeemtoegang en gegevenstoegang. Dit geldt ook voor bezoekerstoegang. Gasten en bezoekers in gebouwen van SISW moeten bij de receptie hun naam registreren en moeten worden vergezeld door geautoriseerd SISW-personeel. SISW en alle derde-partij datacenterleveranciers registreren de namen van de personen die privégebieden van SISW in de datacenters betreden en het moment waarop dat gebeurt.
   f. SISW-werknemers en externe medewerkers moeten op alle locaties van SISW altijd hun ID-kaart dragen.

2. Controle op de systeemtoegang. Er moet worden gewaarborgd dat gegevensverwerkingssystemen die worden gebruikt voor levering van de Cloud Service niet zonder toestemming kunnen worden gebruikt.

   Maatregelen:
   a. SISW of zijn onderaannemers beheren de omgeving om te voldoen aan de vereisten van NIST SP 800-53 Rev 4 AC (Access Control) en IA (Identification and Authentication).
   b. Er worden verschillende autorisatieniveaus gehanteerd om toegang te verlenen tot gevoelige systemen, onder meer die waarop persoonsgegevens worden bewaard en verwerkt. Er zijn processen geïmplementeerd om te waarborgen dat alleen geautoriseerde gebruikers de juiste rechten hebben om gebruikers toe te voegen, te verwijderen of te wijzigen.
   c. Alle gebruikers hebben toegang tot de systemen van SISW met een unieke gebruikersnaam en een wachtwoord dat aan bepaalde minimumvereisten voor complexiteit moet voldoen.
   d. SISW en zijn onderaannemers hebben procedures om te waarborgen dat aangevraagde veranderingen in autorisatie alleen worden geïmplementeerd volgens de richtlijnen (bijvoorbeeld dat zonder autorisatie geen rechten worden verleend). Als een SISW-gebruiker een andere rol krijgt of het bedrijf verlaat, wordt er een procedure uitgevoerd om de toegangsrechten tot de omgeving in te trekken.
   e. SISW en zijn onderaannemers hebben een wachtwoordbeleid ingesteld dat het delen van wachtwoorden verbiedt, dat regelt wat er moet gebeuren wanneer een wachtwoord uitlekt, dat vereist dat alle gebruikerswachtwoorden regelmatig worden veranderd en dat standaardwachtwoorden worden gewijzigd. Er worden gepersonaliseerde gebruikers-ID's toegewezen voor authenticatie. Alle wachtwoorden moeten voldoen

aan de minimumvereisten voor complexiteit en worden in versleutelde vorm opgeslagen. In het geval van domeinwachtwoorden vereist het systeem dat het wachtwoord elke 60 dagen wordt gewijzigd en dat wachtwoorden aan de minimumvereisten voor complexiteit voldoen. Elke SISW-computer heeft een screensaver met wachtwoordbeveiliging.

f. SISW of zijn onderaannemers controleren automatisch de volgende accountgebeurtenissen: aanmaken, wijzigen, inschakelen, uitschakelen en verwijderen. Een systeembeheerder controleert de logboeken periodiek.
g. Netwerken van SISW en zijn onderaannemers worden door firewalls afgeschermd van het openbare internet.
h. SISW en zijn onderaannemers maken bij toegangspunten tot het bedrijfsnetwerk, voor e-mailaccounts en op alle bestandsservers en alle workstations gebruik van up-to-date antivirussoftware.
i. SISW en zijn onderaannemers implementeren beveiligingspatchbeheer om te zorgen dat de relevante beveiligingsupdates worden geïnstalleerd.
j. Volledige remote toegang tot het bedrijfsnetwerk en de kritische infrastructuur van SISW wordt beveiligd door krachtige meerlaags authenticatie.

3. Controle op de gegevenstoegang. Medewerkers die het recht hebben om gegevensverwerkingssystemen te gebruiken, krijgen alleen toegang tot de persoonsgegevens die zij strikt nodig hebben en deze persoonsgegevens mogen niet zonder toestemming tijdens de verwerking, het gebruik of in opslag worden gelezen, gekopieerd, gewijzigd of verwijderd.

   Maatregelen:

   a. Toegang tot persoonlijke, vertrouwelijke of gevoelige informatie wordt alleen verleend indien dat nodig is. Met andere woorden: werknemers of externe derde partijen krijgen alleen toegang tot de informatie die zij nodig hebben om hun werk te doen. SISW gebruikt autorisatiemethoden waarbij wordt gedocumenteerd hoe rechten worden toegewezen en welke rechten worden toegewezen. Alle persoonlijke, vertrouwelijke of anderszins gevoelige gegevens worden beschermd conform het beveiligingsbeleid en de beveiligingsstandaarden van SISW.
   b. Alle productieservers van iedere SISW Cloud Service werken in de relevante datacenters. Beveiligingsmaatregelen ter bescherming van applicaties waarmee persoonlijke, vertrouwelijke of anderszins gevoelige gegevens worden verwerkt, worden regelmatig gecontroleerd. Daartoe maakt SISW ook gebruik van periodieke externe audits om te waarborgen dat deze maatregelen op de juiste wijze worden toegepast.
   c. SISW staat niet toe dat persoonlijke software of andere niet door SISW goedgekeurde software wordt geïnstalleerd op systemen die voor een Cloud Service worden gebruikt.
   d. Indien het nodig is gegevens over te brengen na een defect in de onderliggende gegevensopslagmedia, worden de opslagmedia na de overdracht gedemagnetiseerd (voor magnetische opslag) of versnipperd (voor solid-state of optische opslag).

4. Controle op de gegevensoverdracht. Persoonsgegevens mogen niet zonder toestemming tijdens de overdracht worden gelezen, gekopieerd, gewijzigd of verwijderd.

   Maatregelen:

   a. SISW of zijn onderaannemer beheert de infrastructuur en configuratie zodanig dat wordt voldaan aan de vereisten van NIST SP 800-53 Rev 4 Systems and Communication Protection (SC). Dit omvat netwerkgebaseerde inbraakpreventiesystemen (NIPS) en firewalls aan de systeemgrenzen als bescherming tegen kwaadwillige communicaties aan de buitengrenzen van de infrastructuur. NIPS en firewalls worden geconfigureerd volgens DISA STIG-standaarden. Gegevens worden tijdens de overdracht versleuteld met cryptografiemodules die voldoen aan FIPS 140-2.
   b. Wanneer gegevensdragers fysiek worden verplaatst, neemt SISW passende maatregelen om te zorgen dat de overeengekomen serviceniveaus worden gehaald (bijvoorbeeld encryptie en met lood gevoerde containers).
   c. Overdracht van de persoonsgegevens via interne SISW netwerken wordt op dezelfde manier beschermd als die van andere vertrouwelijke gegevens, conform het beveiligingsbeleid van SISW.
   d. Wanneer de gegevens worden overgestuurd tussen SISW en de Klant, worden maatregelen voor de overdracht van persoonsgegevens toegepast zoals vastgelegd in de Overeenkomst of de relevante documentatie voor de Cloud Service. Dit geldt zowel voor fysieke gegevensoverdracht als voor overdracht via het netwerk. De Klant is verantwoordelijk voor de gegevensoverdracht vanaf SISW's demarcatiepunt (bijvoorbeeld de uitgaande firewall of het datacenter waar de Cloud Service wordt gehost).

5. Controle op gegevensinvoer. Bij de Cloud Service is het mogelijk achteraf te bepalen of en door wie persoonsgegevens zijn ingevoerd, gewijzigd of verwijderd in de infrastructuur die wordt gebruikt om de Cloud Service leveren.

Maatregelen:

a. SISW geeft alleen geautoriseerde medewerkers toegang tot de persoonsgegevens voor zover dit noodzakelijk is voor hun werkzaamheden. SISW heeft een registratiesysteem geïmplementeerd voor het invoeren, wijzigen en verwijderen of blokkeren van persoonsgegevens door SISW of zijn onderaannemers dat vrijwel geheel wordt ondersteund door de Cloud Service.
b. Audittrails bieden voldoende gedetailleerde informatie voor het reconstrueren van voorvallen van ongeautoriseerde activiteit of wanneer een storing is opgetreden of wordt vermoed. Elk record in het voorvallogboek van het besturingssysteem bevat het type voorval, een tijdstempel, de bron van het voorval, de gevolgen van het voorval en de met het voorval geassocieerde gebruiker.

6. Controle op de verwerking. Persoonsgegevens worden uitsluitend verwerkt conform de voorwaarden van de Overeenkomst en eventuele door de Klant verstrekte instructies.

   Maatregelen:

   a. SISW gebruikt controlemechanismen en processen om te waarborgen dat de contracten tussen SISW en zijn klanten, onderaannemers of andere serviceleveranciers strikt worden nageleefd.
   b. Klantgegevens worden tenminste beveiligd met hetzelfde beschermingsniveau als vertrouwelijke informatie volgens de SISW Information Classification-standaard.
   c. Alle werknemers en contractpartners van SISW zijn contractueel gebonden om de vertrouwelijkheid van alle gevoelige informatie, inclusief handelsgeheimen, van klanten en partners van SISW te respecteren.

7. Controle op de beschikbaarheid. Persoonsgegevens worden beschermd tegen onbedoelde of ongeautoriseerde vernietiging of verlies.

   Maatregelen:

   a. SISW maakt gebruik van back-upprocessen en andere maatregelen om te zorgen dat bedrijfskritische systemen indien en wanneer nodig snel kunnen worden hersteld.
   b. SISW werkt met wereldwijde cloudserviceleveranciers om te zorgen dat datacenters altijd beschikbaar zijn.
   c. SISW heeft procedures voor onvoorziene gebeurtenissen en disaster-recoverystrategieën voor Cloud Services.

8. Controle op gegevensscheiding . Persoonsgegevens die voor verschillende doeleinden zijn verzameld, kunnen afzonderlijk worden verwerkt.

   Maatregelen:

   a. Waar van toepassing gebruikt SISW de technische mogelijkheden van de geïnstalleerde software (bijvoorbeeld: multi-tenancy of aparte systeemlandschappen) om de persoonsgegevens van de Klant en die van andere klanten gescheiden te houden.
   b. SISW onderhoudt afzonderlijke omgevingen (met logische of fysieke scheiding) voor elke klant.
   c. Klant (inclusief zijn gerelateerde bedrijven) heeft alleen toegang tot zijn eigen klantomgeving(en).

9. Controle van de gegevensintegriteit. Waarborgt dat de persoonsgegevens tijdens de verwerkingsactiviteiten ongeschonden, compleet en actueel blijven:

   Maatregelen: SISW heeft een meerlaags verdedigingsstrategie geïmplementeerd ter bescherming tegen ongeautoriseerde wijzigingen. Het gaat hierbij om controlemechanismen zoals hierboven beschreven in de gedeelten over controle en maatregelen. De configuratie van firewalls leidt tot meerdere netwerksegmenten met gescheiden publieke en private toegang. Elke set firewallregels bevat specifieke toegangscontroles waarin wordt gedefinieerd welke communicaties tussen deze segmenten zijn toegestaan

   a. Centrum voor beveiligingsbewaking: Automatische software voor het detecteren van indringers wordt gebruikt in combinatie met andere preventieve beveiligingssoftware en forensische software en processen om te waarschuwen bij elk beveiligingsincident, dit te onderzoeken, het zo nodig te melden en te assisteren bij het oplossen .
   b. Antivirussoftware: op alle systemen zijn actuele antivirusdefinities aanwezig die geconfigureerd zijn om te beschermen tegen virussen, wormen, trojans en andere vormen van malware.
   c. Back-up en herstel: alle systemen bevatten een basisniveau van back-upsnapshots van gegevens en configuratie. Indien van toepassing zullen SISW en zijn onderaannemers de omgeving van een klant ook onderhouden met

een hoge-beschikbaarheidsconfiguratie die zorgt dat de gegevens in twee afzonderlijke datacenters op voldoende afstand van elkaar worden opgeslagen.

d. Regelmatige externe audits om te bewijzen dat de beveiligingsmaatregelen worden toegepast. SISW en zijn onderaannemers zullen periodiek externe audits ondergaan om de bovengenoemde beveiligingsmaatregelen te controleren.