DATA SECURITY AGREEMENT

Tussen:

AMPTEC BV, een besloten vennootschap naar Belgisch recht, met maatschappelijke zetel te 3740 Bilzen, Bremakker 45, en ondernemingsnummer 0442.333.460, vertegenwoordigd door Bart Willems bestuurder, Verder genoemd de "**Service Provider**" of "**Amptec**";

En de **KLANT** Verder genoemd als de "**Klant**",

De Service Provider en de Klant worden hierna individueel aangeduid als een "**Partij**" en gezamenlijk als de "**Partijen**".

1. Scope.

Voor zover de Service Provider toegang heeft tot Klantsystemen of Klantfaciliteiten, of Klantgegevens, Persoonlijke Informatie of Vertrouwelijke Informatie (zoals gedefinieerd in artikel 12) verwerkt, vanwege de door de Service Provider geleverde Diensten, is deze Data Security Agreement (hierna: "**DSA**") van toepassing.

De Service Provider verbindt zich ertoe daarbij alle toepasselijke beveiligingsmaatregelen, instructies en beleidsdocumenten na te leven die door de Klant schriftelijk zijn verstrekt, uitdrukkelijk zijn gecommuniceerd of aantoonbaar zijn gedocumenteerd.

Deze verplichtingen gelden eveneens voor alle systemen en faciliteiten van de Service Provider die worden gebruikt om Klantgegevens te verzamelen, te raadplegen, op te slaan, te verwerken, te back-uppen of te verwijderen.

De Service Provider mag Klantgegevens uitsluitend verwerken voor de uitvoering van de overeengekomen Diensten, of in de mate waarin dit uitdrukkelijk is toegestaan onder de Overeenkomst. Elk ander gebruik is verboden.

Dit document beschrijft de technische en organisatorische beveiligingsmaatregelen die Amptec heeft geïmplementeerd ter bescherming van Klantgegevens. De verdeling van verantwoordelijkheden tussen Amptec en de Klant met betrekking tot gegevensbeheer en beveiligingsacties wordt primair uiteengezet in de verantwoordelijkheidsmatrix, opgenomen in de Master Service Agreement (hierna: "**MSA**"), en aangevuld in de toepasselijke Statement(s) of Work (hierna: "**SoW**").

Amptec is niet aansprakelijk voor enige acties of beslissingen die de Klant op eigen initiatief neemt, ongeacht of deze al dan niet uitdrukkelijk zijn opgenomen in de MSA of SoW.

2. Data Security Programma, Policies en Controls.

De Service Provider en zijn personeel (zoals hieronder gedefinieerd en hierna: “Service Provider Personeel”) mogen enkel toegang verkrijgen tot Klantactiva wanneer dit noodzakelijk is voor de uitvoering van de Diensten, binnen de grenzen van hun functie en op basis van een legitieme noodzaak. Het is de Service Provider en zijn Service Provider personeel niet toegestaan om Klantactiva te verwerken of toegankelijk te maken voor onbevoegde personen of entiteiten binnen zijn organisatie of onder zijn controle.

De Service Provider moet gedurende de looptijd van de overeenkomst passende fysieke, elektronische en organisatorische beveiligingsmaatregelen implementeren en onderhouden, gebaseerd op een risicogestuurde aanpak en in overeenstemming met algemeen aanvaarde best practices en internationale normen, waaronder ISO 27001:2022, de CIS Critical Security Controls, de NIST Standards en richtlijnen van de Cloud Security Alliance.

Deze maatregelen moeten ertoe strekken Klantactiva te beschermen tegen ongeoorloofde toegang, gebruik, vernietiging, verlies, openbaarmaking, verwerking of onrechtmatige wijziging.

De Service Provider verklaart, garandeert en verbindt zich ertoe dat zijn beveiligingsbeleid en -maatregelen ten minste voorzien in de elementen zoals uiteengezet in de volgende bepalingen van deze DSA.

2.1 Information Security Programma (iSMS).

- De Service Provider heeft een schriftelijk informatiebeveiligingsbeleid geïmplementeerd dat beschikbaar is voor alle huidige werknemers, aannemers en ander personeel (“Service Provider Personeel”);
- De Service Provider heeft rollen en verantwoordelijkheden toegewezen voor informatiebeveiliging;
- Het informatiebeveiligingsbeleid van de Service Provider wordt ten minste jaarlijks beoordeeld en goedgekeurd door de uitvoerende leiding van de Service Provider;
- De Service Provider heeft een gedocumenteerde standaard en procedures voor veilige toegang op afstand tot klantgegevens en/of Service Provider- of Klantsystemen. Deze procedures omvatten het gebruik van Service Provider-apparaten, inclusief mobiele apparaten, en maken gebruik van passende beveiligingsmaatregelen zoals multi-factor authenticatie (“MFA”) en versleuteling, in overeenstemming met relevante normen en best practices.

2.2 Human Resources Security.

- De Service Provider zorgt ervoor dat alle eigen personeelsleden, evenals ingehuurde externe medewerkers die toegang hebben tot Klantactiva, jaarlijks een verplichte beveiligingsbewustzijnstraining volgen;
- Deze training moet minstens de basisprincipes van informatiebeveiliging, gegevensbescherming, incidentherkenning en verantwoordelijk gebruik van systemen behandelen, en moet afgestemd zijn op het risicoprofiel van de uitgevoerde werkzaamheden.

2.3 Assets en Data Beheer.

- De Service Provider moet Klantgegevens beschermen in overeenstemming met alle schriftelijk overeengekomen informatiebeveiligingsbeleid, procedures en protocollen tussen de Partijen;
- De Service Provider moet ervoor zorgen dat al het Service Provider Personeel op de hoogte is van en voldoet aan het acceptabel gebruiksbeleid van de Service Provider of vergelijkbare beleidslijnen. Deze beleidslijnen moeten bepalingen bevatten die de vereisten en verantwoordelijkheden definiëren voor het gebruik van gegevens, inhoud en/of systemen;
- De Service Provider mag geen toegang verkrijgen tot, opslaan, cachen, downloaden of verwerken van Klantgegevens op een apparaat of systeem dat niet wordt beschermd door de firewall van de Service Provider;
- De Service Provider moet beschikken over en voldoen aan gedocumenteerde procedures voor de veilige verwijdering van Klantgegevens in overeenstemming met de overeengekomen bewaartermijnen en toepasselijke wet- en regelgeving
- De Service Provider moet een actueel en volledig inventaris bijhouden van alle informatie- en andere gerelateerde activa die Klantgegevens verwerken, opslaan of verzenden. Elk actief moet een toegewezen eigenaar hebben die verantwoordelijk is voor het beheer gedurende de volledige levenscyclus van het actief;
- De Service Provider moet ervoor zorgen dat alle informatie- en gerelateerde activa correct worden geclassificeerd op basis van hun gevoeligheid en waarde, en dat passende beveiligingsmaatregelen worden toegepast die overeenkomen met hun classificatie;
- De Service Provider moet procedures implementeren voor het veilig retourneren of verwijderen van activa die Klantgegevens bevatten of toegang daartoe bieden, bij beëindiging van de dienstverlening of wanneer het actief niet langer nodig is.

2.4 Toegangscontrole.

- De Service Provider moet de toegang tot Klantactiva beperken tot uitsluitend geautoriseerd Service Provider Personeel, op basis van het principe van 'need-to-know' en het minimale privilege. Toegangsrechten dienen te worden toegekend via een rolgebaseerd toegangsmodel met duidelijke scheiding van taken. Deze toegangsrechten moeten ten minste elk kwartaal worden beoordeeld en aangepast indien nodig;
- De Service Provider moet Multi-Factor Authentication ("MFA") vereisen en gebruik maken van een Virtual Private Network (VPN) of Zero-Trust Access (ZTA) om op afstand toegang te krijgen tot Service Provider Systemen, Service Provider Faciliteiten, en alle Klantactiva;
- De Service Provider moet ervoor zorgen dat bij beëindiging van het dienstverband of wijziging van de rol van Service Provider Personeel, de toegang tot systemen die Klantgegevens bevatten onmiddellijk wordt ingetrokken;
- De Service Provider moet unieke gebruikers-ID's toewijzen aan alle gebruikers en het gebruik van gedeelde accounts verbieden, tenzij de infrastructuur of software aan de klantzijde dit anders vereist of het technisch niet mogelijk is om onderscheid te maken;
- De Service Provider moet industriestandaarden en best practices afdwingen voor sterke wachtwoorden en levenscyclusbeheer voor alle gebruikers, inclusief regelmatige wijzigingen en het voorkomen van hergebruik van wachtwoorden;
- De Service Provider moet bevoorrechte accounts ten minste elk kwartaal beoordelen om te bevestigen dat rechten en privileges passend zijn voor de toegewezen rollen;
- De Service Provider mag geen e-mails van Klantaccounts doorsturen, noch automatisch noch handmatig, naar niet-Klantaccounts, tenzij dit uitdrukkelijk is toegestaan door de Klant.

2.5 Physical Security.

Indien Klantgegevens worden opgeslagen in een datacenter dat eigendom is van of wordt beheerd door de Service Provider, moet de Service Provider fysieke beveiligingsmaatregelen implementeren en onderhouden om Klantgegevens en het netwerk van de Service Provider te beschermen. Deze maatregelen omvatten onder andere:

- Beheerde toegang tot gebieden waar Klantgegevens worden opgeslagen, verwerkt of verzonden, met behulp van badges en toegangslogboeken;

- Fysieke bescherming en onderhoud van de apparatuur van de Service Provider om verlies, openbaarmaking, schade, diefstal of compromittering van Klantgegevens te voorkomen;
- Veilige verwijdering van apparatuur en fysieke en elektronische media die Klantgegevens bevatten, in overeenstemming met de overeengekomen bewaartermijnen en toepasselijke wet- en regelgeving.

Indien de opslag van Klantgegevens plaatsvindt in een datacenter dat eigendom is van of wordt beheerd door een onderaannemer van de Service Provider, moet de Service Provider ervoor zorgen dat de onderaannemer vergelijkbare fysieke beveiligingsmaatregelen heeft geïmplementeerd en onderhoudt.

2.6 Public Cloud Services.

Indien de Service Provider gebruikmaakt van openbare clouddiensten voor de opslag of verwerking van Klantgegevens, moet de Service Provider de volgende beveiligingsmaatregelen implementeren en onderhouden, in overeenstemming met industriestandaarden en best practices:

- Multi-Factor Authenticatie (MFA): De Service Provider moet MFA vereisen voor alle administratieve gebruikersaccounts die toegang hebben tot de clouddiensten van de Service Provider, ter voorkoming van ongeautoriseerde toegang;
- Scheidingsprincipes en Sleutelbeheer: De Service Provider moet logische scheiding van cloudomgevingen implementeren om Klantgegevens te isoleren van andere gegevens, inclusief die van andere klanten van de Service Provider. Dit omvat het gebruik van sterke sleutelbeheerpraktijken, zoals het toepassen van het principe van scheiding van taken (Separation of Duties) bij sleutelbeheer, zodat geen enkele gebruiker volledige toegang heeft tot zowel encryptie- als decryptiesleutels;
- Encryptie van Klantgegevens: De Service Provider moet industriestandaard encryptie toepassen op alle Klantgegevens:
    - Tijdens transmissie: Alle Klantgegevens moeten worden versleuteld tijdens overdracht over netwerken naar, van en binnen de openbare clouddienst, bijvoorbeeld door het gebruik van Transport Layer Security (TLS);
    - In rust: Alle Klantgegevens die zijn opgeslagen binnen de openbare clouddienst moeten worden versleuteld met behulp van sterke encryptie-algoritmen, zoals AES-256, en de encryptiesleutels moeten worden beheerd via een robuust sleutelbeheersysteem (Key Management System, KMS).

- Monitoring en Logging: De Service Provider moet continue monitoring en logging implementeren voor alle activiteiten binnen de cloudomgevingen, inclusief toegangs- en wijzigingslogboeken, om verdachte activiteiten te detecteren en te reageren op beveiligingsincidenten.

De Service Provider moet regelmatig beoordelingen uitvoeren van de cloudbeveiligingsmaatregelen en -configuraties om ervoor te zorgen dat ze blijven voldoen aan de toepasselijke beveiligingsnormen en dat Klantgegevens adequaat worden beschermd.

2.7 Operations Security.

De Service Provider moet een log- en monitoringstandaard implementeren en handhaven die voldoet aan de volgende vereisten:

- Gebeurtenislogboek: Het systeem moet gebeurtenissen registreren zoals:
    - Gebruikerslogin en -logout;
    - Ongeldige inlogpogingen;
    - Bevoorrechte toegang en activiteiten, inclusief gegevensuitvoer, wijzigingen en beveiligingsbeheer;
    - Toegang tot logboeken door de Klant en Klant Affiliates;
    - Stoppen of pauzeren van logging/logproductie.
- Logbeveiliging: Logbestanden moeten worden beschermd tegen ongeautoriseerde toegang, wijziging en verwijdering. Toegang tot logbestanden moet beperkt zijn tot geautoriseerd personeel en moet worden gecontroleerd en gelogd;
- Logbewaring: Logbestanden moeten worden bewaard gedurende een periode die is overeengekomen tussen de Service Provider en de Klant, en in overeenstemming met toepasselijke wet- en regelgeving.
- Monitoring: De Service Provider moet continue monitoring implementeren om verdachte activiteiten en beveiligingsincidenten te detecteren. Monitoring moet worden uitgevoerd in overeenstemming met de overeengekomen procedures en frequenties.
- Toegankelijkheid voor de Klant: De Klant en diens gelieerde ondernemingen moeten toegang hebben tot relevante logbestanden en monitoringgegevens, zoals overeengekomen in de overeenkomst tussen de Partijen.

2.8 Network Security.

De Service Provider moet de informatiestroom op een gelaagde basis monitoren, detecteren en beperken, inclusief maar niet beperkt tot het gebruik van de volgende beveiligingsmaatregelen:

- Netwerksegmentatie en firewallconfiguratie: Implementatie van netwerksegmentatie en veilige configuratie van firewalls in het hele netwerk van de Service Provider of Virtual Local Area Networks (vLANs), in overeenstemming met industriestandaarden en best practices;
- Web Application Firewalls (WAFs): Alle extern gerichte applicaties moeten worden beschermd met Web Application Firewalls om applicatielaag-aanvallen te detecteren en te blokkeren;
- Demilitarized Zone (DMZ): Onderhoud van een Demilitarized Zone om het interne netwerk en activa te beschermen die diensten leveren aan de Klant en diens gelieerde ondernemingen, waarbij alleen noodzakelijk verkeer wordt toegestaan;
- Intrusion Detection and Prevention Systems (IDS/IPS): Implementatie van inbraakdetectie- en/of preventiesystemen bij inlaatpunten om verdachte activiteiten te detecteren en te voorkomen.

Deze maatregelen moeten regelmatig worden beoordeeld en bijgewerkt om te zorgen voor voortdurende bescherming tegen opkomende bedreigingen en in overeenstemming met de nieuwste beveiligingsnormen.

2.9 Telewerken.

Indien de Service Provider of diens Personeel diensten uitvoert vanaf externe locaties, dient de Service Provider ervoor te zorgen dat aan de volgende vereisten wordt voldaan:

- Afgeschermde werkomgeving: Telewerken mag uitsluitend plaatsvinden in een afgeschermde ruimte (bijv. een privéwoning) en met inachtneming van de “clean desk”-normen. De locatie moet minimale blootstelling aan andere (niet tot de Service Provider behorende) personen garanderen;
- Logging en monitoring: Voor geautoriseerde systemen van de Service Provider (die voldoen aan de hier gespecificeerde normen) moet uitgebreide logging zijn ingeschakeld. Deze logboeken moeten op verzoek van de Klant beschikbaar worden gesteld om potentiële beveiligingsincidenten met Klantgegevens te onderzoeken;
- Gebruik van Geautoriseerde Apparaten: Personeel van de Service Provider dat deelneemt aan het telewerkprogramma mag uitsluitend apparaten gebruiken die geautoriseerd zijn volgens het beveiligingsprogramma van de Service Provider (“Geautoriseerde Apparaten”) en die voldoen aan de volgende normen:

- Elk Geautoriseerd Apparaat moet beveiligingsupdates ontvangen volgens hetzelfde schema als apparaten op locatie;
- Geautoriseerde Apparaten moeten voldoen aan de hier vermelde versleutelingsnormen;
- Personeel van de Service Provider mag geen apparaten gebruiken met administratieve rechten, toegang via remote desktop protocol of rechten om diensten of privileges te wijzigen, tenzij dit vereist is voor hun functie;
- Geautoriseerde Apparaten moeten worden gehard volgens dezelfde of strengere normen als de systemen in de faciliteiten van de Service Provider;
- Technische controles moeten voorkomen dat Klantgegevens lokaal worden opgeslagen op Geautoriseerde Apparaten;
- Geautoriseerde Apparaten moeten een beveiligde, vergrendelende schermbeveiliging hebben die na maximaal vijftien (15) minuten inactiviteit authenticatie vereist;
- Geautoriseerde Apparaten moeten geconfigureerd zijn met een altijd-actieve VPN;
- De VPN mag niet door gebruikers uitgeschakeld kunnen worden;
- Al het netwerkverkeer moet verplicht via de VPN verlopen;
- Multi-Factor Authenticatie (MFA) is vereist voor toegang tot de VPN;
- Alle toegang tot toepassingen van de Klant en diens gelieerde ondernemingen moet verlopen via een beveiligde virtuele desktopinfrastructuur (Amptec RAS) of gelijkwaardige technologie, waarbij directe toegang tot toepassingen en gegevens vanaf Geautoriseerde Apparaten niet is toegestaan:
    - RAS mag geen kopiëren/plakken toelaten van/naar Geautoriseerde Apparaten;
    - Screenshots moeten uitgeschakeld zijn op de VDI.

- Beëindiging van telewerken: De Klant kan, naar eigen goeddunken, verzoeken dat specifiek personeel van de Service Provider stopt met werken op afstand. De Service Provider zal te goeder trouw samenwerken met de Klant om het betreffende personeel zo snel mogelijk terug te laten keren naar de faciliteiten van de Service Provider, in overeenstemming met de lokale vereisten en het beleid van de Service Provider, indien van toepassing.

2.10 Service Provider Management.

De Service Provider is verantwoordelijk voor het waarborgen dat alle personeelsleden en onderaannemers die toegang hebben tot, gebruikmaken van systemen en faciliteiten van de Service Provider, evenals Klantactiva, voldoen aan de vereisten van deze Data Security Agreement (DSA).

De Service Provider moet informatiebeveiligingsovereenkomsten afsluiten met onderaannemers die toegang hebben tot Klantactiva of diensten leveren die resulteren in toegang tot de systemen of faciliteiten van de Service Provider. Deze overeenkomsten moeten in wezen gelijkwaardig zijn aan deze DSA en ten minste de volgende elementen bevatten:

- Beveiligingsverplichtingen: Duidelijke bepalingen over de beveiligingsverplichtingen van de onderaannemer, inclusief naleving van relevante beveiligingsnormen en -praktijken;
- Toegangscontrole: Specificatie van toegangsrechten en -beperkingen met betrekking tot Klantactiva en systemen van de Service Provider;
- Incidentrespons: Procedures voor het melden en afhandelen van beveiligingsincidenten die de onderaannemer betreffen;
- Audits en beoordelingen: Het recht van de Service Provider om audits en beoordelingen uit te voeren om de naleving van de beveiligingsvereisten door de onderaannemer te verifiëren;
- Beëindiging van toegang: Bepalingen over het beëindigen van de toegang van de onderaannemer tot Klantactiva en systemen van de Service Provider bij beëindiging van de overeenkomst of bij niet-naleving van de beveiligingsvereisten.

De Service Provider moet regelmatig de naleving van deze overeenkomsten door onderaannemers monitoren en beoordelen, en passende maatregelen nemen bij constatering van niet-naleving.

2.11 Incident Notificatie en Incident Response.

De Service Provider moet bij een vermoedelijk of bevestigd beveiligingsincident de best practices uit de sector volgen. De Service Provider moet ten minste:

- Melding aan de Klant: Een dergelijk beveiligingsincident zo snel mogelijk na de ontdekking gedetailleerd melden aan de Klant en onmiddellijk passende corrigerende en preventieve maatregelen nemen;
- Openbaarmaking: Geen enkele melding doen of het incident op enige wijze openbaar maken indien dit Klantactiva betreft of raakt, zonder voorafgaande schriftelijke toestemming van de Klant, tenzij wettelijk vereist;

- Onderzoek: Een snelle en grondige onderzoek uitvoeren naar het beveiligingsincident, waaronder – indien nodig en uitsluitend naar goeddunken van de Klant – het inschakelen van een onafhankelijke derde partij of partijen;
- Rapportage: Een rapport aan de Klant verstrekken waarin details staan over het beveiligingsincident, de bekende en potentiële gevolgen voor Klantactiva, de grondoorzaak, en de genomen maatregelen om het incident op te lossen en herhaling te voorkomen;
- Samenwerking: Meewerken aan elk onderzoek naar het beveiligingsincident dat door de Klant wordt verzocht.

2.12 Naleving en Beveiligings Assessments.

- De Service Provider moet voldoen aan alle toepasselijke wet- en regelgeving, inclusief het waarborgen dat het beveiligingsprogramma alle maatregelen implementeert die door de wet- en regelgeving worden vereist.
- Op verzoek van de Klant bezorgt de Service Provider jaarlijks een ondertekend exemplaar van zijn meest recente beveiligingsbeoordelingsrapport, vergezeld van een plan waarin de vastgestelde tekortkomingen worden gedocumenteerd en de voorziene corrigerende acties worden gespecificeerd, inclusief termijnen en verantwoordelijken.
- De Service Provider moet, op eigen kosten, binnen negentig (90) dagen na ontvangst van enig Auditrapport, alle kritieke of ernstige bevindingen corrigeren. Externe audits op vraag van de klant, zullen eventueel ten laste zijn van de klant.

2.13 Beëindiging van de Overeenkomst

Indien de Service Provider wezenlijk tekortschiet in de naleving van deze Data Security Agreement, een beveiligingsincident ondergaat met een wezenlijke impact op de Klant en/of diens Gelieerde Ondernemingen, of indien de Klant een wezenlijke verslechtering vaststelt in de beveiligingsmaatregelen van de Service Provider, heeft de Klant het recht om deze Overeenkomst, alsook alle onderliggende Statements of Work, werkopdrachten of vergelijkbare documentatie, zonder enige boete of schadevergoeding, te beëindigen mits een opzegtermijn van dertig (30) dagen.

De beëindiging treedt in werking op de datum vermeld in de schriftelijke kennisgeving. Bij afloop of beëindiging van de Overeenkomst is de Service Provider verplicht om alle Klantgegevens, naar keuze van de Klant, terug te bezorgen of op veilige wijze te vernietigen. De Service Provider dient daartoe gangbare best practices en sectorale normen toe te passen bij de vernietiging of teruggave van de Klantgegevens, binnen een termijn van negentig (90) dagen na ontvangst van de schriftelijke kennisgeving van beëindiging of afloop van de Overeenkomst, en/of enige toepasselijke Bestelbon of Statement of Work, tenzij in de Overeenkomst, de Bestelbon of de Statement of Work een

kortere termijn is bepaald. Deze verplichting heeft betrekking op alle Klantgegevens, ongeacht of deze zijn opgeslagen op locatie, in datacenters, in cloudomgevingen of op back-ups.

Na afloop of beëindiging van de Overeenkomst moet de Service Provider bevestigen dat zijn toegang, en die van al het personeel onder zijn verantwoordelijkheid, tot alle Klantactiva is ingetrokken of beëindigd. Op verzoek van de Klant moet de Service Provider bovendien schriftelijk bewijs en certificering van de beëindiging of intrekking van dergelijke toegangsrechten verstrekken.

3. Bestaan van de overeenkomst.

Alle bepalingen van deze Data Security Agreement vervallen van rechtswege zodra de Service Provider alle Klantgegevens heeft geretourneerd of vernietigd, en de toegang tot de Klantactiva volledig heeft beëindigd, dit in overeenstemming met de voorwaarden zoals uiteengezet in deze Data Security Agreement en de toepasselijke Managed Services Overeenkomst.

4. Wijzigingen van de Overeenkomst.

Geen enkele bepaling van deze Data Security Agreement mag worden gewijzigd, aangevuld of opgeheven dan middels een schriftelijke overeenkomst die door beide Partijen uitdrukkelijk is ondertekend.

5. Aanvaarding van de Overeenkomst.

Door ondertekening van een Bestelbon, Statement of Work of enig ander document waarin wordt verwezen naar deze Data Security Agreement, bevestigen beide partijen uitdrukkelijk dat zij de bepalingen en voorwaarden van deze overeenkomst volledig hebben gelezen, begrepen en aanvaarden.

Deze aanvaarding impliceert dat alle verplichtingen, verantwoordelijkheden en rechten zoals uiteengezet in deze Data Security Agreement bindend zijn voor beide partijen, en integraal deel uitmaken van de contractuele relatie tussen de partijen.

Indien enige bepaling van deze Data Security Agreement strijdig is met bepalingen in andere documenten die deel uitmaken van de overeenkomst tussen de partijen, prevaleren de bepalingen van deze Data Security Agreement, tenzij uitdrukkelijk schriftelijk anders is overeengekomen door beide partijen.

6. Aansprakelijkheid en Schadeloosstelling.

6.1 Beperking van Aansprakelijkheid.

De Service Provider, diens bestuurders, werknemers, vertegenwoordigers of gelieerde ondernemingen kunnen in geen geval aansprakelijk worden gesteld voor enige schade, verliezen, kosten of boetes, direct of indirect voortvloeiend uit een cybersecurity-incident,

datalek, onrechtmatige toegang, systeeminbreuk of gelijkwaardig beveiligingsvoorval, tenzij in geval van opzettelijke fout of bedrog door de Service Provider. Deze uitsluiting geldt eveneens voor schade veroorzaakt door derde partijen, tenzij de Service Provider contractueel verantwoordelijk wordt gehouden ingevolge uitdrukkelijk schriftelijke afspraken.

6.2 Uitsluiting van Gevolgschade.

De Service Provider is in geen geval aansprakelijk voor enige vorm van indirecte, incidentele, bijzondere of gevolgschade. Dit omvat onder meer winstderving, verlies van omzet, reputatieschade, verminderde commerciële waarde, verlies van verwachte besparingen, verlies of beschadiging van gegevens, alsook onderbreking of stilstand van bedrijfsactiviteiten. Deze uitsluiting geldt ongeacht de oorzaak of rechtsgrond van de schade, en ongeacht of de mogelijkheid ervan vooraf aan de Service Provider werd meegedeeld. Zij geldt eveneens ongeacht of de aansprakelijkheid gebaseerd is op een contractuele, buitencontractuele of andere rechtsgrond, zelfs indien de mogelijkheid van dergelijke schade vooraf aan de Service Provider werd meegedeeld.

6.3 Schadeloosstelling door de Klant.

De Klant verbindt zich ertoe de Service Provider, evenals diens werknemers, bestuurders, vertegenwoordigers en gelieerde ondernemingen, integraal te vrijwaren, verdedigen en schadeloos te stellen tegen alle aanspraken, vorderingen, verliezen, schade, kosten en uitgaven (inclusief redelijke advocatenkosten) die voortvloeien uit of verband houden met:

- Het niet of onvoldoende implementeren door de Klant van door de Service Provider aanbevolen beveiligingsmaatregelen of procedures;
- Enige nalatigheid, fout, schending van contractuele verplichtingen of onrechtmatige daad begaan door de Klant of diens aangestelden;
- Beslissingen of handelingen genomen door de Klant op basis van advies, analyses, aanbevelingen of rapporten verstrekt door de Service Provider, waarbij de Service Provider niet aansprakelijk is tenzij in geval van opzettelijke fout of bedrog.

6.4 Professional Judgment Disclaimer.

De Klant erkent dat de door de Service Provider geleverde diensten van adviserende en ondersteunende aard zijn en gestoeld op professionele beoordeling binnen een voortdurend evoluerend technologisch domein. Hoewel de Service Provider redelijke inspanningen levert om risico's te beperken en adequate aanbevelingen te formuleren, ligt de eindverantwoordelijkheid voor de genomen beslissingen en de implementatie van maatregelen uitsluitend bij de Klant.

7. Force Majeure.

Geen van beide Partijen is aansprakelijk voor enige tekortkoming of vertraging in de uitvoering van haar verplichtingen onder deze Data Security Agreement, voor zover deze het gevolg is van overmacht. Onder overmacht wordt verstaan elke gebeurtenis of omstandigheid die buiten de redelijke controle van een Partij valt, die niet te wijten is aan haar fout of nalatigheid, en die de uitvoering van haar contractuele verplichtingen tijdelijk of blijvend verhindert. Dit omvat onder meer, maar is niet beperkt tot, natuurrampen, oorlog, oproer, terrorisme, overheidsmaatregelen, pandemieën, epidemieën, stroom- of netwerkstoringen, uitval van infrastructuur, stakingen en andere gebeurtenissen van soortgelijke aard.

De Partij die door overmacht wordt getroffen, stelt de andere Partij onverwijld schriftelijk op de hoogte van het bestaan, de aard, de vermoedelijke duur en de gevolgen van de overmachtssituatie. De uitvoering van de overeenkomst wordt geschorst voor de duur van de overmacht, zonder dat hierdoor een recht op schadevergoeding ontstaat voor de andere Partij. De getroffen Partij zal alle redelijke maatregelen treffen om de gevolgen van de overmacht tot een minimum te beperken en de uitvoering van haar verplichtingen te hervatten zodra dit redelijkerwijs mogelijk is.

Indien de overmachtssituatie langer dan zestig dagen aanhoudt, kan elke Partij de overeenkomst geheel of gedeeltelijk beëindigen via schriftelijke kennisgeving, zonder rechterlijke tussenkomst en zonder enige schadevergoeding verschuldigd te zijn.

8. Looptijd en Beëindiging.

Deze Data Security Agreement treedt in werking op de datum van ondertekening door beide Partijen of, indien eerder, op de datum waarop in een Bestelbon, Statement of Work of ander contractueel document expliciet naar deze bepalingen wordt verwezen. Zij blijft van kracht zolang tussen Partijen een geldige contractuele relatie bestaat, hetzij krachtens een hoofdovereenkomst, hetzij krachtens een Bestelbon of Statement of Work, behoudens vroegtijdige beëindiging overeenkomstig onderstaande bepalingen.

De Klant heeft het recht deze Data Security Agreement, evenals alle onderliggende Statements of Work, werkopdrachten of andere toepasselijke documenten, zonder enige schadevergoeding of boete, te beëindigen mits een opzegtermijn van dertig (30) dagen, indien de Service Provider wezenlijk tekortschiet in de naleving van deze Data Security Agreement, indien de Service Provider het voorwerp uitmaakt van een beveiligingsincident met wezenlijke impact op de Klant of diens gelieerde ondernemingen, of indien de Klant een substantiële verslechtering vaststelt in de beveiligingsmaatregelen van de Service Provider. De beëindiging wordt van kracht op de datum vermeld in de schriftelijke kennisgeving van de Klant.

Bij beëindiging of afloop van deze overeenkomst is de Service Provider gehouden om, naar keuze van de Klant, alle Klantgegevens terug te bezorgen of op veilige wijze te vernietigen.

De Service Provider past daarbij algemeen aanvaarde normen en beveiligingspraktijken toe, binnen een termijn van maximaal negentig (90) dagen na ontvangst van de schriftelijke kennisgeving, tenzij een kortere termijn is bepaald in een toepasselijke Bestelbon of Statement of Work. Deze verplichting geldt ongeacht de opslaglocatie van de Klantgegevens, inclusief on-premises, in datacenters, cloudomgevingen of back-ups.

De Service Provider dient na beëindiging of afloop schriftelijk te bevestigen dat zijn toegang tot Klantactiva, evenals die van alle onder zijn verantwoordelijkheid werkzame personen, volledig werd beëindigd of ingetrokken. Op verzoek van de Klant moet de Service Provider tevens schriftelijk bewijs of certificering van deze beëindiging of intrekking overleggen.

De bepalingen van deze Data Security Agreement die naar hun aard bestemd zijn om voort te blijven gelden, blijven onverminderd van kracht na beëindiging. Dit omvat onder meer de bepalingen inzake vertrouwelijkheid, aansprakelijkheid, schadeloosstelling en toepasselijk recht.

9. Overdraagbaarheid.

Geen van beide Partijen mag deze Data Security Agreement, noch enige rechten of verplichtingen die eruit voortvloeien, geheel of gedeeltelijk overdragen, delegeren of uitbesteden aan een derde partij zonder voorafgaande schriftelijke toestemming van de andere Partij. Een dergelijke toestemming mag niet onredelijk worden geweigerd of vertraagd.

Onverminderd het voorgaande, is het de Klant toegestaan deze overeenkomst, zonder voorafgaande toestemming van de Service Provider, over te dragen aan een gelieerde onderneming of in het kader van een fusie, overname, reorganisatie of overdracht van activa, op voorwaarde dat de verkrijgende entiteit schriftelijk bevestigt gebonden te zijn aan de bepalingen van deze Data Security Agreement. De Service Provider blijft in dat geval volledig aansprakelijk voor de correcte uitvoering van zijn verplichtingen onder deze overeenkomst, ook indien deze geheel of gedeeltelijk door een derde worden uitgevoerd.

Elke overdracht in strijd met deze bepaling is van rechtswege nietig en zonder gevolg.

10. Volledige Overeenkomst.

Deze Data Security Agreement vormt, samen met de hoofdovereenkomst, toepasselijke Bestelbonnen, Statements of Work en andere schriftelijke documenten waarin uitdrukkelijk naar deze bepalingen wordt verwezen, de volledige overeenkomst tussen Partijen met betrekking tot de beveiliging van gegevens, Klantactiva en informatieverwerking.

Zij vervangt alle voorafgaande mondelinge of schriftelijke afspraken, verklaringen of voorstellen inzake hetzelfde onderwerp. Geen enkele bepaling uit enig ander contractueel

document doet afbreuk aan deze Data Security Agreement, tenzij door beide Partijen uitdrukkelijk en schriftelijk overeengekomen.

11. Toepasselijk Recht en Bevoegde Rechtbank.

Deze Data Security Agreement wordt uitsluitend beheerst door het Belgisch recht, met uitsluiting van het internationaal privaatrecht en het Weens Koopverdrag.

Alle geschillen die voortvloeien uit of verband houden met deze overeenkomst behoren tot de exclusieve bevoegdheid van de Ondernemingsrechtbank Antwerpen, afdeling Tongeren. Partijen verbinden zich ertoe elk geschil in eerste instantie te trachten op te lossen via schriftelijk overleg binnen een redelijke termijn, onverminderd het recht om voorlopige maatregelen te vorderen.

12. Appendix – Gebruikte Terminologie.

"Toepasselijke wetgeving" betekent alle toepasselijke wetten, regels, voorschriften en normen in elk rechtsgebied waarin de Diensten worden geleverd of waar Klantgegevens of Vertrouwelijke Informatie kunnen worden opgeslagen of verwerkt. Dit omvat onder meer wetgeving inzake privacy, gegevensbescherming en informatiebeveiliging, waaronder begrepen, maar niet beperkt tot, de Algemene Verordening Gegevensbescherming en nationale uitvoeringswetten.

"**Vertrouwelijke informatie**" betekent alle informatie of materiaal, ongeacht de vorm (schriftelijk, mondeling, elektronisch of anderszins) en de drager, die aan de ontvangende partij wordt verstrekt of beschikbaar wordt gesteld onder omstandigheden waaruit redelijkerwijs blijkt dat deze vertrouwelijk is. Dit geldt ongeacht of dergelijke informatie uitdrukkelijk is gemarkeerd als vertrouwelijk of eigendomsrechtelijk. Het omvat ook informatie die de verstrekkende partij verkrijgt van een gelieerde of derde, en die door die partij als vertrouwelijk wordt beschouwd. De partijen komen overeen dat deze Beveiligingsovereenkomst en de bepalingen ervan Vertrouwelijke Informatie vormen. Klantgegevens en Persoonsgegevens worden beschouwd als Vertrouwelijke Informatie van de Klant en/of diens gelieerde ondernemingen, behoudens voor zover deze informatie reeds publiek toegankelijk is zonder schending van deze Overeenkomst.

"Klantactiva" betekent en omvat alle Klantgegevens, Klantsystemen en Klantfaciliteiten.

"**Klantgegevens**" betekent alle gegevens, documenten, informatie of materiaal in eender welk formaat of medium, die (i) door of namens de Klant of diens gelieerde entiteiten aan de Service Provider zijn verstrekt of ter beschikking zijn gesteld, (ii) door de Service Provider worden verzameld, gegenereerd of verwerkt in het kader van de uitvoering van de Diensten, (iii) voortvloeien uit of verband houden met het gebruik van de diensten, systemen of infrastructuur van de Service Provider door de Klant of diens gelieerde entiteiten, of (iv) zijn afgeleid van de voorgaande categorieën. Klantgegevens omvatten tevens alle afgeleide werken, kopieën, bewerkingen, samenvattingen, analyses,

uittreksels of reproducties van dergelijke gegevens. Persoonsgegevens en Vertrouwelijke Informatie van de Klant worden geacht Klantgegevens te zijn.

"**Klantfaciliteit(en)**" Elke fysieke locatie, technische installatie of gebouw, ongeacht eigendomsstructuur of operationele aansturing, die door de Klant of diens gelieerde entiteiten wordt gebruikt in het kader van of in verband met de levering, ondersteuning of beveiliging van de Diensten.

"**Klantsystemen**" Systemen, netwerken, hardware, software, toepassingen, databanken en andere informatietechnologische middelen die eigendom zijn van, beheerd worden door of ter beschikking staan van de Klant of diens gelieerde entiteiten, al dan niet via een derde partij. Deze systemen maken integraal deel uit van de technische omgeving waarin of waarmee de Diensten worden geleverd, ondersteund of beveiligd.

"**Persoonsgegevens"** betekent: (1) alle informatie die betrekking heeft op een geïdentificeerde of identificeerbare natuurlijke persoon, apparaat of huishouden, of (2) alle informatie die wordt gedefinieerd als “persoonlijk identificeerbare informatie”, “persoonsinformatie”, “persoonsgegevens” of vergelijkbare termen zoals gedefinieerd onder toepasselijke wetgeving.

"**Verwerken" of "Verwerking**" betekent elke handeling of geheel van handelingen met betrekking tot Klantgegevens, al dan niet met behulp van geautomatiseerde middelen, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, aanpassen, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorgifte, verspreiden, beschikbaar stellen, aligneren, combineren, beperken, wissen of vernietigen.

"**Beveiligingsincident**" Elke gebeurtenis waarbij sprake is van, of een gegronde verdenking bestaat van, ongeoorloofde of onrechtmatige toegang tot, wijziging van, verlies van, openbaarmaking van of verstoring van de integriteit, vertrouwelijkheid of beschikbaarheid van Klantgegevens, Klantactiva of systemen beheerd door de Service Provider in het kader van deze Overeenkomst. Hieronder vallen tevens inbreuken op beveiligingsmaatregelen die als datalek kwalificeren onder de toepasselijke wetgeving inzake gegevensbescherming.

"**Diensten"** verwijst naar de diensten die onder de Overeenkomst worden geleverd, met inbegrip van hostingdiensten, ondersteuning, professionele diensten, clouddiensten en andere prestaties zoals gespecificeerd in het relevante bestelformulier en/of statement of work.

"Faciliteiten van de Service Provider" betekent elke locatie of infrastructuur die door de Service Provider wordt gebruikt voor de uitvoering van de Diensten of voor de opslag, verwerking, transmissie of toegang tot Vertrouwelijke Informatie van de Klant, ongeacht of deze wordt geëxploiteerd door de Service Provider of door een derde namens hem.

"Systemen van de Service Provider" betekent de systemen, netwerken, hardware, software, toepassingen en overige technologieën die door of namens de Service Provider worden gebruikt voor het verlenen van de Diensten of het verwerken van Vertrouwelijke Informatie van de Klant, ongeacht of deze onder het beheer van de Service Provider vallen of worden gehost door een derde partij.

"Gelieerde ondernemingen" betekent elke entiteit die direct of indirect zeggenschap uitoefent over, wordt gecontroleerd door of onder gezamenlijke zeggenschap staat met een Partij, waarbij “zeggenschap” wordt gedefinieerd als het recht om, direct of indirect, de leiding of het beleid van een entiteit te bepalen door middel van eigendom van stemgerechtigde effecten, overeenkomst of anderszins.

ACCORD SUR LA SÉCURITÉ DES DONNÉES

Entre:

AMPTEC BV, société privée à responsabilité limitée de droit belge, dont le siège social est établi à Bremakker 45, 3740 Bilzen, et dont le numéro d'entreprise est le 0442.333.460, représentée par Bart Willems directeur, ci-après dénommée le « **Prestataire de services** » ou « **Amptec** » ;

et le **CLIENT** ci-après dénommé le « **Client** »,

Le Prestataire et le Client sont ci-après dénommés individuellement une « **Partie** » et collectivement les « **Parties** ».

1. Portée.

Dans la mesure où le Prestataire de services a accès aux Systèmes du Client ou aux Installations du Client, ou traite des Données du Client, des Informations personnelles ou des Informations confidentielles (telles que définies à l'Article 12), en raison des Services fournis par le Prestataire de services, le présent Contrat de sécurité des données (« **DSA** ») s'applique.

Le Prestataire s'engage à respecter toutes les mesures de sécurité, instructions et politiques applicables fournies par écrit par le Client, expressément communiquées ou documentées de manière démontrable.

Ces obligations s'appliquent également à tous les systèmes et installations du Prestataire utilisés pour collecter, accéder, stocker, traiter, sauvegarder ou supprimer les Données Client.

Le Prestataire de services ne peut traiter les Données du Client que pour l'exécution des Services convenus, ou dans la mesure expressément autorisée par le Contrat. Toute autre utilisation est interdite.

Ce document décrit les mesures de sécurité techniques et organisationnelles qu'Amptec a mises en œuvre pour protéger les données des clients. La répartition des responsabilités entre Amptec et le Client en ce qui concerne la gouvernance des données et les actions de sécurité est principalement définie dans la matrice de responsabilité, incluse dans le Contrat-cadre de service (ci-après : « **MSA** »), et complétée dans le(s) Statement(s) of Work(s) applicable(s) (ci-après : « **SoW** »).

Amptec n'est pas responsable des actions ou décisions prises par le Client de sa propre initiative, qu'elles soient ou non expressément énoncées dans le MSA ou l'EDT.

2. Programme, politiques et contrôles de sécurité des données.

Le Prestataire et son personnel (tel que défini ci-après et ci-après, le « Personnel du Prestataire ») ne peuvent accéder aux Actifs du Client que lorsque cela est nécessaire à l'exécution des Services, dans les limites de leur fonction et sur la base d'un besoin légitime. Le Prestataire de services et son personnel ne sont pas autorisés à traiter ou à rendre accessibles les Actifs du Client à des personnes ou entités non autorisées au sein de son organisation ou sous son contrôle.

Le Prestataire de services doit mettre en œuvre et maintenir des mesures de sécurité physiques, électroniques et organisationnelles appropriées pendant toute la durée du contrat, sur la base d'une approche basée sur les risques et conformément aux meilleures pratiques généralement acceptées et aux normes internationales, y compris ISO 27001:2022, les contrôles de sécurité critiques CIS, les normes NIST et les directives de la Cloud Security Alliance.

Ces mesures doivent être conçues pour protéger les Actifs du Client contre l'accès, l'utilisation, la destruction, la perte, la divulgation, le traitement ou la modification illégale non autorisés.

Le Prestataire déclare, garantit et s'engage à ce que ses politiques et mesures de sécurité prévoient au moins les éléments énoncés dans les dispositions suivantes du présent DSA.

2.1 Programme de sécurité de l'information (iSMS).

- Le Fournisseur de services a mis en œuvre une politique écrite de sécurité de l'information qui est à la disposition de tous les employés, sous-traitants et autres membres du personnel actuels (« Personnel du Fournisseur de services ») ;
- Le fournisseur de services a attribué des rôles et des responsabilités en matière de sécurité de l'information ;
- Les politiques de sécurité de l'information du Prestataire de services doivent être examinées et approuvées par la direction générale du Prestataire de services au moins une fois par an ;
- Le Prestataire de services dispose d'une norme et de procédures documentées pour un accès à distance sécurisé aux Données du Client et/ou aux systèmes du Prestataire de services ou du Client. Ces procédures comprennent l'utilisation des appareils du Fournisseur de services, y compris les appareils mobiles, et l'utilisation de mesures de sécurité appropriées telles que l'authentification

multifactorielle (« MFA ») et le cryptage, conformément aux normes et aux meilleures pratiques pertinentes.

2.2 Sécurité des ressources humaines.

- Le Prestataire de services veillera à ce que tous les membres de son propre personnel, ainsi que les employés externes contractuels qui ont accès aux Actifs du Client, suivent chaque année une formation obligatoire de sensibilisation à la sécurité ;
- Cette formation devrait au moins couvrir les bases de la sécurité de l'information, de la protection des données, de la reconnaissance des incidents et de l'utilisation responsable des systèmes, et devrait être adaptée au profil de risque du travail effectué.

2.3 Gestion des actifs et des données.

- Le Prestataire doit protéger les Données du Client conformément à l'ensemble des politiques, procédures et protocoles de sécurité de l'information convenus par écrit entre les Parties ;
- Le fournisseur de services doit s'assurer que tout le personnel du fournisseur de services connaît et respecte les politiques d'utilisation acceptable du fournisseur de services ou des politiques similaires. Ces politiques doivent inclure des dispositions qui définissent les exigences et les responsabilités relatives à l'utilisation des données, du contenu et/ou des systèmes ;
- Le Prestataire de services ne peut pas accéder, stocker, mettre en cache, télécharger ou traiter les Données du Client sur tout appareil ou système qui n'est pas protégé par le pare-feu du Prestataire de services ;
- Le Prestataire doit avoir mis en place et respecter des procédures documentées pour la suppression sécurisée des Données du Client conformément aux durées de conservation convenues et aux lois et réglementations applicables
- Le Prestataire de services doit tenir un inventaire actuel et complet de toutes les informations et autres actifs connexes qui traitent, stockent ou transmettent les Données du Client. Chaque bien doit avoir un propriétaire désigné qui est chargé de le gérer tout au long du cycle de vie du bien.
- Le Prestataire doit s'assurer que toutes les informations et tous les actifs connexes sont correctement classifiés en fonction de leur sensibilité et de leur valeur, et que des mesures de sécurité appropriées sont appliquées qui correspondent à leur classification ;

- Le Prestataire doit mettre en œuvre des procédures de retour ou de cession sécurisées des actifs contenant ou donnant accès aux Données du Client, à la fin du service ou lorsque l'actif n'est plus nécessaire.

2.4 Contrôle d'accès.

- Le Prestataire de services doit restreindre l'accès aux Actifs du Client au seul Personnel autorisé du Prestataire de services, sur la base du principe du besoin d'en connaître et du moindre privilège. Les droits d'accès devraient être accordés dans le cadre d'un modèle d'accès fondé sur les rôles, avec une séparation claire des tâches. Ces droits d'accès devraient être réexaminés au moins une fois par trimestre et ajustés si nécessaire ;
- Le Fournisseur de services doit exiger l'authentification multifacteur (« MFA ») et utiliser un réseau privé virtuel (VPN) ou un accès Zero Trust (ZTA) pour accéder à distance aux systèmes du fournisseur de services, aux installations du fournisseur de services et à tous les actifs du client ;
- Le Prestataire de services doit s'assurer qu'en cas de cessation d'emploi ou de changement de rôle du Personnel du Prestataire de services, l'accès aux systèmes contenant des Données du Client est immédiatement révoqué ;
- Le Prestataire doit attribuer des identifiants d'utilisateur uniques à tous les utilisateurs et interdire l'utilisation de comptes partagés, sauf si l'infrastructure ou le logiciel du côté du client exige le contraire ou s'il n'est pas techniquement possible de faire une distinction ;
- Le fournisseur de services doit appliquer les normes de l'industrie et les meilleures pratiques en matière de mots de passe forts et de gestion du cycle de vie pour tous les utilisateurs, y compris les changements réguliers et la prévention de la réutilisation des mots de passe.
- Le fournisseur de services doit examiner les comptes privilégiés au moins une fois par trimestre pour confirmer que les privilèges et les privilèges sont appropriés pour les rôles attribués.
- Le Prestataire ne peut pas transférer d'e-mails provenant de Comptes Client, que ce soit automatiquement ou manuellement, vers des Comptes non-Client, sauf autorisation expresse du Client.

2.5 Sécurité physique.

Si les Données du Client sont stockées dans un centre de données détenu ou contrôlé par le Prestataire de services, le Prestataire de services doit mettre en œuvre et maintenir

des mesures de sécurité physique pour protéger les Données du Client et le réseau du Prestataire de services. Ces mesures comprennent, entre autres :

- Accès contrôlé aux zones où les Données Client sont stockées, traitées ou transmises, à l'aide de badges et de journaux d'accès ;
- Protection physique et maintenance de l'équipement du Prestataire de services afin d'éviter la perte, la divulgation, l'endommagement, le vol ou la compromission des Données du Client ;
- Élimination sécurisée des équipements et des supports physiques et électroniques contenant des Données Client, conformément aux périodes de conservation convenues et aux lois et réglementations applicables.

Si le stockage des Données du Client a lieu dans un centre de données détenu ou exploité par un sous-traitant du Prestataire, le Prestataire doit s'assurer que le sous-traitant a mis en place et maintient des mesures de sécurité physique similaires.

2.6 Services de cloud public.

Si le Prestataire utilise des services de cloud public pour stocker ou traiter des Données Client, le Prestataire de services doit mettre en œuvre et maintenir les mesures de sécurité suivantes, conformément aux normes et aux meilleures pratiques de l'industrie :

- Authentification multifacteur (MFA) : Le fournisseur de services doit exiger l'authentification multifacteur pour tous les comptes d'utilisateurs administratifs qui accèdent aux services cloud du fournisseur de services, afin d'empêcher tout accès non autorisé ;
- Principes de ségrégation et gestion des clés : Le fournisseur de services doit mettre en œuvre une séparation logique des environnements cloud pour isoler les données du client des autres données, y compris celles des autres clients du fournisseur de services. Cela comprend l'utilisation de pratiques rigoureuses de gestion des clés, telles que l'application du principe de séparation des tâches dans la gestion des clés, afin qu'aucun utilisateur n'ait un accès complet aux clés de chiffrement et de déchiffrement ;
- Chiffrement des Données Client : Le Prestataire de services doit appliquer un chiffrement standard à toutes les Données Client :
    - Pendant la transmission : Toutes les Données du Client doivent être chiffrées en transit sur des réseaux vers, depuis et au sein du service de cloud public, par exemple, par l'utilisation de TLS (Transport Layer Security) ;

- Au repos : toutes les données client stockées dans le service de cloud public doivent être chiffrées à l'aide d'algorithmes de chiffrement puissants, tels que AES-256, et les clés de chiffrement doivent être gérées par le biais d'un système de gestion de clés (KMS) robuste.

- Surveillance et journalisation : Le fournisseur de services doit mettre en œuvre une surveillance et une journalisation continues pour toutes les activités dans les environnements cloud, y compris les journaux d'accès et de modification, afin de détecter les activités suspectes et de répondre aux incidents de sécurité.

Le Fournisseur de services doit procéder à des examens réguliers des mesures et des configurations de sécurité du cloud pour s'assurer qu'elles continuent de répondre aux normes de sécurité applicables et que les Données du Client sont protégées de manière adéquate.

2.7 Sécurité des opérations.

Le fournisseur de services doit mettre en œuvre et tenir à jour une norme de journalisation et de surveillance qui répond aux exigences suivantes :

- Journal des événements : le système doit consigner des événements tels que :
    - Connexion et déconnexion de l'utilisateur ;
    - Tentatives de connexion non valides ;
    - Accès et opérations privilégiés, y compris la sortie de données, les modifications et la gestion de la sécurité ;
    - L'accès aux journaux par le Client et les Affiliés du Client ;
    - Arrêtez ou mettez en pause l'enregistrement/la production de journaux.
- Sécurité des journaux : Les fichiers journaux doivent être protégés contre tout accès, modification et suppression non autorisés. L'accès aux fichiers journaux devrait être limité au personnel autorisé et devrait être surveillé et enregistré ;
- Conservation des journaux : Les fichiers journaux doivent être conservés pendant une durée convenue entre le Prestataire et le Client, et conformément aux lois et réglementations applicables.
- Surveillance : Le Prestataire de services doit mettre en place une surveillance continue pour détecter les activités suspectes et les incidents de sécurité. La surveillance devrait être effectuée conformément aux procédures et aux fréquences convenues.

- Accessibilité pour le Client : Le Client et ses sociétés affiliées doivent avoir accès aux fichiers journaux et aux données de surveillance pertinents, comme convenu dans l'accord entre les Parties.

2.8 Sécurité du réseau.

Le fournisseur de services doit surveiller, détecter et limiter la circulation de l'information sur une base multicouche, y compris, mais sans s'y limiter, l'utilisation des mesures de sécurité suivantes :

- Segmentation du réseau et configuration du pare-feu : Mise en œuvre de la segmentation du réseau et de la configuration sécurisée des pare-feu sur le réseau de réseaux locaux virtuels (vLAN) du fournisseur de services, conformément aux normes et aux meilleures pratiques de l'industrie ;
- Pare-feu d'applications Web (WAF) : toutes les applications externes doivent être protégées par des pare-feu d'applications Web pour détecter et bloquer les attaques de la couche applicative.
- Zone démilitarisée (DMZ) : Maintien d'une zone démilitarisée pour protéger le réseau interne et les actifs qui fournissent des services au Client et à ses affiliés, en n'autorisant que le trafic nécessaire ;
- Systèmes de Détection et de Prévention des Intrusions (IDS/IPS) : Mise en place de systèmes de détection et/ou de prévention des intrusions aux points d'entrée pour détecter et prévenir les activités suspectes.

Ces mesures devraient être régulièrement réexaminées et mises à jour afin d'assurer une protection continue contre les menaces émergentes et conformément aux normes de sécurité les plus récentes.

2.9 Télétravail.

Si le Prestataire de services ou son personnel fournit des services à partir de lieux externes, le Prestataire de services doit s'assurer que les exigences suivantes sont respectées :

- Environnement de travail protégé : Le télétravail ne peut avoir lieu que dans un espace protégé (par exemple une maison privée) et dans le respect des normes de bureau propre. L'emplacement doit garantir une exposition minimale à d'autres personnes (non prestataires de services) ;
- Journalisation et surveillance : la journalisation complète doit être activée sur les systèmes des fournisseurs de services autorisés (qui répondent aux normes

spécifiées ici). Ces journaux doivent être mis à disposition à la demande du Client pour enquêter sur d'éventuels incidents de sécurité impliquant les Données du Client ;

- Utilisation d'appareils autorisés : Le personnel du fournisseur de services qui participe au programme de télétravail ne peut utiliser que des appareils qui sont autorisés en vertu du programme de sécurité du fournisseur de services (« appareils autorisés ») et qui répondent aux normes suivantes :

  - Chaque appareil autorisé doit recevoir les mises à jour de sécurité selon le même calendrier que les appareils locaux.
  - Les appareils autorisés doivent être conformes aux normes de cryptage énumérées ici ;
  - Le personnel du fournisseur de services ne peut pas utiliser d'appareils dotés de privilèges administratifs, d'un accès au protocole de bureau à distance ou de droits de privilège pour modifier des services ou des privilèges, sauf si leur titre de poste l'exige.
  - Les appareils autorisés doivent être renforcés selon des normes identiques ou plus strictes que les systèmes des installations du fournisseur de services ;
  - Les contrôles techniques doivent empêcher le stockage local des Données Client sur les Appareils Autorisés ;
  - Les appareils autorisés doivent être équipés d'un économiseur d'écran sécurisé et verrouillable qui nécessite une authentification après un maximum de quinze (15) minutes d'inactivité.
  - Les appareils autorisés doivent être configurés avec un VPN toujours actif ;
  - Le VPN ne doit pas pouvoir être désactivé par les utilisateurs ;
  - Tout le trafic réseau doit passer par le VPN ;
  - L'authentification multifacteur (MFA) est nécessaire pour accéder au VPN ;
  - Tout accès aux Applications du Client et de ses sociétés affiliées doit se faire par le biais d'une infrastructure de bureau virtuel sécurisée (Amptec RAS) ou d'une technologie équivalente, qui ne permet pas un accès direct aux applications et aux données à partir d'Appareils autorisés :
    - RAS peut ne pas autoriser le copier/coller vers/depuis des appareils autorisés ;
    - Les captures d'écran doivent être désactivées sur le VDI.

- Fin du télétravail : Le client peut, à sa seule discrétion, demander que certains membres du personnel du prestataire de services cessent de travailler à distance. Le Prestataire collaborera de bonne foi avec le Client pour permettre au personnel concerné de retourner dans les installations du Prestataire dans les plus brefs délais, conformément aux exigences locales et aux politiques du Prestataire, le cas échéant.

2.10 Gestion des prestataires de services.

Le Prestataire de services est chargé de s'assurer que tout le personnel et les sous-traitants qui accèdent aux systèmes et aux installations du Prestataire de services, les utilisent, ainsi qu'aux Actifs du Client, respectent les exigences du présent Accord de sécurité des données (DSA).

Le Prestataire doit conclure des accords de sécurité de l'information avec des sous-traitants qui ont accès aux actifs du Client ou fournissent des services qui entraînent un accès aux systèmes ou aux installations du Prestataire de services. Ces accords doivent être essentiellement équivalents à la présente AVD et contenir au moins les éléments suivants :

- Obligations de sécurité : Dispositions claires sur les obligations de sécurité du sous-traitant, y compris le respect des normes et pratiques de sécurité pertinentes ;
- Contrôle d'accès : Spécification des droits d'accès et des restrictions relatives aux actifs du Client et aux systèmes du Prestataire de services ;
- Réponse aux incidents : Procédures de signalement et de traitement des incidents de sécurité qui concernent le sous-traitant ;
- Audits et évaluations : Le droit du Prestataire de réaliser des audits et des évaluations pour vérifier la conformité du sous-traitant aux exigences de sécurité ;
- Résiliation de l'accès : Dispositions relatives à la résiliation de l'accès du sous-traitant aux actifs du client et aux systèmes du fournisseur de services en cas de résiliation du contrat ou de non-respect des exigences de sécurité.

Le Prestataire doit surveiller et évaluer régulièrement le respect de ces accords par les sous-traitants et prendre les mesures appropriées si un non-respect est détecté.

2.11 Notification et réponse aux incidents.

Le fournisseur de services doit suivre les meilleures pratiques de l'industrie en cas d'incident de sécurité suspecté ou confirmé. Le Prestataire doit au moins :

- Notification au Client : Signaler un tel incident de sécurité au Client en détail dès que possible après sa découverte et prendre immédiatement les mesures correctives et préventives appropriées ;
- Divulgation : Effectuer toute notification ou divulguer l'incident de quelque manière que ce soit s'il se rapporte aux actifs du Client ou s'il les affecte, sans le consentement écrit préalable du Client, sauf si la loi l'exige ;
- Enquête : Mener une enquête rapide et approfondie sur l'incident de sécurité, y compris, si nécessaire et à la seule discrétion du Client, faire appel à un ou plusieurs tiers indépendants ;
- Rapports : Fournir au Client un rapport détaillant l'incident de sécurité, l'impact connu et potentiel sur les actifs du Client, la cause profonde et les mesures prises pour résoudre l'incident et éviter qu'il ne se reproduise ;
- Coopération : Coopérer à toute enquête sur l'incident de sécurité demandée par le Client.

2.12 Évaluations de conformité et de sécurité.

- Le Prestataire de services doit se conformer à toutes les lois et réglementations applicables, y compris s'assurer que le programme de sécurité met en œuvre toutes les mesures requises par la loi.
- À la demande du Client, le Prestataire fournit une copie signée annuellement de son dernier rapport d'évaluation de sécurité, accompagné d'un plan documentant les défaillances identifiées et précisant les actions correctives envisagées, y compris les délais et les responsables.
- Le Prestataire doit, à ses frais, dans les quatre-vingt-dix (90) jours suivant la réception de tout Rapport d'Audit, corriger toute constatation critique ou sérieuse. Les audits externes à la demande du client peuvent être à la charge du client.

2.13 Résiliation de l'Accord

Si le Prestataire ne respecte pas matériellement le présent Contrat de sécurité des données, subit un incident de sécurité ayant un impact matériel sur le Client et/ou ses Affiliés, ou si le Client prend connaissance d'une détérioration matérielle des mesures de sécurité du Prestataire de services, le Client a le droit de résilier le présent Contrat, ainsi que tout Cahier des charges sous-jacent, bons de travail ou documents similaires, sans pénalité ni dommages-intérêts, sous réserve d'un préavis de trente (30) jours.

La résiliation prendra effet à la date indiquée dans la notification écrite. À l'expiration ou à la résiliation du Contrat, le Prestataire de services est tenu de restituer ou de détruire en toute sécurité toutes les Données du Client, au choix du Client. À cette fin, le Prestataire de services appliquera les meilleures pratiques courantes et les normes de

l'industrie dans la destruction ou la restitution des Données du Client, dans un délai de quatre-vingt-dix (90) jours après réception de l'avis écrit de résiliation ou d'expiration du Contrat, et/ou de tout Bon de commande du Client ou Cahier des charges applicable, à moins qu'une période plus courte ne soit prévue dans le Contrat, la Commande du Client ou le Cahier des charges. Cette obligation s'applique à toutes les Données du Client, qu'elles soient stockées sur site, dans des centres de données, dans des environnements cloud ou sur des sauvegardes.

À l'expiration ou à la résiliation du Contrat, le Prestataire doit confirmer que son accès, et celui de tout le personnel sous sa responsabilité, à tous les Actifs du Client a été révoqué ou résilié. En outre, à la demande du Client, le Prestataire doit fournir une preuve écrite et une attestation de la résiliation ou de la révocation de ces droits d'accès.

3. Existence de l'Accord.

Toutes les dispositions du présent Contrat de sécurité des données seront résiliées de plein droit lors du retour ou de la destruction de toutes les Données du Client par le Fournisseur de services, et de la résiliation complète de l'accès aux Actifs du Client, conformément aux conditions énoncées dans le présent Contrat de sécurité des données et le Contrat de services gérés applicable.

4. Modifications de l'Accord.

Aucune disposition du présent Accord sur la sécurité des données ne peut être modifiée, complétée ou supprimée si ce n'est par un accord écrit expressément signé par les deux Parties.

5. Acceptation de l'Accord.

En signant un bon de commande, un énoncé des travaux ou tout autre document faisant référence au présent accord de sécurité des données, les deux parties confirment expressément qu'elles ont entièrement lu, compris et accepté les termes et conditions du présent accord.

Cette acceptation implique que toutes les obligations, responsabilités et droits énoncés dans le présent Accord sur la sécurité des données sont contraignants pour les deux parties et font partie intégrante de la relation contractuelle entre les parties.

En cas de conflit entre l'une des dispositions du présent Accord sur la sécurité des données et l'une des dispositions de tout autre document faisant partie de l'accord entre les parties, les dispositions du présent Accord sur la sécurité des données prévaudront, sauf accord contraire exprès et écrit entre les deux parties.

6. Responsabilité et indemnisation.

6.1 Limitation de responsabilité.

En aucun cas, le Prestataire, ses administrateurs, employés, agents ou sociétés affiliées ne pourront être tenus responsables des dommages, pertes, coûts ou amendes, résultant directement ou indirectement d'un incident de cybersécurité, d'une violation de données, d'un accès illégal, d'une brèche de système ou d'un incident de sécurité équivalent, sauf en cas d'erreur volontaire ou de fraude de la part du Prestataire. Cette exclusion s'applique également aux dommages causés par des tiers, à moins que la responsabilité contractuelle du Prestataire ne soit engagée en vertu d'accords écrits exprès.

6.2 Exclusion des dommages indirects.

En aucun cas, le Prestataire ne pourra être tenu responsable des dommages indirects, accessoires, spéciaux ou consécutifs. Cela inclut, mais sans s'y limiter, la perte de bénéfices, la perte de revenus, l'atteinte à la réputation, la valeur commerciale réduite, la perte d'économies anticipées, la perte ou la corruption de données, ainsi que l'interruption ou le temps d'arrêt des opérations commerciales. Cette exclusion s'applique quelle que soit la cause ou le fondement juridique du dommage, et que la possibilité d'un tel dommage ait été communiquée au préalable au Prestataire. Elle s'applique également, que la responsabilité soit fondée sur une base contractuelle, extracontractuelle ou autre base juridique, même si la possibilité de tels dommages a été communiquée au Prestataire de services à l'avance.

6.3 Indemnisation par le client.

Le Client s'engage à indemniser, défendre et dégager de toute responsabilité le Prestataire de services, ainsi que ses employés, administrateurs, agents et sociétés affiliées, à l'égard de toutes réclamations, demandes, pertes, dommages, coûts et dépenses (y compris les honoraires d'avocat raisonnables) découlant de ou en relation avec :

- L'incapacité du Client à mettre en œuvre ou à mettre en œuvre insuffisamment les mesures ou procédures de sécurité recommandées par le Prestataire ;
- Toute négligence, erreur, manquement aux obligations contractuelles ou délit commis par le Client ou ses ayants droit ;
- Décisions ou actions prises par le Client sur la base de conseils, d'analyses, de recommandations ou de rapports fournis par le Prestataire, dont la responsabilité n'est pas engagée sauf en cas de faute intentionnelle ou de dol

6.4 Avis de non-responsabilité du jugement professionnel.

Le Client reconnaît que les prestations fournies par le Prestataire ont un caractère de conseil et d'accompagnement et sont fondées sur une évaluation professionnelle au sein d'un domaine technologique en constante évolution. Bien que le Prestataire fasse des efforts raisonnables pour atténuer les risques et formuler des recommandations

adéquates, la responsabilité ultime des décisions prises et de la mise en œuvre des mesures incombe uniquement au Client.

7. Force majeure.

Aucune des Parties ne sera responsable de tout manquement ou retard dans l'exécution de ses obligations au titre du présent Accord sur la sécurité des données, dans la mesure où il résulterait d'un cas de force majeure. On entend par force majeure tout événement ou circonstance échappant au contrôle raisonnable d'une Partie, qui n'est pas imputable à sa faute ou à sa négligence, et qui empêche temporairement ou définitivement l'exécution de ses obligations contractuelles. Cela inclut, mais sans s'y limiter, les catastrophes naturelles, les guerres, les émeutes, le terrorisme, les actions gouvernementales, les pandémies, les épidémies, les pannes d'électricité ou de réseau, les pannes d'infrastructure, les grèves et d'autres événements de nature similaire.

La Partie affectée par un cas de force majeure informera immédiatement l'autre Partie par écrit de l'existence, de la nature, de la durée probable et des conséquences de la situation de force majeure. L'exécution du contrat est suspendue pendant la durée de la force majeure, sans donner lieu à un droit à indemnisation pour l'autre partie. La Partie affectée prend toutes les mesures raisonnables pour minimiser les conséquences de l'événement de force majeure et pour reprendre l'exécution de ses obligations dès que raisonnablement réalisable.

Si la situation de force majeure persiste pendant plus de soixante jours, l'une ou l'autre des Parties pourra résilier le contrat en tout ou en partie par notification écrite, sans intervention judiciaire et sans être redevable d'une quelconque indemnité.

8. Durée et résiliation.

Le présent accord sur la sécurité des données entre en vigueur à la date de signature par les deux parties ou, si elle est antérieure, à la date à laquelle ces dispositions sont expressément référencées dans une commande client, un cahier des charges ou tout autre document contractuel. Il restera en vigueur aussi longtemps qu'une relation contractuelle valable existera entre les Parties, que ce soit dans le cadre d'un accord-cadre ou d'un Bon de commande ou d'un Cahier des charges, sous réserve d'une résiliation anticipée conformément aux dispositions ci-dessous.

Le Client a le droit de résilier le présent Contrat de sécurité des données, ainsi que tous les énoncés de travail, bons de travail ou autres documents applicables sous-jacents, sans aucune compensation ni pénalité, sous réserve d'un préavis de trente (30) jours, si le Prestataire de services ne se conforme pas matériellement au présent Accord de sécurité des données, si le Prestataire de services fait l'objet d'un incident de sécurité ayant un impact matériel sur le Client ou ses sociétés affiliées, ou si le Client a

connaissance d'une détérioration substantielle des mesures de sécurité du Prestataire. La résiliation entrera en vigueur à la date indiquée dans l'avis écrit du Client.

En cas de résiliation ou d'expiration du présent contrat, le Prestataire de services est tenu, au choix du Client, de restituer ou de détruire en toute sécurité toutes les Données du Client. Le Prestataire de services appliquera ainsi les normes et les pratiques de sécurité généralement acceptées, dans un délai maximum de quatre-vingt-dix (90) jours après la réception de l'avis écrit, à moins qu'un délai plus court ne soit prévu dans un Bon de commande du client ou un Énoncé des travaux applicable. Cette obligation s'applique quel que soit l'emplacement des Données du Client, y compris sur site, dans des centres de données, des environnements cloud ou des sauvegardes.

Le Prestataire doit confirmer par écrit, lors de la résiliation ou de l'expiration, que son accès aux Actifs du Client, ainsi qu'à celui de toutes les personnes travaillant sous sa responsabilité, a été résilié ou révoqué dans son intégralité. À la demande du Client, le Prestataire doit également fournir une preuve écrite ou une certification de cette résiliation ou rétractation.

Les dispositions du présent Accord sur la sécurité des données qui, de par leur nature, sont destinées à survivre à la résiliation. Cela inclut, mais sans s'y limiter, les dispositions relatives à la confidentialité, à la responsabilité, à l'indemnisation et au droit applicable.

9. Portabilité.

Aucune des Parties ne peut transférer, déléguer ou sous-traiter le présent Accord sur la sécurité des données, ni aucun droit ou obligation en découlant, en tout ou en partie, à un tiers sans le consentement écrit préalable de l'autre Partie. Cette autorisation ne peut être refusée ou retardée sans motif raisonnable.

Nonobstant ce qui précède, le Client peut céder le présent Contrat, sans le consentement préalable du Fournisseur de services, à une société affiliée ou dans le cadre d'une fusion, d'une acquisition, d'une réorganisation ou d'un transfert d'actifs, à condition que l'entité acquéreuse confirme par écrit qu'elle est liée par les termes du présent Contrat de sécurité des données. Dans ce cas, le Prestataire reste entièrement responsable de la bonne exécution de ses obligations en vertu du présent contrat, même si elles sont exécutées en tout ou en partie par un tiers.

Toute cession en violation de cette disposition est nulle de plein droit et sans effet.

10. Intégralité de l'accord.

Le présent Accord de sécurité des données, ainsi que l'accord principal, les Commandes du Client applicables, les Énoncés des travaux et autres documents écrits faisant expressément référence à ces dispositions, constituent l'intégralité de l'accord entre les Parties en ce qui concerne la sécurité des données, les actifs du Client et le traitement des informations.

Il remplace tous les accords, déclarations ou propositions antérieurs, oraux ou écrits, sur le même sujet. Rien dans tout autre document contractuel n'affectera le présent Accord sur la sécurité des données, sauf accord exprès écrit des deux parties.

11. Droit applicable et juridiction.

Le présent contrat de sécurité des données est exclusivement régi par le droit belge, à l'exclusion du droit international privé et de la Convention de Vienne sur les ventes.

Tous les litiges découlant du présent contrat ou en relation avec celui-ci relèvent de la compétence exclusive du Tribunal de l'entreprise d'Anvers, division de Tongres. Les parties s'engagent à s'efforcer de résoudre tout différend en premier lieu par voie de consultation écrite dans un délai raisonnable, sans préjudice du droit de demander des mesures provisoires.

12. Annexe – Terminologie utilisée.

« Loi applicable » désigne l'ensemble des lois, règles, réglementations et normes applicables dans chaque juridiction dans laquelle les Services sont fournis ou où les Données du Client ou les Informations confidentielles peuvent être stockées ou traitées. Cela inclut, mais sans s'y limiter, la législation sur la confidentialité, la protection des données et la sécurité de l'information, y compris, mais sans s'y limiter, le Règlement général sur la protection des données et les lois nationales d'application.

« **Informations confidentielles** » désigne toute information ou matériel, quelle que soit sa forme (écrite, orale, électronique ou autre) et son support, qui est fourni ou mis à la disposition de la partie destinataire dans des circonstances qui démontrent raisonnablement qu'il est confidentiel. Cela est vrai, que ces informations soient expressément marquées comme confidentielles ou exclusives. Il comprend également les informations que la partie qui fournit obtient d'une société affiliée ou d'un tiers, et qui sont considérées comme confidentielles par cette partie. Les parties conviennent que le présent Contrat de sécurité et ses dispositions constituent des Informations confidentielles. Les Données du Client et les Données personnelles sont considérées comme des Informations confidentielles du Client et/ou de ses sociétés affiliées, sauf dans la mesure où ces informations sont déjà accessibles au public sans violation du présent Accord.

« Actifs du Client » désigne et inclut toutes les Données du Client, les Systèmes du Client et les Installations du Client.

« **Données client** » désigne toutes données, documents, informations ou matériels, sous quelque format ou support que ce soit, qui (i) sont fournis ou mis à la disposition du Prestataire de services par le Client ou ses entités affiliées ou en son nom, (ii) sont collectés, générés ou traités par le Prestataire de services dans le cadre de l'exécution des Services, (iii) découlent de l'utilisation des Services ou s'y rapportent, Les systèmes

ou l'infrastructure du Fournisseur de services par le Client ou ses entités affiliées, ou (iv) sont dérivés des catégories précédentes. Les données client comprennent également toutes les œuvres dérivées, copies, éditions, résumés, analyses, extraits ou reproductions de ces données. Les Données à caractère personnel du Client et les Informations confidentielles sont considérées comme des Données du client.

« **Installation(s) du Client** » désigne tout emplacement physique, installation technique ou bâtiment, quelle que soit la structure de propriété ou la direction opérationnelle, utilisé par le Client ou ses entités affiliées dans le cadre ou en relation avec la fourniture, l'assistance ou la sécurité des Services.

« **Systèmes du Client** » désigne les systèmes, réseaux, matériels, logiciels, applications, bases de données et autres ressources informatiques détenus, contrôlés ou mis à la disposition du Client ou de ses entités affiliées, que ce soit ou non par l'intermédiaire d'un tiers. Ces systèmes font partie intégrante de l'environnement technique dans lequel ou par l'intermédiaire duquel les Services sont fournis, supportés ou sécurisés.

« **Données personnelles »** désigne : (1) toute information relative à une personne physique, un appareil ou un ménage identifié ou identifiable, ou (2) toute information définie comme « informations personnellement identifiables », « informations personnelles », « données personnelles » ou termes similaires tels que définis par la loi applicable.

« **Traitement » ou « Traitement** » désigne toute opération ou ensemble d'opérations relatives aux Données du Client, que ce soit ou non par des moyens automatisés, telles que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation, l'altération, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion, la mise à disposition, l'alignement, la combinaison, la restriction, l'effacement ou la destruction.

« **Incident de sécurité** » désigne tout événement impliquant ou suspect raisonnable d'accès non autorisé ou illégal, d'altération, de perte, de divulgation ou de perturbation de l'intégrité, de la confidentialité ou de la disponibilité des Données du Client, des actifs du Client ou des systèmes gérés par le Prestataire de services en vertu du présent Contrat. Cela inclut les violations des mesures de sécurité qui constituent une violation de données en vertu des lois applicables en matière de protection des données.

« **Services »** fait référence aux services fournis dans le cadre du Contrat, y compris les services d'hébergement, l'assistance, les services professionnels, les services cloud et toute autre performance spécifiée dans le bon de commande et/ou l'énoncé des travaux concernés.

« Installations du Fournisseur de services » désigne tout emplacement ou infrastructure utilisé par le Fournisseur de services pour l'exécution des Services ou pour

le stockage, le traitement, la transmission ou l'accès aux Informations confidentielles du Client, qu'il soit exploité par le Fournisseur de services ou par un tiers en son nom.

« Systèmes du Fournisseur de services » désigne les systèmes, réseaux, matériels, logiciels, applications et autres technologies utilisés par le Fournisseur de services ou en son nom pour fournir les Services ou traiter les Informations confidentielles du Client, qu'ils soient sous le contrôle du Fournisseur de services ou hébergés par un tiers.

« Affilié » désigne toute entité qui, directement ou indirectement, contrôle, est contrôlée par ou est sous contrôle commun avec une Partie, le terme « contrôle » étant défini comme le droit de déterminer, directement ou indirectement, l'orientation ou les politiques d'une entité par le biais de la propriété de titres avec droit de vote, d'un accord ou autrement.

DATA SECURITY AGREEMENT

Between:

AMPTEC BV, a private limited liability company incorporated under Belgian law, with registered office at Bremakker 45, 3740 Bilzen, and company number 0442.333.460, represented by Bart Willems director, hereinafter referred to as the "**Service Provider**" or "**Amptec**";

And the **CUSTOMER** Further referred to as the "**Customer**",

The Service Provider and the Customer are hereinafter referred to individually as a "**Party**" and collectively as the "**Parties**".

1. Scope.

To the extent that the Service Provider has access to Customer Systems or Customer Facilities, or processes Customer Data, Personal Information or Confidential Information (as defined in Section 12), because of the Services provided by the Service Provider, this Data Security Agreement ("**DSA**") shall apply.

The Service Provider undertakes to comply with all applicable security measures, instructions and policies provided by the Customer in writing, expressly communicated or demonstrably documented.

These obligations also apply to all Service Provider systems and facilities used to collect, access, store, process, back up or delete Customer Data.

The Service Provider may only process Customer Data for the performance of the agreed Services, or to the extent expressly permitted under the Agreement. Any other use is prohibited.

This document describes the technical and organizational security measures that Amptec has implemented to protect Customer Data. The division of responsibilities between Amptec and Customer with respect to data governance and security actions is primarily set forth in the responsibility matrix, included in the Master Service Agreement (hereinafter: "**MSA**"), and supplemented in the applicable Statement(s) of Work (hereinafter: "**SoW**").

Amptec shall not be liable for any actions or decisions Customer takes on its own initiative, whether or not expressly set forth in the MSA or SoW.

2. Data Security Program, Policies and Controls.

The Service Provider and its personnel (as defined below and hereinafter, "Service Provider Personnel") may only access Customer Assets when necessary for the performance of the Services, within the limits of their function and on the basis of a legitimate need. The Service Provider and its Service Provider personnel are not permitted to process or make Customer Assets accessible to unauthorized persons or entities within its organization or under its control.

The Service Provider must implement and maintain appropriate physical, electronic, and organizational security measures throughout the term of the agreement, based on a risk-based approach and in accordance with generally accepted best practices and international standards, including ISO 27001:2022, the CIS Critical Security Controls, the NIST Standards, and Cloud Security Alliance guidelines.

These measures should be designed to protect Customer Assets from unauthorized access, use, destruction, loss, disclosure, processing, or unlawful alteration.

The Service Provider represents, warrants and undertakes that its security policies and measures provide for at least the elements set out in the following provisions of this DSA.

2.1 Information Security Program (iSMS).

- The Service Provider has implemented a written information security policy that is available to all current employees, contractors, and other personnel ("Service Provider Personnel");
- The Service Provider has assigned roles and responsibilities for information security;
- The Service Provider's information security policies shall be reviewed and approved by the Service Provider's executive management at least annually;
- The Service Provider has a documented standard and procedures for secure remote access to Customer Data and/or Service Provider or Customer systems. These procedures include the use of Service Provider devices, including mobile devices, and use appropriate security measures such as multi-factor authentication ("MFA") and encryption, in accordance with relevant standards and best practices.

2.2 Human Resources Security.

- The Service Provider shall ensure that all of its own staff members, as well as contracted external employees who have access to Customer Assets, undergo mandatory security awareness training on an annual basis;
- This training should at least cover the basics of information security, data protection, incident recognition and responsible use of systems, and should be tailored to the risk profile of the work performed.

2.3 Assets and data management.

- The Service Provider must protect Customer Data in accordance with all information security policies, procedures and protocols agreed upon in writing between the Parties;
- The Service Provider must ensure that all Service Provider Personnel are aware of and comply with the Service Provider's acceptable use policies or similar policies. These policies should include provisions that define the requirements and responsibilities for the use of data, content, and/or systems;
- The Service Provider may not access, store, cache, download, or process Customer Data on any device or system that is not protected by the Service Provider's firewall;
- The Service Provider must have in place and comply with documented procedures for the secure deletion of Customer Data in accordance with the agreed retention periods and applicable laws and regulations
- The Service Provider must maintain a current and complete inventory of all information and other related assets that process, store or transmit Customer Data. Each asset must have an assigned owner who is responsible for managing it throughout the asset's lifecycle;
- The Service Provider must ensure that all information and related assets are properly classified according to their sensitivity and value, and that appropriate security measures are applied that match their classification;
- The Service Provider must implement procedures for the secure return or disposal of assets that contain or provide access to Customer Data, upon termination of service or when the asset is no longer needed.

2.4 Access control.

- The Service Provider must restrict access to Customer Assets to only authorized Service Provider Personnel, based on the principle of need-to-know and least privilege. Access rights should be granted through a role-based access model with

clear separation of duties. These access rights should be reviewed at least quarterly and adjusted if necessary;

- The Service Provider must require Multi-Factor Authentication ("MFA") and use a Virtual Private Network (VPN) or Zero-Trust Access (ZTA) to remotely access Service Provider Systems, Service Provider Facilities, and all Customer assets;
- The Service Provider must ensure that upon termination of employment or change of Service Provider Personnel role, access to systems containing Customer Data is immediately revoked;
- The Service Provider must assign unique user IDs to all users and prohibit the use of shared accounts, unless the infrastructure or software on the customer side requires otherwise or it is not technically possible to distinguish;
- The Service Provider must enforce industry standards and best practices for strong passwords and lifecycle management for all users, including regular changes and preventing password reuse;
- The Service Provider must review privileged accounts at least quarterly to confirm that privileges and privileges are appropriate for the assigned roles;
- The Service Provider may not forward emails from Customer Accounts, either automatically or manually, to non-Customer Accounts, unless expressly authorized by Customer.

2.5 Physical Security.

If Customer Data is stored in a data center owned or controlled by the Service Provider, the Service Provider must implement and maintain physical security measures to protect Customer Data and the Service Provider's network. These measures include, among other things:

- Controlled access to areas where Customer Data is stored, processed, or transmitted, using badges and access logs;
- Physical protection and maintenance of the Service Provider's equipment to prevent loss, disclosure, damage, theft, or compromise of Customer Data;
- Secure disposal of equipment and physical and electronic media containing Customer Data, in accordance with agreed retention periods and applicable laws and regulations.

If the storage of Customer Data takes place in a data center owned or operated by a subcontractor of the Service Provider, the Service Provider must ensure that the subcontractor has implemented and maintains similar physical security measures.

2.6 Public Cloud Services.

If the Service Provider uses public cloud services to store or process Customer Data, the Service Provider must implement and maintain the following security measures, in accordance with industry standards and best practices:

- Multi-Factor Authentication (MFA): The Service Provider must require MFA for all administrative user accounts that access the Service Provider's cloud services, to prevent unauthorized access;
- Segregation Principles and Key Management: The Service Provider must implement logical separation of cloud environments to isolate Customer Data from other data, including that of other customers of the Service Provider. This includes using strong key management practices, such as applying the Separation of Duties principle in key management, so that no user has full access to both encryption and decryption keys;
- Encryption of Customer Data: The Service Provider must apply industry-standard encryption to all Customer Data:
    - During Transmission: All Customer Data must be encrypted in transit over networks to, from, and within the public cloud service, for example, through the use of Transport Layer Security (TLS);
    - At rest: All Customer Data stored within the public cloud service must be encrypted using strong encryption algorithms, such as AES-256, and the encryption keys must be managed through a robust Key Management System (KMS).
- Monitoring and Logging: The Service Provider should implement continuous monitoring and logging for all activities within the cloud environments, including access and change logs, to detect suspicious activities and respond to security incidents.

The Service Provider must conduct regular reviews of the cloud security measures and configurations to ensure that they continue to meet applicable security standards and that Customer Data is adequately protected.

2.7 Operations Security.

The Service Provider must implement and maintain a logging and monitoring standard that meets the following requirements:

- Event log: The system should log events such as:
    - User login and logout;
    - Invalid login attempts;

- Privileged access and operations, including data output, modifications, and security management;
- Access to logs by the Client and Client Affiliates;
- Stop or pause logging/log production.

- Log Security: Log files must be protected from unauthorized access, modification, and deletion. Access to log files should be restricted to authorized personnel and should be monitored and logged;
- Log Retention: Log files must be retained for a period of time agreed between the Service Provider and the Customer, and in accordance with applicable laws and regulations.
- Monitoring: The Service Provider should implement continuous monitoring to detect suspicious activities and security incidents. Monitoring should be carried out in accordance with the agreed procedures and frequencies.
- Accessibility for Customer: Customer and its affiliates must have access to relevant log files and monitoring data, as agreed to in the agreement between the Parties.

2.8 Network Security.

The Service Provider must monitor, detect and limit the flow of information on a layered basis, including but not limited to the use of the following security measures:

- Network Segmentation and Firewall Configuration: Implementation of network segmentation and secure configuration of firewalls across the Service Provider's network of Virtual Local Area Networks (vLANs), in accordance with industry standards and best practices;
- Web Application Firewalls (WAFs): All externally facing applications must be protected with Web Application Firewalls to detect and block application layer attacks;
- Demilitarized Zone (DMZ): Maintenance of a Demilitarized Zone to protect the internal network and assets that provide services to the Customer and its affiliates, allowing only necessary traffic;
- Intrusion Detection and Prevention Systems (IDS/IPS): Implementation of intrusion detection and/or prevention systems at inlet points to detect and prevent suspicious activity.

These measures should be regularly reviewed and updated to ensure ongoing protection against emerging threats and in line with the latest security standards.

2.9 Teleworking.

If the Service Provider or its Personnel performs services from external locations, the Service Provider must ensure that the following requirements are met:

- Shielded work environment: Teleworking may only take place in a shielded space (e.g. a private home) and in compliance with clean desk standards. The location must ensure minimal exposure to other (non-Service Provider) persons;
- Logging and monitoring: Authorized Service Provider systems (that meet the standards specified here) must have comprehensive logging enabled. These logs must be made available at Customer's request to investigate potential security incidents involving Customer Data;
- Use of Authorized Devices: Service Provider personnel participating in the telework program may only use devices that are authorized under the Service Provider's security program ("Authorized Devices") and that meet the following standards:
    - Each Authorized Device must receive security updates on the same schedule as on-premises devices;
    - Authorized Devices must comply with the encryption standards listed here;
    - Service Provider personnel may not use devices with administrative privileges, remote desktop protocol access, or privilege rights to modify services or privileges, unless required by their job title;
    - Authorized Devices must be hardened to the same or more stringent standards as the systems in the Service Provider's facilities;
    - Technical controls must prevent Customer Data from being stored locally on Authorized Devices;
    - Authorized Devices must have a secure, locking screen saver that requires authentication after up to fifteen (15) minutes of inactivity;
    - Authorized Devices must be configured with an always-on VPN;
    - The VPN must not be able to be disabled by users;
    - All network traffic must go through the VPN;
    - Multi-Factor Authentication (MFA) is required to access the VPN;
    - All access to Applications of Customer and its affiliates must be through a secure virtual desktop infrastructure (Amptec RAS) or equivalent technology,

which does not permit direct access to applications and data from Authorized Devices:

  - RAS may not allow copying/pasting to/from Authorized Devices;
  - Screenshots must be disabled on the VDI.

- Termination of Telework: Customer may, in its sole discretion, request that specific personnel of the Service Provider cease to work remotely. The Service Provider shall cooperate in good faith with the Customer to allow the affected personnel to return to the Service Provider's facilities as soon as possible, in accordance with local requirements and the Service Provider's policies, if applicable.

2.10 Service Provider Management.

The Service Provider is responsible for ensuring that all personnel and subcontractors who access, use Service Provider's systems and facilities, as well as Customer Assets, comply with the requirements of this Data Security Agreement (DSA).

The Service Provider must enter into information security agreements with subcontractors who have access to Customer assets or provide services that result in access to the Service Provider's systems or facilities. These agreements must be essentially equivalent to this DSA and contain at least the following elements:

- Security obligations: Clear provisions on the subcontractor's security obligations, including compliance with relevant security standards and practices;
- Access Control: Specification of access rights and restrictions in relation to Customer assets and systems of the Service Provider;
- Incident response: Procedures for reporting and handling security incidents that concern the subcontractor;
- Audits and Assessments: The right of the Service Provider to conduct audits and assessments to verify the subcontractor's compliance with security requirements;
- Termination of Access: Provisions on terminating the subcontractor's access to Customer Assets and Service Provider systems upon termination of the agreement or upon non-compliance with security requirements.

The Service Provider must regularly monitor and assess subcontractors' compliance with these agreements, and take appropriate action if non-compliance is detected.

2.11 Incident Notification and Incident Response.

The Service Provider must follow industry best practices in the event of a suspected or confirmed security incident. The Service Provider must at least:

- Notification to Customer: To report such a security incident to Customer in detail as soon as possible after discovery and to take appropriate corrective and preventive action immediately;
- Disclosure: Make any notification or disclose the incident in any way if it relates to or affects Customer assets, without the prior written consent of the Customer, unless required by law;
- Investigation: Conducting a prompt and thorough investigation of the security incident, including – if necessary and at the sole discretion of the Customer – engaging an independent third party or parties;
- Reporting: Provide a report to Customer detailing the security incident, the known and potential impact on Customer assets, the root cause, and the measures taken to resolve the incident and prevent its recurrence;
- Cooperation: Cooperate with any investigation into the security incident requested by Customer.

2.12 Compliance and security assessments.

- The Service Provider must comply with all applicable laws and regulations, including ensuring that the security program implements all measures required by law.
- At the Customer's request, the Service Provider shall provide an annual signed copy of its most recent security assessment report, accompanied by a plan documenting the deficiencies identified and specifying the corrective actions envisaged, including deadlines and those responsible.
- The Service Provider must, at its own expense, within ninety (90) days of receipt of any Audit Report, correct any critical or serious findings. External audits at the request of the customer may be at the expense of the customer.

2.13 Termination of the Agreement

If the Service Provider materially fails to comply with this Data Security Agreement, suffers a security incident with a material impact on the Customer and/or its Affiliates, or if the Customer becomes aware of a material deterioration in the Service Provider's security measures, the Customer has the right to terminate this Agreement, as well as any underlying Statements of Work, work orders or similar documentation, without penalty or damages, subject to thirty (30) days' notice.

The termination will take effect on the date specified in the written notification. Upon expiration or termination of the Agreement, the Service Provider is obliged to return or securely destroy all Customer Data, at the Customer's option. To this end, the Service Provider shall apply common best practices and industry standards in the destruction or

return of the Customer Data, within a period of ninety (90) days after receipt of the written notice of termination or expiration of the Agreement, and/or any applicable Customer Order or Statement of Work, unless a shorter period is provided in the Agreement, the Customer Order or the Statement of Work. This obligation applies to all Customer Data, whether stored on-premises, in data centers, in cloud environments, or on backups.

Upon expiration or termination of the Agreement, the Service Provider must confirm that its access, and that of all personnel under its responsibility, to all Customer Assets has been revoked or terminated. In addition, upon Customer's request, the Service Provider must provide written evidence and certification of the termination or revocation of such access rights.

3. Existence of the Agreement.

All provisions of this Data Security Agreement shall terminate by operation of law upon the Service Provider's return or destruction of all Customer Data, and complete termination of access to the Customer Assets, in accordance with the terms set forth in this Data Security Agreement and the applicable Managed Services Agreement.

4. Modifications to the Agreement.

No provision of this Data Security Agreement may be modified, supplemented or waived except by a written agreement expressly signed by both Parties.

5. Acceptance of the Agreement.

By signing a Customer Order, Statement of Work or any other document referring to this Data Security Agreement, both parties expressly confirm that they have fully read, understood and accepted the terms and conditions of this Agreement.

This acceptance implies that all obligations, responsibilities and rights set forth in this Data Security Agreement are binding on both parties, and form an integral part of the contractual relationship between the parties.

If any provision of this Data Security Agreement conflicts with any provision of any other documents that form part of the agreement between the parties, the provisions of this Data Security Agreement shall prevail unless expressly agreed otherwise in writing by both parties.

6. Liability and Indemnification.

6.1 Limitation of Liability.

In no event shall the Service Provider, its directors, employees, agents or affiliates be held liable for any damages, losses, costs or fines, directly or indirectly resulting from any cybersecurity incident, data breach, unlawful access, system breach or equivalent security incident, except in the case of wilful error or fraud by the Service Provider. This

exclusion also applies to damage caused by third parties, unless the Service Provider is held contractually responsible pursuant to express written agreements.

6.2 Exclusion of Consequential Damages.

In no event shall the Service Provider be liable for any indirect, incidental, special or consequential damages. This includes, but is not limited to, loss of profits, loss of revenue, reputational damage, reduced commercial value, loss of anticipated savings, loss or corruption of data, as well as interruption or downtime of business operations. This exclusion applies regardless of the cause or legal basis of the damage, and regardless of whether the possibility of such damage has been communicated to the Service Provider in advance. It also applies regardless of whether the liability is based on a contractual, non-contractual or other legal basis, even if the possibility of such damages has been communicated to the Service Provider in advance.

6.3 Indemnification by Customer.

Customer undertakes to fully indemnify, defend and hold harmless the Service Provider, as well as its employees, directors, agents and affiliates, from and against any and all claims, demands, losses, damages, costs and expenses (including reasonable attorneys' fees) arising out of or in connection with:

- Customer's failure to implement or insufficiently implement security measures or procedures recommended by the Service Provider;
- Any negligence, error, breach of contractual obligations or tort committed by the Client or its assigns;
- Decisions or actions taken by the Customer based on advice, analyses, recommendations or reports provided by the Service Provider, where the Service Provider shall not be liable except in the case of wilful error or fraud.

6.4 Professional Judgment Disclaimer.

The Customer acknowledges that the services provided by the Service Provider are of an advisory and supportive nature and are based on professional assessment within a constantly evolving technological domain. Although the Service Provider makes reasonable efforts to mitigate risks and formulate adequate recommendations, the ultimate responsibility for the decisions taken and the implementation of measures lies solely with the Customer.

7. Force Majeure.

Neither Party shall be liable for any failure or delay in the performance of its obligations under this Data Security Agreement, to the extent that it results from force majeure. Force

majeure means any event or circumstance beyond the reasonable control of a Party, which is not attributable to its fault or negligence, and which temporarily or permanently prevents the performance of its contractual obligations. This includes, but is not limited to, natural disasters, war, riots, terrorism, government action, pandemics, epidemics, power or network failures, infrastructure outages, strikes, and other events of a similar nature.

The Party affected by force majeure shall immediately inform the other Party in writing of the existence, nature, probable duration and consequences of the force majeure situation. The performance of the agreement is suspended for the duration of the force majeure, without giving rise to a right to compensation for the other Party. The affected Party shall take all reasonable measures to minimise the consequences of the force majeure event and to resume performance of its obligations as soon as reasonably practicable.

If the force majeure situation persists for more than sixty days, either Party may terminate the agreement in whole or in part by written notice, without judicial intervention and without being liable for any compensation.

8. Term and Termination.

This Data Security Agreement shall enter into force on the date of signature by both Parties or, if earlier, on the date on which these provisions are expressly referenced in a Customer Order, Statement of Work or other contractual document. It shall remain in force for as long as a valid contractual relationship exists between the Parties, whether under a master agreement or under an Order Form or Statement of Work, subject to early termination in accordance with the provisions below.

Customer shall have the right to terminate this Data Security Agreement, as well as any underlying Statements of Work, work orders or other applicable documents, without any compensation or penalty, subject to thirty (30) days' notice, if the Service Provider materially fails to comply with this Data Security Agreement, if the Service Provider is the subject of a security incident with a material impact on Customer or its affiliates, or if Customer becomes aware of a material deterioration in the Service Provider's security measures. Termination will be effective on the date specified in Customer's written notice.

Upon termination or expiration of this agreement, the Service Provider is obliged, at the option of the Customer, to return or securely destroy all Customer Data. The Service Provider shall thereby apply generally accepted standards and security practices, within a maximum period of ninety (90) days after receipt of the written notice, unless a shorter period is provided in an applicable Customer Order or Statement of Work. This obligation applies regardless of the location of the Customer Data, including on-premises, in data centers, cloud environments, or backups.

The Service Provider must confirm in writing upon termination or expiration that its access to Customer Assets, as well as that of all persons working under its responsibility, has been terminated or revoked in full. Upon Customer's request, the Service Provider must also provide written proof or certification of such termination or withdrawal.

The provisions of this Data Security Agreement that by their nature are intended to survive termination. This includes, but is not limited to, the provisions on confidentiality, liability, indemnification and applicable law.

9. Portability.

Neither Party may transfer, delegate or subcontract this Data Security Agreement, nor any rights or obligations arising from it, in whole or in part, to any third party without the prior written consent of the other Party. Such authorisation shall not be unreasonably refused or delayed.

Notwithstanding the foregoing, Customer may assign this Agreement, without the prior consent of the Service Provider, to an affiliate or in connection with a merger, acquisition, reorganization or transfer of assets, provided that the acquiring entity confirms in writing that it is bound by the terms of this Data Security Agreement. In that case, the Service Provider remains fully liable for the correct performance of its obligations under this agreement, even if they are performed in whole or in part by a third party.

Any assignment in violation of this provision is automatically null and void and without effect.

10. Entire Agreement.

This Data Security Agreement, together with the main agreement, applicable Customer Orders, Statements of Work and other written documents expressly referring to these provisions, constitutes the entire agreement between the Parties with respect to the security of data, Customer assets and information processing.

It replaces all prior oral or written agreements, declarations or proposals on the same subject. Nothing in any other contractual document shall affect this Data Security Agreement, unless expressly agreed to by both Parties in writing.

11. Governing Law and Jurisdiction.

This Data Security Agreement is exclusively governed by Belgian law, to the exclusion of private international law and the Vienna Sales Convention.

All disputes arising from or in connection with this agreement fall under the exclusive jurisdiction of the Antwerp Enterprise Court, Tongeren division. The parties undertake to seek to resolve any dispute in the first instance by written consultation within a reasonable time, without prejudice to the right to seek interim measures.

12. Appendix – Terminology used.

"Applicable Law" means all applicable laws, rules, regulations, and standards in each jurisdiction in which the Services are provided or where Customer Data or Confidential Information may be stored or processed. This includes, but is not limited to, privacy, data protection and information security legislation, including, but not limited to, the General Data Protection Regulation and national implementing laws.

"**Confidential Information**" means any information or material, regardless of its form (written, oral, electronic or otherwise) and medium, which is provided or made available to the receiving party under circumstances which reasonably show it to be confidential. This is true regardless of whether such information is expressly marked as confidential or proprietary. It also includes information that the providing party obtains from an affiliate or third party, and which is considered confidential by that party. The parties agree that this Security Agreement and its provisions constitute Confidential Information. Customer Data and Personal Data shall be considered Confidential Information of Customer and/or its affiliates, except to the extent that such information is already publicly accessible without breach of this Agreement.

"Customer Assets" means and includes all Customer Data, Customer Systems, and Customer Facilities.

"**Customer Data**" means any data, documents, information or material in any format or medium, which (i) is provided or made available to the Service Provider by or on behalf of the Customer or its affiliated entities, (ii) is collected, generated or processed by the Service Provider in the course of the performance of the Services, (iii) arises out of or relates to the use of the Services, Service Provider systems or infrastructure by Customer or its affiliated entities, or (iv) are derived from the foregoing categories. Customer Data also includes any derivative works, copies, edits, summaries, analyses, extracts, or reproductions of such data. Customer Personal Data and Confidential Information shall be deemed to be Customer Data.

"**Customer Facility(s)**" means any physical location, technical installation, or building, regardless of ownership structure or operational direction, used by Customer or its affiliated entities in connection with or in connection with the provision, support, or security of the Services.

"**Customer Systems**" means systems, networks, hardware, software, applications, databases and other information technology resources owned, controlled or available to Customer or its affiliated entities, whether or not through a third party. These systems are an integral part of the technical environment in which or through which the Services are provided, supported or secured.

"**Personal Data"** means: (1) any information that relates to an identified or identifiable natural person, device, or household, or (2) any information defined as "personally

identifiable information," "personal information," "personal data," or similar terms as defined under applicable law.

"**Process" or "Processing**" means any operation or set of operations with respect to Customer Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, making available, alignment, combination, restriction, erasure or destruction.

"**Security Incident**" means any event involving or reasonable suspicion of unauthorized or unlawful access to, alteration of, loss of, disclosure of, or disruption of the integrity, confidentiality, or availability of Customer Data, Customer assets, or systems managed by the Service Provider under this Agreement. This includes breaches of security measures that qualify as a data breach under applicable data protection laws.

"**Services"** refers to the services provided under the Agreement, including hosting services, support, professional services, cloud services, and other performance as specified in the relevant order form and/or statement of work.

"Service Provider Facilities" means any location or infrastructure used by the Service Provider for the performance of the Services or for the storage, processing, transmission or access of Customer Confidential Information, whether operated by the Service Provider or by a third party on its behalf.

"Service Provider Systems" means the systems, networks, hardware, software, applications, and other technologies used by or on behalf of the Service Provider to provide the Services or process Customer Confidential Information, whether under the control of the Service Provider or hosted by a third party.

"Affiliates" means any entity that directly or indirectly controls, is controlled by, or is under common control with a Party, where "control" is defined as the right to determine, directly or indirectly, the direction or policies of an entity through ownership of voting securities, agreement, or otherwise.