Technische und organisatorische Maßnahmen (TOM)

usecaise GmbH

Fleehook 1
48683 Ahaus

Fon +49 (0) 2561 8693 0

hello@usecaise.com
www.usecaise.com

usecaise

Änderungshistorie

Version 1.1.1 | Datum 25.06.2026 | Bearbeiter: usecaise GmbH | Bemerkung: Diverse Anpassungen
Version 1.1 | Datum 22.06.2026 | Bearbeiter: usecaise GmbH | Bemerkung: Ergänzung Managed n8n Service
Version 1.0 | Datum 21.04.2026 | Bearbeiter: usecaise GmbH | Bemerkung: Erstversion

1. Einleitung und Geltungsbereich

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOM) gemäß Art. 32 DSGVO, die die usecaise GmbH (Fleehook 1, 48683 Ahaus) zum Schutz personenbezogener Daten im Rahmen des Betriebs der usecaise Plattform sowie der damit verbundenen Managed Services (insbesondere des Managed n8n Service) umsetzt. Die usecaise Plattform ist eine cloudbasierte KI-Automatisierungsplattform, die als SaaS-Lösung in deutschen Rechenzentren betrieben wird.
Ziel der nachfolgend dargestellten Maßnahmen ist es, ein dem Risiko angemessenes Schutzniveau für die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sowie die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall sicherzustellen.
Die Maßnahmen werden überprüft und bei Bedarf an den Stand der Technik angepasst. Soweit die usecaise GmbH personenbezogene Daten im Auftrag ihrer Kunden verarbeitet, gelten diese TOM als Bestandteil der jeweiligen Auftragsverarbeitung gemäß Art. 28 DSGVO.

2. Datenschutzmanagement und organisatorische Maßnahmen

Die usecaise GmbH betreibt ein IT-Sicherheits- und Datenschutzmanagement, das auf die Anforderungen einer KI-Automatisierungsplattform mit sensiblen Kundendaten ausgerichtet ist und die Vorgaben der DSGVO sowie anerkannte IT-Sicherheitsprinzipien berücksichtigt. Im Einzelnen sind folgende organisatorische Maßnahmen umgesetzt:

- Alle Mitarbeiter sind auf das Datengeheimnis und zur Vertraulichkeit verpflichtet.
- Schulungen zu Datenschutz und IT-Sicherheit werden für jeden Mitarbeiter jährlich verpflichtend wiederholt.
- Die Vorlage eines unbedenklichen polizeilichen Führungszeugnisses ist im Onboarding-Prozess obligatorisch.
- Verbindliche Richtlinien und Verfahrensanweisungen regeln den Umgang mit Daten und IT-Systemen.
- Für die usecaise Plattform sind über den Dienst ILERT Monitoring-Benachrichtigungen eingerichtet, die im Störungsfall mehrere Personen aus dem Bereich DevOps sowie Entwicklung informieren.
- Ein Verarbeitungsverzeichnis gemäß Art. 30 DSGVO wird geführt; die TOM sind dokumentiert.
- Die Verantwortung für Qualifizierungs- und Sensibilisierungsmaßnahmen (IT-Sicherheit, Datenschutz, KI-Ethik) liegt bei der Geschäftsführung.

3. Sicherheit der Verarbeitung (Art. 32 DSGVO)

Durch die nachfolgenden technischen und organisatorischen Maßnahmen wird ein angemessener Schutz der verarbeiteten personenbezogenen Daten im Sinne des Art. 32 Abs. 1 DSGVO sichergestellt.

3.1 Wahrung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1.1 Zutrittskontrolle

Der unbefugte Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, wird verhindert. Der Betrieb erfolgt in nach ISO/IEC 27001 zertifizierten Rechenzentren in Deutschland. Umgesetzt sind insbesondere:

- Zutrittskontrollsysteme zu den Rechenzentren
- Videoüberwachung und Sicherheitspersonal
- physische Zutrittssicherungen zum Schutz der Serverhardware
- Sicherung vor Elementarschäden (u. a. Brandschutz, redundante Stromversorgung) im Rechenzentrum

3.1.2 Zugangskontrolle

Es ist sichergestellt, dass die IT-Systeme nicht von Unbefugten genutzt werden können. Folgende Maßnahmen sind getroffen:

- Benutzerkonten werden über einen gesicherten Registrierungsprozess unter https://my.usecaise.eu angelegt.
- Die Kommunikation zwischen Client und Server erfolgt über verschlüsselte Verbindungen (HTTPS/TLS).
- Administrative Zugänge im Backend sind durch Mehrfaktor-Authentifizierung (MFA) gesichert.
- Administrative Zugänge werden überprüft.
- Der Zugang ist mindestens durch Benutzername und Kennwort geschützt.
- Die von Mitarbeitern genutzten Notebooks sind festplattenverschlüsselt; Arbeitsplätze werden durch Bildschirmsperren bei Inaktivität gesichert.
- Bereitgestellte Umgebungen werden mit einer Basis-Härtung (sichere Standardkonfiguration, reduzierte Angriffsfläche) initial konfiguriert; der Zugriff auf das n8n-Frontend des Managed n8n Service ist durch Authentifizierung geschützt.

3.1.3 Zugriffskontrolle

Durch ein bedarfsorientiertes Berechtigungskonzept wird sichergestellt, dass Benutzer ausschließlich auf die für ihre Aufgabe erforderlichen Daten zugreifen können:

- Im Standard hat jeder Nutzer ausschließlich Zugriff auf den eigenen Workspace sowie die eigenen Usecaises und AIgents.
- Der Zugriff auf weitere Ressourcen ist nur nach expliziter Freigabe über die Sharing-Funktion möglich; beim Teilen eines Workspace mit einem Team wird je Mitglied eine Rolle (Mitwirkender oder Nutzer) festgelegt.
- Erweiterte Systemberechtigungen bestehen ausschließlich für Mitarbeiter der usecaise GmbH, die diese zur Aufgabenerfüllung benötigen.

3.1.4 Trennungskontrolle

Zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet:

- Im Rahmen des Managed n8n Service werden dedizierte, logisch getrennte n8n-Instanzen je Kunde mit eigenem Zugangskonzept bereitgestellt.
- Das Testsystem (dedizierte Staging-Umgebung) ist von der Produktivumgebung getrennt und enthält ausschließlich Testdaten, keine produktiven Nutzdaten.

3.1.5 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- In der Plattform hinterlegte Credentials zur Anbindung von Drittsystemen werden verschlüsselt gespeichert.
- Chat-Verläufe können AES-256 verschlüsselt geführt werden
- Sämtliche Datenübertragungen erfolgen transportverschlüsselt über HTTPS/TLS.

3.2 Wahrung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.2.1 Weitergabekontrolle

Bei der Übertragung personenbezogener Daten wird sichergestellt, dass diese nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Jede elektronische Datenübertragung erfolgt über verschlüsselte Verbindungen (HTTPS/TLS); dies gilt auch für API-Zugriffe und administrative Zugriffe.
- Für die Anbindung kundeninterner Systeme können kundenspezifische Firewall-Regeln nach dem Least-Privilege-Prinzip eingerichtet und dokumentiert werden.

• Mit Auftragsverarbeitern bestehen soweit möglich Auftragsverarbeitungsverträge (AVV) gemäß Art. 28 DSGVO.

3.2.2 Eingabekontrolle

Es ist nachvollziehbar, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden:

• Sicherheitsrelevante Ereignisse und Nutzeraktivitäten werden in einem Audit-Log protokolliert.
• Protokolliert werden u. a. Anmeldungen, Konfigurationsvorgänge, Datenquellenzugriffe und API-Aufrufe.
• Protokolldaten werden über einen Zeitraum von rund 90 Tagen aufbewahrt.
• Administrative Tätigkeiten und Störungen werden zusätzlich im internen Ticketsystem dokumentiert.

3.3 Wahrung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.3.1 Verfügbarkeitskontrolle

Personenbezogene und weitere schützenswerte Daten werden gegen zufällige Zerstörung oder Verlust geschützt:

• Die Infrastruktur ist auf einen betriebsstabilen Betrieb ausgelegt.
• Angestrebt wird eine Verfügbarkeit von 99,0 % im Monatsmittel (Zielwert, keine zugesicherte Verfügbarkeit).
• Ein Monitoring überwacht zentrale Systemkomponenten der usecaise Plattform; bei Störungen oder Überschreitung definierter Schwellwerte werden über den Dienst ILERT Benachrichtigungen an die zuständigen Personen ausgelöst.
• Für die Managed-Umgebungen erfolgen ein planbares Update- und Patch-Management (einschließlich sicherheitsrelevanter Patches) sowie automatisierte Backups.
• Automatisierte tägliche Sicherungen relevanter Datenbanken und Konfigurationen werden in einem separaten Rechenzentrumsabschnitt aufbewahrt; Backups werden mindestens 30 Tage vorgehalten.
• Schutz vor Schadsoftware sowie CDN- und DDoS-Schutz sind implementiert.
• Nicht mehr benötigte Datenträger werden über zertifizierte Dienstleister gemäß DIN EN 15713 entsorgt.

3.3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Die Wiederherstellung der Verfügbarkeit nach einem Zwischenfall ist vorgesehen:

- Die Integrität des Gesamtsystems kann über vorgehaltene Backups und Snapshots wiederhergestellt werden.
- Die Wiederherstellbarkeit wird durch manuelle Tests überprüft.

3.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

3.4.1 Überprüfung und Wirksamkeitskontrolle

Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird überprüft und bewertet:

- Der Betrieb erfolgt in nach ISO/IEC 27001 zertifizierten Rechenzentren; das Sicherheitskonzept orientiert sich an anerkannten IT-Sicherheitsprinzipien.
- Datenbank-Transaktionen werden durch ACID-konforme Datenbanksysteme abgesichert; bei kritischen Schreiboperationen finden Integritätsprüfungen statt.
- Im Entwicklungsprozess werden automatisierte Tests eingesetzt (u. a. CI/CD-Pipelines, Unit- und Integrationstests).
- Neuerungen werden erst nach Tests in der getrennten Testumgebung in die Produktivumgebung übernommen.

3.4.2 Vorfallreaktion (Incident Response)

Für die Erkennung und Behandlung von Sicherheitsvorfällen und Störungen bestehen folgende Maßnahmen:

- Über das Monitoring werden bei Fehlern oder Schwellwertüberschreitungen Benachrichtigungen ausgelöst, sodass Störungen erkannt und behoben werden können.
- Maßnahmen zur Störungsbehebung werden intern eingeleitet; bei Bedarf wird externer Support hinzugezogen.
- Kunden können Störungen über hello@usecaise.com oder +49 (0) 2561 8693 0 melden.
- Störungen werden im Ticketsystem dokumentiert.
- Datenschutzverletzungen werden den betroffenen Auftraggebern unverzüglich gemeldet.

3.4.3 Auftragskontrolle (Auftragsverarbeitung gemäß Art. 28 DSGVO)

Die Verarbeitung personenbezogener Daten im Auftrag erfolgt ausschließlich nach Weisung des Auftraggebers:

- Für Auftragsverarbeiter liegen Auftragsverarbeitungsverträge (AVV) gemäß Art. 28 DSGVO vor.
- Hosting und Rechenzentrumsbetrieb der usecaise Plattform erfolgen durch die OVH SAS in einem Rechenzentrum in Deutschland; ergänzend werden weitere Dienste eingebunden (u. a. CDN-/DDoS-Schutz, transaktionaler E-Mail-Versand).
- Der Rechenzentrumsbetrieb des Managed n8n Service erfolgt durch die ambiFOX GmbH in einem Rechenzentrum in Deutschland.
- Im usecaise Produkt sind verschiedene LLM-Anbieter integriert. Ein Teil dieser Anbieter verarbeitet Daten außerhalb der EU (z. B. ChatGPT/OpenAI, Gemini/Google, Claude/Anthropic); daneben stehen EU-Anbieter zur Verfügung (z. B. Mistral). DSGVO-konforme Modelle sind gesondert gekennzeichnet, sodass auf Wunsch ein EU-konformer Betrieb möglich ist. Die Nutzung der jeweiligen Modelle unterliegt zusätzlich den Bedingungen der jeweiligen Anbieter.

3.5 Speicherbegrenzung und Löschung

Personenbezogene Daten werden nicht länger als für den jeweiligen Zweck erforderlich gespeichert:

- Nach Beendigung des Vertrags werden die personenbezogenen Kundendaten gelöscht.
- Chat-Sessions werden nach 30 Tagen gelöscht, sofern sie nicht innerhalb dieser Frist erneut aufgerufen (reaktiviert) werden.
- Im System verbleibende Chat-Sessions liegen anonymisiert vor, sodass kein Bezug zu einer Person mehr herstellbar ist.

4. Ansprechpartner und Fragen zum Datenschutz

Bei Fragen zu Datenschutz und Datensicherheit im Zusammenhang mit der usecaise Plattform wenden Sie sich bitte an:
usecaise GmbH
Fleehook 1, 48683 Ahaus
E-Mail: hello@usecaise.com
Telefon: +49 (0) 2561 8693 0

Weiterführende datenschutzrechtliche Informationen sind unter
https://usecaise.com/index.php/privacy/ veröffentlicht.