

SOMMAIRE GÉNÉRAL / INHALTSVERZEICHNIS / TABLE OF CONTENTS

DE : Datenschutzerklärung (Webseite & Applikation)	Page 2
FR : Politique de Confidentialité Globale (Site & Application)	Page 4
EN : Global Privacy Policy (Website & Application)	Page 6

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.

**Delphisoft Deutschland GmbH**

Gugelstraße 32B
D-91077 Neunkirchen am Brand
Tel.: +49 9131 6258966
E-Mail: info@delphisoft.de
Website: www.delphisoft.de

Sitz: Neunkirchen a. B.
Amtsgericht: Bamberg HRB 10110
Geschäftsführer: Jonathan Breyse
USt-IdNr.: DE318864149

Sparkasse Erlangen
IBAN: DE06 7635 0000 0060 0912 93
SWIFT: BYLADEM1ERH
Konto-Nr.: 60091293

DATENSCHUTZERKLÄRUNG – AKUITY SOC**ARTIKEL 1: VERANTWORTLICHER UND DATENSCHUTZBEAUFTRAGTER**

Der Verantwortliche für die Datenverarbeitung auf dieser Webseite und innerhalb der SaaS-Applikation Akuity SOC im Sinne der DS-GVO und des BDSG ist:

- Unternehmen: Delphisoft Deutschland GmbH, Gugelstraße 32B, D-91077 Neunkirchen am Brand, Deutschland.
- Handelsregister: Amtsgericht Bamberg HRB 10110 – USt-IdNr.: DE318864149.
- Gesetzlicher Vertreter (Geschäftsführer): Jonathan Breyse.
- DS-GVO / DPO Kontakt: support@delphisoft.de.

ARTIKEL 2: ALLGEMEINE BESTIMMUNGEN, HOSTING UND LOGISCHE SICHERHEIT**2.1. Verschlüsselung der Datenströme (SSL/TLS)**

Aus offensichtlichen Sicherheitsgründen und um das System vor dem Abfangen hochvertraulicher Daten zu schützen (insbesondere beim OAuth2-Onboarding und bei Konfigurationen von API-Schlüsseln), nutzt die gesamte Webseite und Applikation eine SSL- oder TLS-Verschlüsselung über HTTPS. Alle Anfragen, die zwischen Ihrem Browser und unseren Infrastrukturen übertragen werden, sind von Ende zu Ende verschlüsselt.

2.2. Hosting der Web-Infrastruktur (Vercel)

Die Benutzeroberfläche (Frontend Next.js) sowie die Edge-Middlewares für Routing und Token-Verifizierung werden von der Vercel Inc. gehostet. Um die Souveränität der Datenströme zu gewährleisten, hat Delphisoft seine Deployments so konfiguriert, dass sie ausschließlich im europäischen Rechenzentrum von Vercel in Frankfurt, Deutschland (West) – eu-central-1 – fra1, ausgeführt werden. Eine dauerhafte Speicherung personenbezogener Applikations-Logs durch diesen Dritten findet nicht statt.

2.3. Verwendung von Cookies und lokalen Speichertechnologien

Um eine flüssige Navigation zu ermöglichen und den Zugriff auf das Cockpit abzusichern, nutzt die Plattform Akuity SOC ausschließlich sogenannte „essentielle“ technische Cookies. Ohne Ihre ausdrückliche Zustimmung werden in der SaaS-Applikation keine Drittanbieter-Cookies zu Werbe- oder Marketing-Targeting-Zwecken gesetzt. Gemäß Artikel 6 Absatz 1 Buchstabe f) der DS-GVO und § 25 Absatz 2 des deutschen TDDDG sind diese Tracker von der Einwilligung befreit, da sie für die Bereitstellung des vom Nutzer ausdrücklich gewünschten Online-Kommunikationsdienstes unbedingt erforderlich sind.

Liste der von der Applikation verwendeten, unbedingt erforderlichen technischen Tracker:

- sb-access-token (Supabase Session Cookie):
 - *Art und Rolle:* Verschlüsseltes Session-Cookie, konfiguriert mit den Sicherheitsattributen „HTTP-Only“ und „Secure“. Es speichert das JWT-Authentifizierungstoken des Analysten.
 - *Zweck:* Aufrechterhaltung der aktiven Analysten-Sitzung, Überprüfung der logischen Zugriffsrechte und Abfangen von Verbindungen ohne MFA, um diese zum Sicherheits-Challenge (AAL1 zu AAL2) weiterzuleiten.
 - *Speicherdauer:* Wird beim Schließen des Browsers oder nach Ablauf des Sitzungstokens automatisch gelöscht.
- next-intl-locale (Internationalisierung):
 - *Art und Rolle:* Lokales technisches Cookie.
 - *Zweck:* Speichern der vom Analysten ausgewählten Interface-Sprache (Französisch, Deutsch oder Englisch), um die korrekte Anzeige von Menüs, Schaltflächen und während der Sitzung generierten Berichten sicherzustellen.
 - *Speicherdauer:* Persistent (begrenzt auf 1 Jahr).
- NEXT_JWT_MFA_CLAIM (Vercel Edge Middleware Context):
 - *Art und Rolle:* Technische Daten, die im Edge-Speicher (Vercel Runtime) verarbeitet werden.
 - *Zweck:* Ermöglicht es der Middleware, in weniger als 50ms sofort zu validieren, ob die aktive Sitzung über das erforderliche Vertrauensniveau verfügt, um eine kritische SOAR-Aktion (Blockierung, Isolation) auszuführen, wodurch schwere Serveranfragen vermieden werden.
 - *Speicherdauer:* Flüchtige Sitzung, die sofort bei der Abmeldung gelöscht wird.

ARTIKEL 3: VOLLSTÄNDIGE KARTOGRAFIE DER DATENVERARBEITUNG (DELPHISOFT ALS VERANTWORTLICHER)

Der Herausgeber verarbeitet die Daten von physischen Nutzern (Besucher, Interessenten, Kundenanalysten) ausschließlich zu den nachfolgend detailliert aufgeführten Zwecken:

A. Verarbeitung von Server-Logfiles (Server-Logfiles)

- *Verarbeitete Daten:* Browsertyp und -version, Betriebssystem, Referrer-URL, anonyme gehashte IP-Adresse, Datum und Uhrzeit der Anfrage. Diese Informationen werden vom Vercel-Server automatisch erfasst, sobald Sie einfach auf der

Webseite navigieren und Ihr Browser diese an uns übermittelt.

- *Zweck:* Gewährleistung der technischen Stabilität, Optimierung der Anzeige und Ermöglichung der Post-Incident-Analyse im Falle einer Cyberattacke (DDoS) gegen die Plattform.
- *Rechtsgrundlage:* Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DS-GVO) an einer stabilen und sicheren Webseite.
- *Speicherdauer:* Automatische Löschung innerhalb von 7 rollierenden Tagen.

B. Kontaktformulare und Demonstrationsanfragen (Sales-Led)

- *Verarbeitete Daten:* Name, Vorname, geschäftliche E-Mail-Adresse (generische Domains wie @gmail.com, @yahoo.fr usw. werden von unseren Algorithmen automatisch gefiltert und abgelehnt), Firmenname, gewähltes Profil (Direkt oder MSSP) und Inhalt der Anfrage.
- *Zweck:* Kommerzielle Kontaktaufnahme, Planung und Durchführung von geführten Demonstrationssitzungen durch unsere Cyber-Ingenieure.
- *Rechtsgrundlage:* Vorvertragliche Maßnahmen auf Anfrage des Interessenten (Art. 6 Abs. 1 lit. b DS-GVO).
- *Speicherdauer:* Die Daten werden für die Dauer aufbewahrt, die für die Bewertung der geschäftlichen Möglichkeit erforderlich ist, und maximal 12 Monate nach der letzten ergebnislosen Interaktion gelöscht.

C. Registrierung, Authentifizierung und Testphase (14 Tage Trial)

- *Verarbeitete Daten:* System-IDs, E-Mail-Adresse des Analysten, über Supabase Auth irreversibel gehashtes Passwort, Konfiguration und Aktivierungsstatus der MFA (TOTP-Geheimnisse), IP-Adresse bei der Authentifizierung und interne Audit-Logs (Rückverfolgbarkeit des Analysten, der eine SOAR-Aktion ausführt).
- *Zweck:* Bereitstellung des Test-Workspace, Erzwingen der obligatorischen Zwei-Faktor-Vertrauensebene (AAL2) zur Verhinderung von Session-Hijacking und Senden der Benachrichtigungs-E-Mail am 14. Tag, um den Wechsel zum kostenpflichtigen Modell anzubieten.
- *Rechtsgrundlage:* Erfüllung des kostenlosen Testvertrags (Art. 6 Abs. 1 lit. b DS-GVO).
- *Speicherdauer:* Wenn der Kunde das kostenpflichtige Abonnement ablehnt, werden der Workspace und alle damit verbundenen technischen Metadaten für eine Nachfrist von 30 Tagen aufbewahrt und anschließend einer automatischen, vollständigen und unwiderruflichen Bereinigung unterzogen.

**Delphisoft Deutschland GmbH**

Gugelstraße 32B
D-91077 Neunkirchen am Brand
Tel.: +49 9131 6258966
E-Mail: info@delphisoft.de
Website: www.delphisoft.de

Sitz: Neunkirchen a. B.
Amtsgericht: Bamberg HRB 10110
Geschäftsführer: Jonathan Breyse
USt-IdNr.: DE318864149

Sparkasse Erlangen
IBAN: DE06 7635 0000 0060 0912 93
SWIFT: BYLADEM1ERH
Konto-Nr.: 60091293

D. Rechnungsverwaltung und Quotenüberwachung

- Verarbeitete Daten: Physische Rechnungsadresse des Unternehmens, Kontaktdaten des Buchhaltungsansprechpartners, innergemeinschaftliche MwSt.-Nummer (vorbehaltlich der sofortigen Validierung über die VIES-API der Europäischen Kommission), exaktes Volumen der von unseren Pipelines erfassten Vorfälle und Anzahl der verknüpften aktiven Tenants.
- Zweck: Erstellung der monatlichen Rechnung im Nachhinein zu Beginn jedes Monats, Berechnung von Paketüberschreitungen (Overage billing) und Anwendung der Regeln zur sofortigen Aussetzung des Workspace am Tag 30 im Falle eines Zahlungsverzugs.
- Rechtsgrundlage: Erfüllung des Haupt-SaaS-Vertrags (Art. 6 Abs. 1 lit. b DS-GVO) und Einhaltung unserer gesetzlichen buchhalterischen und steuerlichen Verpflichtungen nach deutschem Recht (Art. 6 Abs. 1 lit. c DS-GVO).
- Speicherdauer: Gesetzliche Aufbewahrungspflicht von 10 Jahren für Rechnungen und Buchhaltungsunterlagen gemäß den Anforderungen der deutschen Abgabenordnung (AO).
- Zwingende Abgrenzung: Die Verarbeitung operativer Daten unserer Kunden (Rolle als Auftragsverarbeiter)

ARTIKEL 4: VON DER CHROME-ERWEITERUNG VERARBEITETE DATEN (AKUITY SOC COPILOT)**A. Authentifizierungs- und Sitzungsdaten (Lokaler Speicher)**

Die Erweiterung speichert dauerhaft im lokalen Speicher des Browsers (chrome.storage.local):

- Eindeutige Benutzererkennung (Supabase User ID) und Sitzungstoken (JWT): Erforderlich, um die aktive Sitzung des Analysten aufrechtzuerhalten und Anfragen an die API zu sichern.
- Sprachpräferenz: Die vom Analysten gewählte Sprache für die Anzeige der Erweiterungsoberfläche.

B. Browser-Kontextdaten (Tab-Lesezugriffe)

Die Erweiterung analysiert in Echtzeit den aktiven Browser-Tab, um ausschließlich Folgendes zu extrahieren:

- Die Microsoft Defender-Vorfall-ID (Incident ID) in der URL des aktiven Tabs (wenn der Host security.microsoft.com ist und der Pfad /incidents/{id} oder /incident2/{id} entspricht).
- Die Microsoft-Mandantenkennung (Tenant ID), die in den URL-Parametern (tid oder tenantid) vorhanden ist, um den Vorfall dem richtigen Kunden zuzuordnen.

Hinweis: Die Erweiterung ignoriert und sammelt keinen Browserverlauf für Websites und Tabs außerhalb des Microsoft Defender-Portals.

C. In der Benutzeroberfläche angezeigte Vorfalldaten (Side Panel / Seitenbereich)

Wenn die Erweiterung bei einem Microsoft Defender-Vorfall aktiv ist, ruft sie über die API ab und zeigt in ihrem Seitenbereich an:

- Vorfalldetails: Titel, KI-generierte Zusammenfassung, Schweregrad des Vorfalls.
- Beweismittel (Evidence & Assets): Listen der Zielmaschinen (Hostnames), der betroffenen Benutzer (UPNs/geschäftliche E-Mails), Kompromittierungsindikatoren (SHA-256-Datei-Hashes) und erkannte verdächtige Netzwerkverbindungen.

D. Daten zum KI-Austausch und Behebungsvorschläge (Chat)

Bei Verwendung des Tabs "KI-Assistent":

- Anfragen des Analysten: Ausgewählte vordefinierte Prompts (z. B. Anforderungen von KQL-Abfragen, PowerShell-Befehle zur Behebung, Auswirkungsanalyse usw.) oder vom Analysten eingegebene benutzerdefinierte Fragen.
- Konversationsverlauf: Wird vorübergehend und flüchtig im Sitzungsspeicher des Seitenbereichs (sessionStorage) gespeichert. Dieser Verlauf wird gelöscht, sobald die Browsersitzung geschlossen wird oder auf die Schaltfläche "Verlauf löschen" geklickt wird.

ARTIKEL 5: AUSSCHLUSS AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

Im Rahmen ihrer Anwendungsfunktion verbindet sich die Applikation Akuity SOC alle 10 Minuten über die Microsoft Graph-API mit den Produktionsumgebungen unserer Kunden, um dort Sicherheitswarnungen zu extrahieren. Dieser automatisierte Datenstrom erfasst Daten bezüglich der Endnutzer unserer Kunden (UPN, E-Mail-Adressen von Zielmitarbeitern, Azure AD-Kennungen, IP-Adressen der angegriffenen Endgeräte, Rohbeschreibungen von Vorfällen). Für alle diese Cyber-Überwachungsdaten handelt die Delphisoft Deutschland GmbH ausschließlich als Auftragsverarbeiter (Auftragsverarbeiter) im Sinne von Artikel 28 der DS-GVO. Diese Verarbeitungen werden nicht durch die vorliegende einseitige Richtlinie geregelt, sondern sind streng durch die im Rahmen der Kontoerstellung zwingend zu akzeptierenden Weisungen des Kunden innerhalb des Auftragsverarbeitungsvertrags (AVV / DPA) eingeraht. Delphisoft untersagt sich selbst, diese Daten für eigene Rechnung zu nutzen, einzusehen oder zu verwerten.

ARTIKEL 6: DATENWEITERGABE UND ZUGELASSENE WEITERE AUFTRAGSVERARBEITER (SUB-PROCESSORS)

Um das SaaS zu betreiben, stützt sich Delphisoft auf modernste technologische Infrastrukturen, deren Verarbeitung geografisch auf die Zone der Europäischen Union beschränkt ist:

- Supabase Inc.: Hosting unserer PostgreSQL-Produktionsdatenbank, isoliert durch RLS-Richtlinien, ansässig in der AWS-Region Frankfurt (Deutschland).
- Microsoft Ireland Operations Ltd.: Technische Ausführung unserer Ingestions-Pipelines (Azure Logic Apps), lokalisiert in der Azure-Region Germany West Central in Frankfurt (Deutschland).
- Google Cloud EMEA Ltd.: API für die KI-Anreicherung über Google Gemini via den souveränen europäischen Endpunkt aiplatform.eu.rep.googleapis.com (EU-Zone). Die gesendeten Anfragen sind vertraulich und werden von Google niemals gespeichert oder zur Schulung seiner Modelle genutzt.
- Resend Inc. / AWS: Technisches Routing von E-Mail-Warnmeldungen und transaktionalen Benachrichtigungen zur Schließung von Workspaces.

ARTIKEL 7: IHRE RECHTE ALS BETROFFENE PERSON (ART. 15-22 DS-GVO)

Als physischer Nutzer der Plattform (Analyst oder kommerzieller Kontakt) gewährt Ihnen die europäische und deutsche Gesetzgebung folgende Rechte gegenüber unserem Datenschutzbeauftragten:

- Auskunftsrecht (Art. 15 DS-GVO): Erhalt einer vollständigen Kopie der personenbezogenen Daten, die wir über Sie speichern.
- Recht auf Berichtigung (Art. 16 DS-GVO): Korrektur oder Aktualisierung eines unvollständigen oder fehlerhaften Profils.
- Recht auf Löschung (Art. 17 DS-GVO): Beantragung der Löschung Ihrer Informationen, vorbehaltlich dessen, dass für uns keine steuerliche oder gesetzliche Aufbewahrungspflicht mehr besteht.
- Widerspruchsrecht und Widerruf der Einwilligung (Art. 21 und 7 DS-GVO): Jederzeitiger Widerspruch gegen den Erhalt von E-Mails mit kommerziellen Informationen oder Widerruf einer Autorisierung.

Sie können alle diese Rechte ausüben, indem Sie einfach an die offizielle Adresse schreiben: support@delphisoft.de. Zudem haben Sie das Recht, eine Beschwerde bei der zuständigen Aufsichtsbehörde in Bayern einzureichen: Bayerisches Landesamt für Datenschutzaufsicht (BayLDA).



Delphisoft Deutschland GmbH

Gugelstraße 32B
D-91077 Neunkirchen am Brand
Tel.: +49 9131 6258966
E-Mail: info@delphisoft.de
Website: www.delphisoft.de

Sitz: Neunkirchen a. B.
Amtsgericht: Bamberg HRB 10110
Geschäftsführer: Jonathan Breyse
USt-IdNr.: DE318864149

Sparkasse Erlangen
IBAN: DE06 7635 0000 0060 0912 93
SWIFT: BYLADEM1ERH
Konto-Nr.: 60091293

DÉCLARATION DE PROTECTION DES DONNÉES – AKUITY SOC

ARTICLE 1 : RESPONSABLE DU TRAITEMENT ET DELEGUE A LA PROTECTION DES DONNEES

Le responsable du traitement des données sur ce site internet et au sein de l'application SaaS Akuity SOC au sens du RGPD et du BDSG est :

- Société : Delphisoft Deutschland GmbH, Gugelstraße 32B, D-91077 Neunkirchen am Brand, Allemagne .
- Immatriculation : Amtsgericht Bamberg HRB 10110 – USt-IdNr.: DE318864149.
- Représentant légal (Geschäftsführer) : Jonathan Breysse.
- Contact RGPD / DPO : support@delphisoft.de.

ARTICLE 2 : DISPOSITIONS GENERALES, HEBERGEMENT ET SECURITE LOGIQUE

2.1. Chiffrement des flux (SSL/TLS)

Pour des raisons de sécurité évidentes et pour prémunir le système contre l'interception de données hautement confidentielles (notamment lors de l'onboarding OAuth2 et des configurations de clés d'API), l'intégralité du site et de l'application utilise un chiffrement de type SSL ou TLS via HTTPS. Toutes les requêtes transitent entre votre navigateur et nos infrastructures sont chiffrées de bout en bout.

2.2. Hébergement de l'infrastructure web (Vercel)

L'interface utilisateur (Frontend Next.js) et les middlewares Edge de routage et de vérification des jetons sont hébergés auprès de la société Vercel Inc.. Afin de garantir la souveraineté des flux, Delphisoft a configuré ses déploiements pour s'exécuter exclusivement au sein du centre de données européen de Vercel situé à Francfort, Allemagne (West) – eu-central-1 – fra1. Aucun stockage de logs applicatifs nominatifs n'est opéré de manière permanente par ce tiers.

2.3. Utilisation des Cookies et Technologies de Stockage Local

Pour offrir une navigation fluide et sécuriser l'accès au cockpit, la plateforme Akuity SOC utilise exclusivement des cookies techniques dits "essentiels". Aucun cookie tiers à visée publicitaire ou de ciblage marketing n'est déposé sur l'application SaaS sans votre accord exprès.

Conformément à l'article 6, paragraphe 1, point f) du RGPD et au § 25, paragraphe 2 du TDDDG allemand, ces traceurs sont dispensés de consentement car ils sont strictement indispensables à la fourniture du service de communication en ligne expressément demandé par l'utilisateur.

Liste des traceurs techniques indispensables utilisés par l'application :

- **sb-access-token (Supabase Session Cookie) :** *
 - *Nature et rôle* : Cookie de session chiffré, configuré avec les attributs de sécurité *HTTP-Only* et *Secure*. Il stocke le jeton JWT d'authentification de l'analyste.
 - *Finalité* : Maintenir la session de l'analyste active, vérifier ses droits d'accès logiques et intercepter les connexions sans MFA afin de les rediriger vers le challenge de sécurité (AAL1 vers AAL2).
 - *Durée de conservation* : Supprimé automatiquement à la fermeture du navigateur ou à l'expiration du jeton de session.
- **next-intl-locale (Internationalisation) :**
 - *Nature et rôle* : Cookie technique local.
 - *Finalité* : Mémoriser la langue d'interface sélectionnée par l'analyste (Français, Allemand ou Anglais) pour assurer l'affichage correct des menus, des boutons et des rapports générés au cours de sa session.
 - *Durée de conservation* : Persistant (limité à 1 an).
- **NEXT_JWT_MFA_CLAIM (Vercel Edge Middleware Context) :**
 - *Nature et rôle* : Donnée technique traitée en mémoire Edge (Vercel Runtime).
 - *Finalité* : Permettre au middleware de valider instantanément, en moins de 50ms, si la session active dispose du niveau de confiance requis pour exécuter une action SOAR critique (blocage, isolation), évitant ainsi les requêtes serveurs lourdes.
 - *Durée de conservation* : Session volatile, effacée immédiatement à la déconnexion.

ARTICLE 3 : CARTOGRAPHIE EXHAUSTIVE DES TRAITEMENTS DE DONNEES (DELPHISOFT EN TANT QUE RESPONSABLE)

L'éditeur traite les données des utilisateurs physiques (visiteurs, prospects, analystes clients) pour les finalités exclusives détaillées ci-après :

A. Traitement des fichiers journaux du serveur (Server-Logfiles)

Lors de la simple navigation sur le site, le serveur Vercel collecte automatiquement des informations que votre navigateur nous transmet.

- Données traitées : Type et version du navigateur, système d'exploitation, URL de provenance (referrer), adresse IP hachée anonyme, date et heure de la requête.
- Finalité : Assurer la stabilité technique, optimiser l'affichage et permettre l'analyse post-incident en cas de cyberattaque (DDoS) contre la plateforme.

- Base juridique : Intérêt légitime (Art. 6, par. 1, al. f du RGPD) à disposer d'un site stable et sécurisé.
- Durée de conservation : Suppression automatisée sous 7 jours glissants.

B. Formulaires de contact et Demandes de Démonstration (Sales-Led)

- Données traitées : Nom, prénom, e-mail professionnel (les domaines génériques @gmail.com, @yahoo.fr, etc. sont filtrés et rejetés d'office par nos algorithmes), raison sociale, profil choisi (Direct ou MSSP), et contenu de la demande .
- Finalité : Prise de contact commerciale, planification et exécution des sessions de démonstration guidées par nos cyber-ingénieurs.
- Base juridique : Mesures précontractuelles prises à la demande du prospect (Art. 6, par. 1, al. b du RGPD).
- Durée de conservation : Les données sont conservées pendant toute la durée nécessaire à l'évaluation de l'opportunité commerciale, et supprimées au maximum 12 mois après la dernière interaction sans suite.

C. Inscription, Authentification et Période d'Essai (Trial 14 jours)

- Données traitées : Identifiants système, e-mail de l'analyste, mot de passe haché de manière irréversible via Supabase Auth, configuration et état d'enrôlement du MFA (secrets TOTP), adresse IP lors de l'authentification et logs d'audit interne (traçabilité de l'analyste qui exécute une action SOAR).
- Finalité : Provisionner le Workspace d'essai, forcer le contrôle de niveau de confiance double-facteur (AAL2) obligatoire pour bloquer les vols de session, et envoyer l'e-mail de notification au 14ème jour proposant de basculer vers le modèle payant.
- Base juridique : Exécution du contrat d'essai gratuit (Art. 6, par. 1, al. b du RGPD).
- Durée de conservation : Si le client refuse l'abonnement payant, le Workspace et toutes les métadonnées techniques associées sont conservés pendant un délai de grâce de 30 jours, puis font l'objet d'une purge automatique, complète et irréversible.

D. Gestion de la Facturation et Suivi des Quotas

- Données traitées : Adresse physique de facturation de l'entreprise, coordonnées du contact comptable, numéro de TVA intracommunautaire (soumis à validation instantanée via l'API VIES de la Commission Européenne), volume exact des incidents comptabilisés par nos pipelines et nombre de locataires actifs rattachés.
- Finalité : Émettre la facture mensuelle à terme échu au début de chaque mois, calculer les



Delphisoft Deutschland GmbH

Gugelstraße 32B
D-91077 Neunkirchen am Brand
Tel.: +49 9131 6258966
E-Mail: info@delphisoft.de
Website: www.delphisoft.de

Sitz: Neunkirchen a. B.
Amtsgericht: Bamberg HRB 10110
Geschäftsführer: Jonathan Breysse
USt-IdNr.: DE318864149

Sparkasse Erlangen
IBAN: DE06 7635 0000 0060 0912 93
SWIFT: BYLADEM1ERH
Konto-Nr.: 60091293

dépassements de forfaits (Overage billing), et appliquer les règles de suspension immédiate du Workspace à J+30 en cas de défaut de paiement.

- Base juridique : Exécution du contrat SaaS principal (Art. 6, par. 1, al. b du RGPD) et respect de nos obligations légales comptables et fiscales selon le droit allemand (Art. 6, par. 1, al. c du RGPD).
- Durée de conservation : Archivage légal obligatoire de 10 ans pour les factures et pièces comptables, conformément aux exigences du Code fiscal allemand (Abgabenordnung - AO).
- Démarcation impérative : Le traitement des données opérationnelles de nos clients (Rôle de Sous-traitant)

ARTICLE 4 : DONNEES TRAITEES PAR L'EXTENSION CHROME (AKUITY SOC COPILOT)

A. Données d'authentification et de session (Stockage local)

L'extension stocke de façon persistante dans le stockage local du navigateur (chrome.storage.local) :

- Identifiant utilisateur unique (Supabase User ID) et jeton de session (JWT) : Nécessaires pour maintenir la session active de l'analyste et sécuriser les requêtes vers l'API.
- Préférence linguistique : La langue choisie par l'analyste pour l'affichage de l'interface de l'extension.

B. Données de contexte de navigation (Lectures d'onglets)

L'extension analyse en temps réel l'onglet actif du navigateur pour extraire uniquement :

- L'identifiant de l'incident Microsoft Defender dans l'URL de l'onglet actif (lorsque l'hôte est security.microsoft.com et le chemin correspond à /incidents/{id} ou /incident2/{id}).
- L'identifiant de locataire Microsoft (Tenant ID) présent dans les paramètres d'URL (tid ou tenantid) afin d'associer l'incident au bon client.

Note : L'extension ignore et ne collecte aucun historique de navigation pour les sites et onglets en dehors du portail Microsoft Defender.

C. Données d'incidents affichées dans l'interface (Side Panel)

Lorsque l'extension est active sur un incident Microsoft Defender, elle récupère de l'API et affiche dans son panneau latéral :

- Les détails de l'incident : Titre, résumé généré par l'IA, niveau de sévérité de l'incident.
- Les éléments de preuve (Evidence & Assets) : Listes des machines ciblées (Hostnames), des utilisateurs concernés (UPNs/Emails professionnel), des

indicateurs de compromission (hashes de fichiers SHA-256) et des connexions réseau suspectes détectées.

D. Données d'échanges avec l'IA et suggestions de remédiation (Chat)

Lors de l'utilisation de l'onglet "Assistant IA" :

- Requêtes de l'analyste : Prompts prédéfinis sélectionnés (ex. : demandes de requêtes KQL, commandes PowerShell de remédiation, analyse d'impact, etc.) ou questions personnalisées saisies par l'analyste.
- Historique de la conversation : Stocké de manière temporaire et volatile dans la mémoire de session du panneau latéral (sessionStorage). Cet historique est effacé dès la fermeture de la session de navigation ou au clic sur le bouton "Effacer l'historique".

ARTICLE 5 : EXCLUSION CONTRAT DE SOUS-TRAITANCE (AVV)

Dans le cadre de son fonctionnement applicatif, l'application Akuity SOC se connecte toutes les 10 minutes via l'API Microsoft Graph aux environnements de production de nos clients pour y extraire les alertes de sécurité.

Ce flux automatisé ingère des données relatives aux utilisateurs finaux de nos clients (UPN, adresses e-mail de collaborateurs cibles, identifiants Azure AD, adresses IP des terminaux attaqués, descriptions brutes des incidents).

Pour l'ensemble de ces données de supervision cyber, Delphisoft Deutschland GmbH agit exclusivement en qualité de Sous-traitant (*Auftragsverarbeiter*) au sens de l'article 28 du RGPD. Ces traitements ne sont pas régis par la présente politique unilatérale, mais sont encadrés de manière stricte par les instructions du Client formalisées au sein de l'*Auftragsverarbeitungsvertrag* (AVV / DPA) accepté obligatoirement lors de la création du compte. Delphisoft s'interdit d'utiliser, de consulter ou de valoriser ces données pour son propre compte.

ARTICLE 6 : PARTAGE DES DONNEES ET SOUS-TRAITANTS ULTERIEURS AUTORISES (SUB-PROCESSORS)

Pour faire fonctionner le SaaS, Delphisoft s'appuie sur des infrastructures technologiques de pointe dont le traitement est géographiquement restreint à la zone Union Européenne :

- Supabase Inc. : Hébergement de notre base PostgreSQL de production, isolée par politiques RLS, située sur la région AWS Francfort (Allemagne).
- Microsoft Ireland Operations Ltd. : Exécution technique de nos pipelines d'ingestion (Azure Logic Apps) localisés sur la région Azure Germany West Central à Francfort (Allemagne).

- Google Cloud EMEA Ltd. : API d'enrichissement IA Google Gemini via le point de terminaison européen souverain aiplatform.eu.rep.googleapis.com (Zone UE). Les requêtes envoyées sont confidentielles et ne sont jamais stockées ni exploitées par Google pour entraîner ses modèles.

- Resend Inc. / AWS : Routage technique des alertes par e-mail et des notifications transactionnelles de fermeture de workspace.

ARTICLE 7 : VOS DROITS EN TANT QUE PERSONNE CONCERNEE (ART. 15-22 RGPD)

En tant qu'utilisateur physique de la plateforme (analyste ou contact commercial), la législation européenne et allemande vous accorde les droits suivants auprès de notre délégué à la protection des données :

- Droit d'accès (Art. 15 RGPD) : Obtenir la copie complète des données nominatives que nous détenons sur vous.
- Droit de rectification (Art. 16 RGPD) : Corriger ou mettre à jour un profil incomplet ou erroné.
- Droit à l'effacement / Suppression (Art. 17 RGPD) : Demander la destruction de vos informations, sous réserve que nous n'ayons plus d'obligation fiscale ou légale de les conserver.
- Droit d'opposition et de retrait du consentement (Art. 21 et 7 RGPD) : Vous opposer à tout moment à la réception d'e-mails d'information commerciale ou révoquer une autorisation.

Vous pouvez exercer l'ensemble de ces droits en écrivant simplement à l'adresse officielle : support@delphisoft.de. De plus, vous disposez du droit d'introduire une réclamation auprès de l'autorité de contrôle compétente en Bavière : *Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)*.



Delphisoft Deutschland GmbH

Gugelstraße 32B
D-91077 Neunkirchen am Brand
Tel.: +49 9131 6258966
E-Mail: info@delphisoft.de
Website: www.delphisoft.de

Sitz: Neunkirchen a. B.
Amtsgericht: Bamberg HRB 10110
Geschäftsführer: Jonathan Breyse
USt-IdNr.: DE318864149

Sparkasse Erlangen
IBAN: DE06 7635 0000 0060 0912 93
SWIFT: BYLADEM1ERH
Konto-Nr.: 60091293

PRIVACY POLICY – AKUITY SOC**ARTICLE 1: DATA CONTROLLER AND DATA PROTECTION OFFICER**

The data controller for data processing on this website and within the Akuity SOC SaaS application within the meaning of the GDPR and the BDSG is:

- Company: Delphisoft Deutschland GmbH, Gugelstraße 32B, D-91077 Neunkirchen am Brand, Germany.
- Registration: Amtsgericht Bamberg HRB 10110 – USt-IdNr.: DE318864149.
- Statutory Representative (Geschäftsführer): Jonathan Breyse.
- GDPR / DPO Contact: support@delphisoft.de.

ARTICLE 2: GENERAL PROVISIONS, HOSTING AND LOGICAL SECURITY**2.1. Flow Encryption (SSL/TLS)**

For obvious security reasons and to safeguard the system against the interception of highly confidential data (notably during OAuth2 onboarding and API key configurations), the entirety of the website and application utilizes SSL or TLS encryption via HTTPS. All requests transiting between your browser and our infrastructure are encrypted end-to-end.

2.2. Hosting of the Web Infrastructure (Vercel)

The user interface (Frontend Next.js) and Edge routing and token verification middlewares are hosted with Vercel Inc. In order to guarantee flow sovereignty, Delphisoft has configured its deployments to run exclusively within Vercel's European data center located in Frankfurt, Germany (West) – eu-central-1 – fra1. No permanent storage of nominative application logs is performed by this third party.

2.3. Use of Cookies and Local Storage Technologies

To offer fluid navigation and secure access to the cockpit, the Akuity SOC platform exclusively uses technical cookies known as "essential". No third-party cookies for advertising or marketing targeting purposes are placed on the SaaS application without your express consent. In accordance with Article 6, paragraph 1, point f) of the GDPR and § 25, paragraph 2 of the German TDDG, these trackers are exempt from consent because they are strictly indispensable for providing the online communication service explicitly requested by the user.

List of indispensable technical trackers used by the application:

- **sb-access-token (Supabase Session Cookie):**

- *Nature and role:* Encrypted session cookie, configured with HTTP-Only and Secure security attributes. It stores the analyst's authentication JWT token.
- *Purpose:* Keep the analyst's session active, verify their logical access rights, and intercept connections without MFA in order to redirect them to the security challenge (AAL1 to AAL2).
- *Retention period:* Automatically deleted when closing the browser or upon expiration of the session token.

- **next-intl-locale (Internationalization):**

- *Nature and role:* Local technical cookie.
- *Purpose:* Remember the interface language selected by the analyst (French, German, or English) to ensure the correct display of menus, buttons, and reports generated during their session.
- *Retention period:* Persistent (limited to 1 year).

- **NEXT_JWT_MFA_CLAIM (Vercel Edge Middleware Context):**

- *Nature and role:* Technical data processed in Edge memory (Vercel Runtime).
- *Purpose:* Allow the middleware to instantly validate, in less than 50ms, if the active session has the required confidence level to execute a critical SOAR action (blocking, isolation), thereby avoiding heavy server requests.
- *Retention period:* Volatile session, cleared immediately upon disconnection.

ARTICLE 3: EXHAUSTIVE MAPPING OF DATA PROCESSING (DELPHISOFT AS CONTROLLER)

The publisher processes the data of natural users (visitors, prospects, client analysts) for the exclusive purposes detailed below:

A. Server Log Files Processing (Server-Logfiles)

- Processed data: Browser type and version, operating system, referrer URL, anonymous hashed IP address, date and time of the request. This data is automatically collected by the Vercel server when you simply browse the site and your browser transmits it to us.
- Purpose: Ensure technical stability, optimize display, and enable post-incident analysis in the event of a cyberattack (DDoS) against the platform.
- Legal basis: Legitimate interest (Art. 6, par. 1, al. f of the GDPR) to maintain a stable and secure website.
- Retention period: Automated deletion within 7 rolling days.

B. Contact Forms and Demonstration Requests (Sales-Led)

- Processed data: Last name, first name, professional email (generic domains like @gmail.com, @yahoo.fr, etc. are automatically filtered and rejected by our algorithms), company name, selected profile (Direct or MSSP), and content of the request.
- Purpose: Commercial contact, planning, and execution of demonstration sessions guided by our cyber-engineers.
- Legal basis: Pre-contractual measures taken at the request of the prospect (Art. 6, par. 1, al. b of the GDPR).
- Retention period: Data is retained for as long as necessary to evaluate the commercial opportunity, and deleted a maximum of 12 months after the last interaction without follow-up.

C. Registration, Authentication and Trial Period (14-day Trial)

- Processed data: System identifiers, analyst's email, password irreversibly hashed via Supabase Auth, MFA enrollment configuration and status (TOTP secrets), IP address during authentication, and internal audit logs (traceability of the analyst executing a SOAR action).
- Purpose: Provision the trial Workspace, enforce the mandatory two-factor trust level control (AAL2) to prevent session hijacking, and send the notification email on the 14th day offering to switch to the paid model.
- Legal basis: Performance of the free trial contract (Art. 6, par. 1, al. b of the GDPR).
- Retention period: If the customer refuses the paid subscription, the Workspace and all associated technical metadata are retained for a 30-day grace period, then undergo an automatic, complete, and irreversible purge.

D. Billing Management and Quota Monitoring

- Processed data: Physical billing address of the company, contact details of the accounting contact, intra-community VAT number (subject to instant validation via the European Commission's VIES API), exact volume of incidents counted by our pipelines, and number of active attached tenants.
- Purpose: Issue the monthly invoice in arrears at the beginning of each month, calculate plan overages (Overage billing), and apply the rules for immediate suspension of the Workspace at day 30 in the event of default of payment.
- Legal basis: Performance of the main SaaS contract (Art. 6, par. 1, al. b of the GDPR) and compliance with our statutory accounting and tax obligations under German law (Art. 6, par. 1, al. c of the GDPR).

**Delphisoft Deutschland GmbH**

Gugelstraße 32B
D-91077 Neunkirchen am Brand
Tel.: +49 9131 6258966
E-Mail: info@delphisoft.de
Website: www.delphisoft.de

Sitz: Neunkirchen a. B.
Amtsgericht: Bamberg HRB 10110
Geschäftsführer: Jonathan Breyse
USt-IdNr.: DE318864149

Sparkasse Erlangen
IBAN: DE06 7635 0000 0060 0912 93
SWIFT: BYLADEM1ERH
Konto-Nr.: 60091293

- Retention period: Mandatory legal archiving of 10 years for invoices and accounting documents, in accordance with the requirements of the German Tax Code (Abgabenordnung - AO).
- Imperative Demarcation: The processing of our customers' operational data (Role of Processor)

ARTICLE 4: DATA PROCESSED BY THE CHROME EXTENSION (AKUITY SOC COPILOT)

A. Authentication and session data (Local Storage)

The extension persistently stores in the browser's local storage (chrome.storage.local):

- Unique user identifier (Supabase User ID) and session token (JWT): Necessary to maintain the analyst's active session and secure requests to the API.
- Language preference: The language chosen by the analyst for the extension's interface display.

B. Browsing context data (Tab readings)

The extension analyzes the active browser tab in real time to extract only:

- The Microsoft Defender incident identifier in the URL of the active tab (when the host is security.microsoft.com and the path corresponds to /incidents/{id} or /incident2/{id}).
- The Microsoft Tenant ID present in the URL parameters (tid or tenantid) in order to associate the incident with the correct client.

Note: The extension ignores and does not collect any browsing history for sites and tabs outside the Microsoft Defender portal.

C. Incident data displayed in the interface (Side Panel)

When the extension is active on a Microsoft Defender incident, it retrieves from the API and displays in its side panel:

- Incident details: Title, AI-generated summary, incident severity level.
- Evidence elements (Evidence & Assets): Lists of targeted machines (Hostnames), affected users (UPNs/Professional emails), indicators of compromise (SHA-256 file hashes), and suspicious network connections detected.

D. AI interaction data and remediation suggestions (Chat)

When using the "AI Assistant" tab:

- Analyst requests: Selected predefined prompts (e.g., KQL query requests, PowerShell remediation commands, impact analysis, etc.) or custom questions entered by the analyst.
- Conversation history: Stored temporarily and volatily in the side panel's session memory

(sessionStorage). This history is cleared as soon as the browsing session is closed or upon clicking the "Clear history" button.

ARTICLE 5: DATA PROCESSING AGREEMENT EXCLUSION (AVV)

As part of its application functionality, the Akuity SOC application connects every 10 minutes via the Microsoft Graph API to our customers' production environments to extract security alerts. This automated flow ingests data relating to our customers' end users (UPN, email addresses of target employees, Azure AD identifiers, IP addresses of attacked terminals, raw descriptions of incidents). For all of this cyber-supervision data, Delphisoft Deutschland GmbH acts exclusively as a Processor (Auftragsverarbeiter) within the meaning of Article 28 of the GDPR. These processing operations are not governed by this unilateral policy, but are strictly framed by the Customer's instructions formalized within the Auftragsverarbeitungsvertrag (AVV / DPA) which must mandatory be accepted during account creation. Delphisoft refrains from using, consulting, or leveraging this data for its own account.

ARTICLE 6: DATA SHARING AND AUTHORIZED SUB-PROCESSORS

To operate the SaaS, Delphisoft relies on cutting-edge technological infrastructures whose processing is geographically restricted to the European Union zone:

- Supabase Inc.: Hosting of our production PostgreSQL database, isolated by RLS policies, located in the AWS Frankfurt region (Germany).
- Microsoft Ireland Operations Ltd.: Technical execution of our ingestion pipelines (Azure Logic Apps) located in the Azure Germany West Central region in Frankfurt (Germany).
- Google Cloud EMEA Ltd.: Google Gemini AI enrichment API via the sovereign European endpoint aiplatform.eu.rep.googleapis.com (EU Zone). Sent requests are confidential and are never stored or used by Google to train its models.
- Resend Inc. / AWS: Technical routing of email alerts and transactional notifications for workspace closure.

ARTICLE 7: YOUR RIGHTS AS A DATA SUBJECT (ART. 15-22 GDPR)

As a natural user of the platform (analyst or commercial contact), European and German legislation grants you the following rights with our data protection officer:

- Right of access (Art. 15 GDPR): Obtain a complete copy of the nominative data we hold about you.
- Right to rectification (Art. 16 GDPR): Correct or update an incomplete or erroneous profile.

- Right to erasure / Deletion (Art. 17 GDPR): Request the destruction of your information, provided that we no longer have a tax or legal obligation to retain it.

- Right to object and withdraw consent (Art. 21 and 7 GDPR): Object at any time to receiving commercial information emails or revoke an authorization.

You can exercise all of these rights by simply writing to the official address: support@delphisoft.de. In addition, you have the right to lodge a complaint with the competent supervisory authority in Bavaria: Bayerisches Landesamt für Datenschutzaufsicht (BayLDA).



Delphisoft Deutschland GmbH

Gugelstraße 32B
D-91077 Neunkirchen am Brand
Tel.: +49 9131 6258966
E-Mail: info@delphisoft.de
Website: www.delphisoft.de

Sitz: Neunkirchen a. B.
Amtsgericht: Bamberg HRB 10110
Geschäftsführer: Jonathan Breyse
USt-IdNr.: DE318864149

Sparkasse Erlangen
IBAN: DE06 7635 0000 0060 0912 93
SWIFT: BYLADEM1ERH
Konto-Nr.: 60091293