Anlage 2 (TOM)

Technische und organisatorische Maßnahmen der intrinsify GmbH

Stand: 23.02.2026

Verantwortliche Personen
Katharina Staudinger, Geschäftsführerin
Christopher H. Stappert, Leiter IT

Sensitivitätsstufe
Öffentlich

Prüfungsintervall
Jährlich

Präambel zur Sicherheitsarchitektur: intrinsify agiert als „Remote-First"-Unternehmen ohne eigene physische Serverräume. Die Verarbeitung erfolgt auf Systemen zertifizierter Cloud-Provider (siehe Anlage 2). Die nachfolgenden Maßnahmen beschreiben die Absicherung der Cloud-Infrastruktur, der Endgeräte der Mitarbeiter und der Software-Architektur.

Geltungsbereich: Dieses Dokument soll Dritten, wie Lieferanten und Dienstleistern, als umfassende Selbstauskunft dienen, um ihre Anfragen zur Informationssicherheit zu beantworten. Die hier aufgeführten Kriterien geben einen Einblick in Sicherheitspraktiken und demonstrieren das Engagement für den Schutz sensibler Daten.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle (Physischer Zugang)

- **Rechenzentren:** Die physische Sicherheit der Server obliegt den Cloud-Providern (z. B. AWS, Google Cloud, Azure). Diese verfügen über Hochsicherheitskonzepte (24/7 Sicherheitsdienst, biometrische Zugangskontrollen, Videoüberwachung) und sind nach ISO 27001 sowie SOC2 und SOC3 zertifiziert.
- **Arbeitsplätze (Homeoffice):** Die Mitarbeiter sind vertraglich verpflichtet, in privaten Räumlichkeiten sicherzustellen, dass Dritte (z. B. Familienangehörige, Besucher) keinen Blick auf Bildschirme oder Zugriff auf Hardware haben.
- **Büroräume:** Soweit Co-Working-Spaces genutzt werden, erfolgt keine Verarbeitung sensibler Daten auf öffentlich einsehbaren Bildschirmen.

Zugangskontrolle (Systemzugang)

- **Authentifizierung:** Der Zugriff auf interne Systeme erfordert strikte Authentifizierungsverfahren. Wo technisch möglich, ist eine Zwei-Faktor-Authentifizierung (2FA) verpflichtend aktiviert. Für alle administrativen Zugriffe (Cloud-Accounts, Repositories,

Datenbank-Administration, Support-Tools, Monitoring) sowie für produktive Konten mit erweiterten Rechten ist MFA aktiviert.

-
- **Passwort-Management:** Einsatz eines Enterprise-Passwort-Managers. Durchsetzung komplexer Passwort-Richtlinien.
- **Gerätesicherheit:** Sämtliche dienstlichen Endgeräte (Laptops/Mobilgeräte) sind mittels Festplattenverschlüsselung (z. B. FileVault, BitLocker) gesichert. Eine automatische Bildschirmsperre bei Inaktivität ist konfiguriert.
- **Datenschutzkonforme Entsorgung:** Prozesse zur sicheren Löschung/Vernichtung von Daten auf ausgemusterten Endgeräten (PCs) sind definiert, um eine datenschutzkonforme Entsorgung zu gewährleisten.
- **Malwareschutz (Prävention & Resilienz):** Eine mehrstufige Strategie schützt Endgeräte (native macOS-Sicherheitsarchitektur, z. B. Gatekeeper/XProtect) und die zentrale Cloud-Infrastruktur (Echtzeit-Virenprüfung). Die lückenlose Datenversionierung in der Cloud dient der Resilienz gegen Ransomware.

Zugriffskontrolle (Berechtigungen)

- **Berechtigungskonzept (RBAC/Least Privilege):**Zugriffsrechte werden rollenbasiert (RBAC) über eine dokumentierte Rollen- und Berechtigungsmatrix vergeben. Dabei gilt das „Need-to-Know“-Prinzip (Minimalrechte / Least Privilege), sodass Mitarbeiter nur Zugriff auf Daten haben, die sie für ihre Aufgabenerfüllung benötigen.
- **Administrative Rechte:** Die Anzahl der Administratoren ist auf das notwendige Minimum beschränkt.
- **Nutzer-Lifecycle-Management:** Die Vergabe und der Entzug von Zugriffsrechten erfolgen über einen dokumentierten Joiner/Mover/Leaver-Prozess, um die zeitnahe Deprovisionierung bei Austritt oder die Anpassung der Rechte bei Rollenwechsel zu gewährleisten.
- **Rezertifizierung:** Privilegierte Zugriffe werden quartalsweise einer Rezertifizierung (Access Reviews) unterzogen, um die Einhaltung der Minimalrechte und die Notwendigkeit der Berechtigungen regelmäßig zu überprüfen.
  Verschlüsselung: Daten werden in den Datenbanken der Cloud-Provider verschlüsselt gespeichert (Encryption at Rest).

Trennungskontrolle

- **Logische Mandantentrennung:** Die Daten verschiedener Kunden werden softwareseitig (logisch) strikt getrennt verarbeitet. Eine Vermischung von Datenbeständen ist durch die Softwarearchitektur ausgeschlossen.
- **Systemtrennung:** Die Produktentwicklung basiert auf einer strikten Drei-System-Landschaft (Lokale Entwicklung, Test, Production). Echte Kundendaten werden ausschließlich in der Produktionsumgebung gespeichert und verarbeitet. Lokale Entwicklungs- und Test-Umgebungen nutzen getrennte Datenbanken ohne Kundendaten.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

- **Datenexporte und Weitergabe:** Die Übermittlung und der Export von Daten werden auf definierte, dokumentierte Prozesse beschränkt. Standardmäßig werden nur aggregierte Reports herausgegeben.

- **Umgang mit Rohdaten:** Die Herausgabe von Rohdaten (z.B. vollständige Transkripte) erfolgt nicht.
- **Protokollierung und Verschlüsselung:** Alle Datenübergaben an Dritte erfolgen verschlüsselt und werden zur Nachvollziehbarkeit protokolliert (Export-Auditlog).
- **Übertragung:** Jegliche Datenübertragung über öffentliche Netze erfolgt verschlüsselt nach aktuellem Stand der Technik (HTTPS/TLS 1.2 oder höher).
- **VPN:** Der administrative Zugriff auf die Cloud-Infrastruktur erfolgt über gesicherte Verbindungen (VPN) oder vergleichbare Zero-Trust-Konzepte.
- **IP-Logging:** Sofern möglich, findet eine Reduktion des IP-Loggings statt (z.B. durch Kürzung, Anonymisierung oder Verhinderung)
- **Anonymisierung und Pseudonymisierung:** Es wird eine Pseudonymisierung verwendet, indem Nutzer über generische Links (nur Diagnose-Modul) Zugriff auf eine Serversession erhalten. Eine direkte Rückverfolgung zur natürlichen Person ist nicht möglich. Ein Korrelationspotential zur Re-Identifizierung besteht lediglich durch die Verknüpfung dieser Session-Daten mit internen Logging-Daten. Dies ist für die Leistungserbringung nicht relevant.
- **Re-Identifikationsschutz in Reports:** Es werden Aggregationsregeln angewendet, um kleine Auswertungszellen („small cells“) zu verhindern. Dazu gehört die Festlegung einer Mindestgruppengröße, sowie Kombinationssperren bei dimensionsübergreifenden Filtern. Die Nennung von Beispielen oder Zitaten erfolgt ausschließlich oberhalb dieses definierten Schwellenwertes.

Eingabekontrolle

- **Vertraulichkeit:** Alle Mitarbeitenden sind auf Vertraulichkeit verpflichtet.
- **PII-Redaction und Minimierung:** Teilnehmende im Chat werden zur Vermeidung identifizierbarer Angaben (keine Namen/Identifikatoren) angeleitet. Eine automatische Erkennung und Maskierung typischer Identifikatoren (z.B. E-Mail/Telefon/IDs) soll vor der Weiterverarbeitung und/oder Persistenz erfolgen.
- **LLM Data Handling:** Für die externe LLM-Verarbeitung werden nur erforderliche Daten übermittelt (Payload-Minimierung). Vertraglich werden Zusagen zur Nichtnutzung für Modelltraining („no training“) sowie definierte Retention und Logging beim Anbieter festgelegt. Provider- und Modellwechsel werden dokumentiert und vorab bewertet.
- **Protokollierung & Monitoring:** Es existiert ein dokumentiertes Logging- und Monitoring-Konzept, das Logkategorien, die Zweckbindung, die Speicherdauer (Retention), Zugriffsregelungen und den Manipulationsschutz festlegt. Systemseitig erfolgt eine detaillierte Protokollierung (Logging) von Eingabe-, Änderungs- und Löschvorgängen, um die Nachvollziehbarkeit aller Aktionen zu gewährleisten
- **Log-Trennung und Zugriff:** Security-Logs und Applikationslogs werden getrennt gespeichert. Der Zugriff auf Logs ist rollenbasiert geregelt, um deren Manipulationsschutz zu gewährleisten.
- **Alerting:** Alerting-Regeln sind für sicherheitsrelevante Events implementiert, um eine proaktive Reaktion des Security-Teams zu ermöglichen.
- **Nachvollziehbarkeit:** Jeder Zugriff ist über individuelle Benutzerkonten einer natürlichen Person zuordenbar.
- **Dokumentenmanagement:** Das Unternehmen arbeitet nach dem Prinzip des papierlosen Büros. Die Authentizität und Unveränderbarkeit von Schriftgut wird, wo erforderlich, durch den Einsatz von e-Signature-Verfahren gewährleistet.
- **Weisungskontrolle**: Die Verarbeitung personenbezogener Daten erfolgt ausschließlich weisungsgebunden und entsprechend den dokumentierten Anweisungen des Auftraggebers.

- **Löschung & Aufbewahrung:** Es existieren dokumentierte Aufbewahrungs- und Löschfristen (Retention-Matrix) je Datenkategorie (Inhaltsdaten, Metadaten, Logs, Exporte). Es erfolgt eine projektbezogene Löschung von Rohdaten 90 Tage nach Projektabschluss oder Aggregation (sofern vertraglich vereinbart), zusätzlich zu geltenden Löschregeln. Jegliche Geschäftsvorgänge werden entsprechend der gesetzlichen Aufbewahrungsfristen vorgehalten.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Verfügbarkeitskontrolle

- **Patch- und Vulnerability Management:** Kontinuierliches, automatisiertes Monitoring von Software-Abhängigkeiten auf Sicherheitslücken. Kritische Patches werden in einem wöchentlichen Software Integrity Review (SIR) priorisiert und nach erfolgreicher Test-Pipeline kontrolliert in die Produktion überführt.
- **Backups:** Es werden automatisierte, regelmäßige Backups der Datenbanken durch die Cloud-Provider erstellt. Die Backups werden georedundant oder in separaten Verfügbarkeitszonen gespeichert.
- **Redundanz:** Die Infrastruktur ist redundant ausgelegt (z. B. Serverless-Architektur, Load Balancer), um Ausfälle einzelner Komponenten kompensieren zu können.
- **Notfall- und Wiederanlaufkonzept:** intrinsify unterhält ein Notfall- und Wiederanlaufkonzept (Business Continuity). Die Prozesse zur Wiederherstellung von Daten (Disaster Recovery) sind definiert und ihre Funktionsfähigkeit wird durch regelmäßige Tests der Backups überprüft.

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

Datenschutz-Management

- **Sicherheitsanalysen & Audits: i**ntrinsify führt regelmäßige Sicherheitsanalysen durch. Die Sicherheitseinstellungen und Berechtigungen werden zudem regelmäßig auditiert.
- **Incident Management:** Es existiert ein Prozess zur Meldung und Bearbeitung von Sicherheitsvorfällen und Datenschutzverletzungen.
- **Mitarbeiterschulung:** Mitarbeiter werden regelmäßig zum Thema Datenschutz und IT-Sicherheit sensibilisiert und auf das Datengeheimnis verpflichtet.
- **Auftragskontrolle:** Subunternehmer werden sorgfältig ausgewählt und vertraglich zur Einhaltung gleicher Sicherheitsstandards verpflichtet (Abschluss von AVV). Die Einhaltung wird durch Prüfung von Zertifikaten (SOC 2, ISO 27001) überwacht.