SOMMAIRE GÉNÉRAL / INHALTSVERZEICHNIS / TABLE OF CONTENTS

CLAUSE DE LANGUE ET DE PRIMAUTÉ / SPRACHEN- UND VORRANGKLAUSEL / LANGUAGE PREVALENCE CLAUSE

- DE : Dieses Dokument wird in deutscher, englischer und französischer Sprache bereitgestellt. Im Falle von Abweichungen, Auslegungskonflikten oder Streitigkeiten bezüglich der Bedeutung rechtlicher oder technischer Begriffe ist ausschließlich die deutsche Fassung maßgeblich.

- FR : Ce document est mis à la disposition du Client en allemand, anglais et français. En cas de contradiction, de divergence d'interprétation ou de litige concernant la signification de termes légaux ou techniques, la version allemande (*Deutsch*) prévaut de plein droit et de manière exclusive sur les versions anglaise et française.

- EN : This document is provided in German, English, and French for the Customer's convenience. In the event of any discrepancy, conflict of interpretation, or dispute regarding the meaning of legal or technical terms, the German version (*Deutsch*) shall prevail over the English and French versions.

AUFTRAGSVERARBEITUNGSVERTRAG (AVV / ART. 28 DS-GVO)

ZWISCHEN:

Delphisoft Deutschland GmbH, Gugelstraße 32B, D-91077 Neunkirchen am Brand, Deutschland, eingetragen im Handelsregister des Amtsgerichts Bamberg unter der Nummer HRB 10110. Nachfolgend bezeichnet als **„Auftragsverarbeiter“** oder **„Delphisoft“**.

UND:

Der juristischen Person, die in der vertraglichen Grundlage oder dem Bestellschein als Kunde identifiziert ist. Nachfolgend bezeichnet als **„Verantwortlicher“** oder **„Kunde“**.

§ 1 GEGENSTAND UND DAUER

1.1. Rechtlicher Rahmen und Formalisierung

Dieser Vertrag (AVV) formalisiert die gegenseitigen Verpflichtungen der Parteien im Bereich des Schutzes personenbezogener Daten gemäß den zwingenden Anforderungen von Artikel 28 der Datenschutz-Grundverordnung (DS-GVO).

1.2. Anwendungsbereich und technischer Umfang

Diese Vereinbarung gilt von Rechts wegen für alle Datenverarbeitungsvorgänge, die von Delphisoft automatisiert über die SaaS-Plattform „Akuity SOC“ (oder „Akuity Guard“) im Auftrag und nach Weisung des Kunden durchgeführt werden.

1.3. Dauer und vertragliche Verknüpfung

Die Dauer dieses AVV ist untrennbar mit der Dauer des über die AGB geregelten Haupt-SaaS-Abonnements verbunden. Seine Kündigung oder technische Aussetzung hat dieselben Auswirkungen auf die Datenverarbeitung.

§ 2 ZWECK UND SPEZIFIKATION DER VERARBEITUNG

Die Art, der Zweck, die Kategorien der betroffenen Personen und die Arten der personenbezogenen Daten, die Gegenstand der automatisierten Verarbeitung sind (insbesondere durch die kontinuierliche Abfrage alle 10 Minuten durch die Azure Logic Apps-Pipeline), sind in der **Anlage 1** dieses Vertrages explizit detailliert und festgelegt.

§ 3 PFLICHTEN VON DELPHISOFT

Delphisoft verpflichtet sich formell zur Einhaltung der folgenden kumulativen Verpflichtungen:

3.1. Ausschließliche Verarbeitung nach Weisung

Personenbezogene Daten nur auf der Grundlage dokumentierter und schriftlicher Weisungen des Kunden zu verarbeiten. Die Aktivierung der Ingestions-Flows und die Parametrierung der Microsoft Graph-APIs stellen die Hauptanweisung zur Ausführung dar.

3.2. Unverzügliche Warnpflicht

Den Kunden unverzüglich und schriftlich zu informieren, wenn sie der Ansicht ist, dass eine übermittelte Weisung einen offenkundigen Verstoß gegen die DS-GVO, das Recht der Europäischen Union oder die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) darstellt

3.3. Geheimhaltungspflicht

Sicherzustellen, dass das gesamte technische Personal (Cyber-Ingenieure, Entwickler), das zur Verarbeitung der Betriebsdaten berechtigt ist, einer strengen vertraglichen oder gesetzlichen Verschwiegenheits- und Berufsgeheimnispflicht unterliegt.

3.4. Logische Sicherheit

Alle in Anlage 3 dokumentierten technischen und organisatorischen Maßnahmen (TOMs) umzusetzen und aufrechtzuerhalten, um ein den Cyber-Risiken angemessenes Sicherheitsniveau zu gewährleisten.

§ 4 UNTERAUFTRAGSVERHÄLTNISSE

4.1. Allgemeine Genehmigung

Der Kunde erteilt Delphisoft hiermit eine allgemeine schriftliche Genehmigung zur Beauftragung weiterer Auftragsverarbeiter (*Sub-processors*). Die am Tag der Unterzeichnung gültige Erstliste der Auftragsverarbeiter ist in der **Anlage 2** beigefügt.

4.2. Änderungsverfahren

Delphisoft verpflichtet sich, dem Kunden jede geplante Hinzufügung oder Ersetzung eines weiteren Auftragsverarbeiters mindestens fünfzehn (15) Kalendertage vor dessen technischem Inkrafttreten schriftlich anzuzeigen. Der Kunde verfügt über eine Frist von 15 Tagen ab Erhalt dieser Benachrichtigung, um einen schriftlichen und begründeten Einspruch zu erheben, der auf schwerwiegenden Sicherheitskriterien beruht. Erfolgt innerhalb dieser Frist kein Einspruch, gilt der weitere Auftragsverarbeiter als endgültig genehmigt.

§ 5 RECHTE DER BETROFFENEN PERSONEN

5.1. Technische Unterstützung

Angesichts der Art der Verarbeitung im autonomen SaaS-Modus unterstützt Delphisoft den Kunden durch entsprechende Softwarekonfigurationen und Extraktionswerkzeuge dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen (Rechte auf Auskunft, Berichtigung, Löschung oder Widerspruch) nachzukommen.

5.2. Weiterleitung von Anträgen

Erhält Delphisoft einen Antrag auf Wahrnehmung von Rechten, der direkt von einem Mitarbeiter oder Endnutzer des Kunden stammt, ist es ihr untersagt, darauf zu antworten, und sie leitet diesen unverzüglich auf elektronischem Weg an den Kunden weiter.

§ 6 MELDUNG VON DATENSCHUTZVERLETZUNGEN

Delphisoft verpflichtet sich, dem Kunden jede Verletzung des Schutzes personenbezogener Daten (*Data Breach*), die die logische Sicherheit seines Workspace beeinträchtigt, innerhalb von maximal achtundvierzig (48) Stunden nach Kenntnisnahme schriftlich über die offiziellen Kanäle des technischen Supports zu melden. Diese schriftliche Meldung wird so dokumentiert, dass der Kunde seinen Informationspflichten gegenüber der zuständigen Aufsichtsbehörde, insbesondere dem *Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)*, nachkommen kann.

§ 7 UNTERSTÜTZUNG UND DATENSCHUTZ-FOLGENABSCHÄTZUNGEN

Delphisoft stellt dem Kunden die angemessene Unterstützung und die erforderliche Infrastrukturdokumentation (wie ihr Technisches Weißbuch) zur Verfügung, damit dieser die Einhaltung der Artikel 32 bis 36 der DS-GVO gewährleisten kann, insbesondere für die Durchführung von Datenschutz-Folgenabschätzungen (DSFA), die durch die Integration der beratenden KI Google Gemini erforderlich werden.

§ 8 KONTROLLRECHTE DES KUNDEN

8.1. Rahmen des jährlichen Audits

Der Kunde ist berechtigt, einmal pro Vertragsjahr auf eigene Kosten ein dokumentarisches Compliance-Audit durchzuführen, indem er einen externen, unabhängigen Prüfer beauftragt, der gesetzlich zur Verschwiegenheit verpflichtet ist.

8.2. Modalitäten der Durchführung

Dieses Audit muss Delphisoft zwingend schriftlich mit einer Frist von mindestens dreißig (30) Werktagen angekündigt werden, darf ausschließlich während der Geschäftszeiten des Unternehmens stattfinden und darf den Betrieb der SaaS-Plattform oder die Sicherheit der Workspaces anderer Kunden in keiner Weise stören. Delphisoft verpflichtet sich, dem Prüfer ihre internen Sicherheitsrichtlinien, ihr Technisches Weißbuch und ihre Rückverfolgbarkeitsprotokolle (Logs) zu übermitteln, um diese Überprüfung zu ermöglichen.

§ 9 VERBLEIB DER DATEN BEI VERTRAGSENDE

Gemäß den in Artikel 8 der AGB definierten Bedingungen für die Vertragslaufzeit und den Lebenszyklus versendet Delphisoft bei Kündigung des Abonnements oder nach Ablauf einer 14-tägigen Testphase automatisch eine Abschluss-E-Mail, die eine vollständige Kopie der Betriebsdaten in Form einer bereinigten CSV-Datei enthält. Nach Ablauf der Nachfrist von 30 Tagen löscht Delphisoft alle in der PostgreSQL-Produktionsdatenbank gespeicherten personenbezogenen Daten endgültig, unwiderruflich und vollständig, es sei denn, es besteht eine gesetzliche Aufbewahrungspflicht nach deutschem Handels- oder Steuerrecht.

§ 10 HAFTUNG UND SCHLUSSBESTIMMUNGEN

10.1. Vorrang der AGB

Die Parteien vereinbaren ausdrücklich, dass die gesamte und kumulative zivilrechtliche Haftung aus Verletzungen dieses AVV vollständig den finanziellen Obergrenzen und Haftungsausschlüssen unterliegt, die in Artikel 12 der AGB (Allgemeine Geschäftsbedingungen) von Delphisoft geregelt und begrenzt sind.

10.2. Vorrang vor Drittvereinbarungen

Im Falle von Widersprüchen zwischen den Bestimmungen dieses AVV und anderen vertraglichen Dokumenten, die die Parteien binden, gehen die Bestimmungen dieser Vereinbarung vor, soweit es sich um die strikten Verpflichtungen zum Schutz personenbezogener Daten handelt.

ANLAGE 1: DETAILS DER VERARBEITUNG

- **Zweck**: Automatisierte Erfassung, Korrelation, temporäre Speicherung und Anreicherung durch Sprachmodelle (KI) von Microsoft Defender XDR-Incident-Logs zur Echtzeitüberwachung, zum Threat Hunting und für SOAR-Eindämmungsmaßnahmen.
- **Betroffene Personen**: Mitarbeiter, Kollegen, Unterauftragnehmer und Endadministratoren des Kunden, die den überwachten Microsoft-Tenants zugeordnet sind.
- **Verarbeitete Daten**: Profil-IDs (UPN, geschäftliche E-Mails, Entra ID-ID); Technische Daten und Protokolle (öffentliche IPs, Geolokalisierungsdaten der Warnmeldungen, Microsoft Device ID); Sicherheitsmetadaten (Rohbeschreibungen von Microsoft Defender XDR-Incidents, die kontextuell personenbezogene Daten in den Angriffslogs enthalten können).

ANNEXE 2 : AUFTRAGSVERARBEITER

Weitere Auftragsverarbeiter	Erbrachte Leistung	Physischer Standort der Daten	Übermittlungsgarantien
Microsoft Ireland Operations Ltd.	Ausführung der Ingestions-Pipeline (Azure Logic Apps), Graph-API-Routing und Azure Key Vault.	Azure-Region germany-west-central (Frankfurt, Deutschland).	Speicherung und Verarbeitung innerhalb der EU.
Supabase Inc. / AWS	Hosting der zentralisierten transaktionalen PostgreSQL-Datenbank.	AWS-Region Europa eu-central-1 (Frankfurt, Deutschland).	Speicherung innerhalb der EU. Standardvertragsklauseln (SCC).
Google Cloud EMEA Ltd.	API zur Anreicherung und Analyse durch KI (Vertex AI / Gemini Pro).	Google Cloud-Region Europa (EU). Endpunkt: aiplatform.eu.rep.googleapis.com / locations/eu/*.	Verarbeitung innerhalb der EU. Keine Speicherung oder Wiederverwendung für Training. Standardvertragsklauseln (SCC).
Vercel Inc.	Hosting der Benutzeroberfläche (Frontend Next.js) und Ausführung der Edge-Routing-Middlewares.	Region Frankfurt, Deutschland (West) – eu-central-1 (fra1).	Lokalisierte Edge-Verarbeitung in Deutschland. Standardvertragsklauseln (SCC).
Resend Inc.	Weiterleitung und Versand von transaktionalen E-Mails (Warnmeldungen und Berichte).	AWS-Cloud-Infrastrukturen.	Enthält nur die E-Mail-Adresse des Empfänger-Analysten. Standardvertragsklauseln (SCC).

ANLAGE 3: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOMs)

- **Physische Sicherheit**: Die Daten werden in Tier III/Tier IV-Rechenzentren von Microsoft Azure und AWS in Frankfurt verarbeitet, die über biometrische Zugangskontrollen und eine kontinuierliche 24/7-Überwachung verfügen.
- **Zugriffssicherheit**: Vertragliche und technische Verpflichtung zur Aktivierung von MFA (AAL2) für alle Analysten, die sich mit dem Cockpit verbinden. Verwendung von JWT-Token mit begrenzter Lebensdauer und dem Azure Key Vault für API-Schlüssel.
- **Multi-Tenant-Isolierung**: Native Implementierung der logischen Isolierung auf Ebene der PostgreSQL-Datenbank (Supabase) über Row-Level Security (RLS)-Regeln. Die eindeutige gehashte ID des Workspace wird bei jeder Transaktion kryptografisch überprüft.
- **Verschlüsselung**: Systematische Nutzung des TLS 1.3-Protokolls (HTTPS) für Daten im Transit und des AES-256-Algorithmus für die transparente Verschlüsselung im Ruhezustand (Encryption at rest) auf Supabase-Volumes.
- **Bereinigung exportierter Daten**: Systematische algorithmische Bereinigung bei der Generierung von CSV-Exports (Schutz vor Excel-Formelinjektionen und XSS-Schwachstellen).
- **Applikative Resilienz**: Next.js / Server Actions-Architektur mit Try-Catch-Blöcken und Error Boundaries, um Fehler von Drittanbieter-APIs zu isolieren, ohne Ausfälle oder Datenbankkorruption zu verursachen.

ACCORD DE SOUS-TRAITANCE DE DONNÉES PERSONNELLES (ART. 28 RGPD)

ENTRE :

Delphisoft Deutschland GmbH, Gugelstraße 32B, D-91077 Neunkirchen am Brand, Allemagne, immatriculée au Amtsgericht de Bamberg sous le numéro HRB 10110.

Ci-après dénommée "le Sous-traitant" ou "Delphisoft".

ET :

La personne morale identifiée comme Client dans la Base Contractuelle ou le Bon de Commande.

Ci-après dénommée "le Responsable de traitement" ou "le Client".

§ 1 OBJET ET DURÉE

1.1. Cadre juridique et formalisation

Le présent contrat (AVV) formalise les obligations réciproques des Parties en matière de protection des données à caractère personnel, conformément aux exigences impératives de l'article 28 du Règlement Général sur la Protection des Données (RGPD).

1.2. Champ d'application et périmètre technique

Le présent accord s'applique de plein droit à l'ensemble des opérations de traitement de données exécutées de manière automatisée par Delphisoft via la plateforme SaaS "Akuity SOC" (ou "Akuity Guard") pour le compte et sur instructions du Client.

1.3. Durée et corrélation contractuelle

La durée du présent AVV est intrinsèquement liée à la durée de l'abonnement SaaS principal régi par les AGB. Sa résiliation ou sa suspension technique entraîne les mêmes effets sur le traitement des données.

§ 2 FINALITE ET SPECIFICATION DU TRAITEMENT

La nature, la finalité, les catégories de personnes concernées et les types de données personnelles faisant l'objet du traitement automatisé (notamment via l'interrogation continue effectuée toutes les 10 minutes par le pipeline Azure Logic Apps) sont explicitement détaillés et figés au sein de l'Anlage 1 (Annexe 1) du présent contrat.

§ 3 OBLIGATIONS DE DELPHISOFT

Delphisoft s'engage formellement à respecter les obligations cumulatives suivantes :

3.1. Traitement exclusif sur instructions

Ne traiter les données personnelles que sur la base d'instructions documentées et écrites du Client. L'activation des flux d'ingestion et le paramétrage des API Microsoft Graph constituent l'instruction principale d'exécution.

3.2. Devoir d'alerte immédiat

Informer immédiatement et par écrit le Client si elle estime qu'une instruction transmise constitue une violation manifeste du RGPD, du droit de l'Union Européenne ou des dispositions de la loi fédérale allemande sur la protection des données (BDSG).

3.3. Obligation de secret

Veiller à ce que l'ensemble du personnel technique (ingénieurs cyber, développeurs) habilité à traiter les données d'exploitation soit soumis à une obligation contractuelle ou légale stricte de confidentialité et de secret professionnel.

3.4. Sécurité logique

Mettre en œuvre et maintenir l'ensemble des mesures techniques et organisationnelles (TOMs) documentées à l'Anlage 3 afin d'assurer un niveau de sécurité adapté aux risques cyber.

§ 4 SOUS-TRAITANCE ULTERIEURE

4.1. Autorisation générale

Le Client octroie par les présentes une autorisation générale écrite à Delphisoft pour recruter des sous-traitants ultérieurs (*Sub-processors*). La liste initiale des sous-traitants validée au jour de la signature est annexée à l'Anlage 2.

4.2. Procédure de modification

Delphisoft s'oblige à notifier par écrit au Client tout projet d'ajout ou de remplacement d'un sous-traitant ultérieur au moins quinze (15) jours calendaires avant sa prise d'effet technique. Le Client dispose d'un délai de 15 jours à compter de la réception de cette notification pour émettre une objection écrite et motivée reposant sur des critères sérieux de sécurité. À défaut d'objection dans ce délai, le sous-traitant est réputé définitivement agréé.

§ 5 DROITS DES PERSONNES CONCERNEES

5.1. Assistance technique

Compte tenu de la nature du traitement en mode SaaS autonome, Delphisoft aide le Client, par le biais de configurations logicielles et d'outils d'extraction appropriés, à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées (droits d'accès, de rectification, de suppression ou d'opposition).

5.2. Transmission des demandes

Si Delphisoft reçoit une demande d'exercice de droits émanant directement d'un collaborateur ou utilisateur final du Client, elle s'interdit d'y répondre et la réoriente sans délai vers le Client par voie électronique.

§ 6 NOTIFICATION DES VIOLATIONS DE DONNEES

Delphisoft s'engage à notifier au Client par écrit, par les canaux officiels du support technique, toute violation de données à caractère personnel (*Data Breach*) affectant la sécurité logique de son Workspace, dans un délai maximal de quarante-huit (48) heures après en avoir pris connaissance. Cette notification écrite sera documentée de manière à permettre au Client de remplir ses obligations de déclaration auprès de l'autorité de contrôle compétente, notamment le *Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)*.

§ 7 ASSISTANCE ET ANALYSES D'IMPACT

Delphisoft fournit au Client l'assistance raisonnable et les documentations d'infrastructure nécessaires (telles que son Livre Blanc Technique) pour lui permettre de garantir sa conformité aux articles 32 à 36 du RGPD, notamment pour la réalisation d'analyses d'impact relatives à la protection des données (AIPD / *DSFA*) rendues obligatoires par l'intégration de l'IA consultative Google Gemini.

§ 8 DROITS DE CONTROLE DU CLIENT

8.1. Cadre de l'audit annuel

Le Client est autorisé à mener un audit documentaire de conformité une fois par année contractuelle, à ses frais exclusifs, en mandatant un auditeur externe indépendant soumis réglementairement au secret professionnel.

8.2. Modalités d'exécution

Cet audit doit obligatoirement être notifié par écrit à Delphisoft avec un préavis minimal de trente (30) jours ouvrables, s'exécuter exclusivement pendant les heures d'ouverture de l'entreprise et ne présenter aucun caractère perturbateur pour l'exploitation de la plateforme SaaS ou la sécurité des autres workspaces clients. Delphisoft s'engage à transmettre à l'auditeur ses politiques de sécurité internes, son Livre Blanc Technique et ses journaux de traçabilité pour satisfaire à cette vérification.

§ 9 SORT DES DONNEES EN FIN DE CONTRAT

Conformément aux modalités d'engagement et de cycle de vie définies à l'Article 8 des AGB, lors de la résiliation de l'abonnement ou du terme d'un essai de 14 jours, Delphisoft procède automatiquement à l'envoi d'un e-mail de clôture contenant une copie exhaustive des données opérationnelles sous forme de fichier CSV assaini. À l'expiration du délai de grâce de 30 jours, Delphisoft détruit de manière définitive, irréversible et complète l'ensemble des données personnelles stockées dans la base PostgreSQL de production, sauf obligation légale de conservation imposée par le droit commercial ou fiscal allemand.

§ 10 RESPONSABILITÉ ET CLAUSES FINALES

10.1. Primauté des AGB

Les Parties conviennent expressément que la responsabilité civile globale et cumulative découlant des manquements au présent AVV est intégralement soumise, régie et limitée par les plafonds financiers et les cadres d'exonérations définis à l'Article 12 des AGB (CGV) de Delphisoft.

10.2. Primauté sur les accords tiers

En cas de contradiction entre les dispositions du présent AVV et tout autre document contractuel liant les Parties, les clauses du présent accord prévalent s'agissant des obligations strictes de protection des données.

ANNEXE 1 : DÉTAILS DU TRAITEMENT

- Finalité : Collecte automatisée, corrélation, stockage temporaire et enrichissement par modèles linguistiques (IA) des logs d'incidents Microsoft Defender XDR pour la surveillance en temps réel, le *Threat Hunting* et les actions SOAR de confinement.
- Personnes concernées : Salariés, collaborateurs, sous-traitants et administrateurs du Client finaux rattachés aux locataires (*tenants*) Microsoft supervisés.
- Données traitées : Identifiants de profils (UPN, e-mails professionnels, ID Entra ID); Données techniques et logs (IP publiques, données de géolocalisation des alertes, Device ID Microsoft); Métadonnées de sécurité (descriptions brutes des incidents Microsoft Defender XDR pouvant contenir contextuellement des données nominatives incluses dans les logs d'attaque).

ANNEXE 2 : SOUS-TRAITANTS

Sous-traitant ultérieur	Prestation fournie	Localisation physique des données	Garanties de transfert
Microsoft Ireland Operations Ltd.	Exécution du pipeline d'ingestion (Azure Logic Apps), routage API Graph et Azure key Vault	Région Azure germany-west-central (Francfort, Allemagne).	Stockage et traitement au sein de l'UE.
Supabase Inc. / AWS	Hébergement de la base de données PostgreSQL transactionnelle centralisée.	Région AWS Europe eu-central-1 (Francfort, Allemagne).	Stockage au sein de l'UE. Clauses contractuelles types (SCC).
Google Cloud EMEA Ltd.	API d'enrichissement et d'analyse par IA (Vertex AI / Gemini Pro).	Région Google Cloud Europe (UE). Point de terminaison : aiplatform.eu.rep.googleapis.com / locations/eu/*.	Traitement au sein de l'UE. Pas de stockage ni de réutilisation pour entraînement Clauses contractuelles types (SCC).
Vercel Inc.	Hébergement de l'interface utilisateur (Frontend Next.js) et exécution des middlewares de routage Edge.	Région Francfort, Allemagne (West) – eu-central-1 (fra1).	Traitement Edge localisé en Allemagne. Clauses contractuelles types (SCC).
Resend Inc.	Acheminement et envoi des e-mails transactionnels (alertes et rapports).	Infrastructures Cloud AWS.	Contient uniquement l'adresse e-mail de l'analyste destinataire. Clauses contractuelles types (SCC).

ANNEXE 3 : MESURES TECHNIQUES ET ORGANISATIONNELLES

- Sécurité Physique : Les données sont traitées dans les centres de données Tier III/Tier IV de Microsoft Azure et d'AWS situés à Francfort, disposant de contrôles d'accès biométriques et d'une surveillance continue 24/7.
- Sécurité des Accès : Obligation contractuelle et technique d'activer le MFA (AAL2) pour l'ensemble des analystes se connectant au cockpit. Utilisation de jetons JWT à durée de vie limitée et coffre-fort Azure Key Vault pour les clés d'API.
- Isolation Multi-tenant : Implémentation native de l'isolation logique au niveau de la base de données PostgreSQL (Supabase) via des règles *Row-Level Security (RLS)*. L'identifiant haché unique du Workspace est vérifié cryptographiquement à chaque transaction.
- Chiffrement : Utilisation systématique du protocole TLS 1.3 (HTTPS) pour les données en transit et de l'algorithme AES-256 pour le chiffrement transparent au repos (*Encryption at rest*) sur les volumes Supabase.
- Assainissement des données exportées : Nettoyage algorithmique systématique lors de la génération des exports CSV (protection contre les injections de formules Excel et les failles XSS).
- Résilience applicative : Architecture Next.js / Server Actions construite avec des blocs *Try-Catch* et *Error Boundaries* pour isoler les erreurs d'API tierces sans provoquer d'indisponibilité ni de corruption de base de données.

DATA PROCESSING AGREEMENT (DPA / ART. 28 GDPR)

BETWEEN:

Delphisoft Deutschland GmbH, Gugelstraße 32B, D-91077 Neunkirchen am Brand, Germany, registered with the Amtsgericht of Bamberg under number HRB 10110. Hereinafter referred to as "the Processor" or "Delphisoft".

AND:

The legal entity identified as the Customer in the Contractual Base or the Purchase Order. Hereinafter referred to as "the Controller" or "the Customer".

§ 1 PURPOSE AND DURATION

1.1. Legal framework and formalization

This agreement (DPA) formalizes the mutual obligations of the Parties regarding personal data protection, in accordance with the mandatory requirements of Article 28 of the General Data Protection Regulation (GDPR).

1.2. Scope and technical perimeter

This agreement applies by operation of law to all data processing operations executed automatically by Delphisoft via the "Akuity SOC" (or "Akuity Guard") SaaS platform on behalf of and under the instructions of the Customer.

1.3. Duration and contractual correlation

The duration of this DPA is intrinsically linked to the duration of the main SaaS subscription governed by the AGB (Terms and Conditions). Its termination or technical suspension entails the same effects on data processing.

§ 2 PURPOSE AND SPECIFICATION OF PROCESSING

The nature, purpose, categories of data subjects, and types of personal data subject to automated processing (notably via the continuous polling performed every 10 minutes by the Azure Logic Apps pipeline) are explicitly detailed and fixed within Anlage 1 (Annex 1) of this agreement.

§ 3 OBLIGATIONS OF DELPHISOFT

Delphisoft formally undertakes to comply with the following cumulative obligations:

3.1. Processing exclusively on instructions

Process personal data only on the basis of documented and written instructions from the Customer. The activation of ingestion flows and the configuration of Microsoft Graph APIs constitute the main execution instruction.

3.2. Duty of immediate alert

Immediately inform the Customer in writing if it considers that a transmitted instruction constitutes a manifest violation of the GDPR, European Union law, or the provisions of the German Federal Data Protection Act (BDSG).

3.3. Obligation of secrecy

Ensure that all technical personnel (cyber engineers, developers) authorized to process operational data are bound by a strict contractual or statutory obligation of confidentiality and professional secrecy.

3.4. Logical security

Implement and maintain all technical and organizational measures (TOMs) documented in Anlage 3 to ensure a level of security appropriate to cyber risks.

§ 4 SUB-PROCESSING

4.1. General authorization

The Customer hereby grants a general written authorization to Delphisoft to engage sub-processors. The initial list of sub-processors approved as of the date of signature is annexed to Anlage 2.

4.2. Modification procedure

Delphisoft undertakes to notify the Customer in writing of any project to add or replace a sub-processor at least fifteen (15) calendar days prior to its technical effective date. The Customer has a period of 15 days from receipt of this notification to issue a written and reasoned objection based on serious security criteria. In the absence of an objection within this period, the sub-processor shall be deemed definitively approved.

§ 5 RIGHTS OF DATA SUBJECTS

5.1. Technical assistance

Given the nature of the processing in autonomous SaaS mode, Delphisoft assists the Customer, through appropriate software configurations and extraction tools, in fulfilling its obligation to respond to requests for exercising data subjects' rights (rights of access, rectification, erasure, or objection).

5.2. Forwarding of requests

If Delphisoft receives a request to exercise rights directly from an employee or end-user of the Customer, it shall refrain from responding to it and shall forward it without delay to the Customer by electronic means.

§ 6 NOTIFICATION OF DATA BREACHES

Delphisoft undertakes to notify the Customer in writing, via official technical support channels, of any personal data breach (*Data Breach*) affecting the logical security of its Workspace, within a maximum period of forty-eight (48) hours after becoming aware of it. This written notification will be documented in such a way as to enable the Customer to fulfill its reporting obligations to the competent supervisory authority, notably the *Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)*.

§ 7 ASSISTANCE AND IMPACT ASSESSMENTS

Delphisoft provides the Customer with reasonable assistance and necessary infrastructure documentation (such as its Technical White Paper) to enable it to ensure compliance with Articles 32 to 36 of the GDPR, particularly for conducting data protection impact assessments (DPIA / DSFA) made mandatory by the integration of the consultative AI Google Gemini.

§ 8 AUDIT RIGHTS OF THE CUSTOMER

8.1. Framework of the annual audit

The Customer is authorized to conduct a documentary compliance audit once per contractual year, at its sole expense, by mandating an independent external auditor legally bound by professional secrecy.

8.2. Modalities of execution

This audit must imperatively be notified in writing to Delphisoft with a minimum notice period of thirty (30) business days, executed exclusively during the company's business hours, and must not cause any disruption to the operation of the SaaS platform or the security of other customer workspaces. Delphisoft undertakes to transmit its internal security policies, Technical White Paper, and traceability logs to the auditor to satisfy this verification.

§ 9 FATE OF DATA AT CONTRACT END

In accordance with the engagement and lifecycle modalities defined in Article 8 of the AGB, upon termination of the subscription or the expiry of a 14-day trial, Delphisoft automatically sends a closing email containing an exhaustive copy of operational data in the form of a sanitized CSV file. Upon expiration of the 30-day grace period, Delphisoft definitively, irreversibly, and completely destroys all personal data stored in the production PostgreSQL database, unless a legal retention obligation is imposed by German commercial or tax law.

§ 10 LIABILITY AND FINAL CLAUSES

10.1. Prevalence of the AGB

The Parties expressly agree that the global and cumulative civil liability arising from breaches of this DPA is fully subject to, governed by, and limited by the financial caps and exemption frameworks defined in Article 12 of Delphisoft's AGB (Terms and Conditions).

10.2. Prevalence over third-party agreements

In the event of a conflict between the provisions of this DPA and any other contractual document binding the Parties, the clauses of this agreement shall prevail regarding strict data protection obligations.

ANNEX 1: DETAILS OF PROCESSING

- Purpose: Automated collection, correlation, temporary storage, and enhancement by language models (AI) of Microsoft Defender XDR incident logs for real-time monitoring, Threat Hunting, and SOAR containment actions.
- Data subjects: Employees, collaborators, sub-contractors, and end-customer administrators attached to the supervised Microsoft tenants.
- Processed data: Profile identifiers (UPN, professional emails, Entra ID ID); Technical data and logs (public IPs, alert geolocation data, Microsoft Device ID); Security metadata (raw descriptions of Microsoft Defender XDR incidents that may contextually contain nominative data included in attack logs).

ANNEX 2: SUB-PROCESSORS

Sub-processor	Service Provided	Physical Location of Data	Transfer Guarantees
Microsoft Ireland Operations Ltd.	Execution of the ingestion pipeline (Azure Logic Apps), Graph API routing, and Azure Key Vault.	Azure region germany-west-central (Frankfurt, Germany).	Storage and processing within the EU.
Supabase Inc. / AWS	Hosting of the centralized transactional PostgreSQL database.	AWS region Europe eu-central-1 (Frankfurt, Germany).	Storage within the EU. Standard Contractual Clauses (SCC).
Google Cloud EMEA Ltd.	API for enrichment and analysis by AI (Vertex AI / Gemini Pro).	Google Cloud Europe region (EU). Endpoint: aiplatform.eu.rep.googleapis.com / locations/eu/*.	Processing within the EU. No storage or reuse for training. Standard Contractual Clauses (SCC).
Vercel Inc.	Hosting of the user interface (Frontend Next.js) and execution of Edge routing middlewares.	Frankfurt, Germany region (West) – eu-central-1 (fra1).	Edge processing localized in Germany. Standard Contractual Clauses (SCC).
Resend Inc.	Routing and sending of transactional emails (alerts and reports).	AWS Cloud infrastructures.	Contains only the email address of the recipient analyst. Standard Contractual Clauses (SCC).

ANNEX 3: TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

- Physical Security: Data is processed in Tier III/Tier IV data centers of Microsoft Azure and AWS located in Frankfurt, featuring biometric access controls and continuous 24/7 monitoring.
- Access Security: Contractual and technical obligation to activate MFA (AAL2) for all analysts connecting to the cockpit. Use of limited-lifetime JWT tokens and Azure Key Vault for API keys.
- Multi-tenant Isolation: Native implementation of logical isolation at the PostgreSQL database level (Supabase) via Row-Level Security (RLS) rules. The unique hashed ID of the Workspace is cryptographically verified at each transaction.
- Encryption: Systematic use of the TLS 1.3 protocol (HTTPS) for data in transit and the AES-256 algorithm for transparent encryption at rest on Supabase volumes.
- Sanitization of exported data: Systematic algorithmic cleaning when generating CSV exports (protection against Excel formula injections and XSS vulnerabilities).
- Application resilience: Next.js / Server Actions architecture built with Try-Catch blocks and Error Boundaries to isolate third-party API errors without causing downtime or database corruption.