Logicc

Technische und organisatorische Maßnahmen (TOMs)

Stand: 1. Oktober 2026 · erzeugt am 09. November 2026

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Wahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen hat Logicc angemessene technische und organisatorische Sicherheitsmaßnahmen ergriffen und wird diese beibehalten, um die Kundendaten vor Sicherheitsvorfällen zu schützen und die Sicherheit und Vertraulichkeit der Kundendaten zu wahren ("technische und organisatorische Maßnahmen"). Diese Maßnahmen beinhalten folgende Aspekte:

1. Vertraulichkeit

1.1 Zutrittskontrolle

Logicc betreibt keine eigenen Rechenzentren oder Serverräume. Die Anwendung wird auf Cloud-Infrastruktur in ISO/IEC 27001-zertifizierten Rechenzentren betrieben. Die physische Zutrittskontrolle der Rechenzentren wird durch die Hosting-Anbieter gemäß deren vertraglich vereinbarten technischen und organisatorischen Maßnahmen gewährleistet. Für die Geschäftsräume von Logicc gelten folgende Maßnahmen:

- Digitales Zutrittskontrollsystem mit individuellen Zutrittsberechtigungen für Mitarbeiter.
- Authentisierung mittels persönlichem Zugangscode oder biometrischem Faktor.
- Protokollierung von Zutrittsereignissen.
- Vergabe und Entzug von Zutrittsberechtigungen entsprechend der betrieblichen Erforderlichkeit.
- Besucher und externe Dienstleister werden nur durch berechtigte Mitarbeiter eingelassen und dürfen sich in nicht öffentlich zugänglichen Bereichen nicht unbeaufsichtigt aufhalten.

1.2 Zugangskontrolle

Logicc wird angemessene Maßnahmen treffen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Technische Maßnahmen:
- Verwendung individueller Benutzerkonten und starker, eindeutiger Authentisierungsmerkmale.
- Einsatz von Multi-Faktor-Authentifizierung oder Passkeys, soweit dies technisch unterstützt wird und insbesondere für privilegierte oder sicherheitsrelevante Zugänge.
- Verwendung eines zentral freigegebenen Passwortmanagements zur Erzeugung und sicheren Speicherung eindeutiger Zugangsdaten.
- Änderung von Zugangsdaten bei bekannt gewordener oder vermuteter Kompromittierung sowie bei sonstigem sicherheitsbezogenem Anlass.
- Automatische Sperrung inaktiver Sitzungen nach einem definierten Zeitraum.
- Zentrale Verwaltung der von Logicc bereitgestellten Endgeräte zur Durchsetzung und Überwachung

von Sicherheitskonfigurationen, Betriebssystemaktualisierungen und Gerätekonformität.
- Vollständige Festplattenverschlüsselung der von Logicc bereitgestellten Endgeräte.
- Verwaltung von Benutzerberechtigungen.
- Organisatorische Maßnahmen:
- IT-Sicherheitsrichtlinie, die den sicheren Umgang mit Passwörtern, Zugangsdaten und mobilen Geräten regelt.
- Nutzung von Logicc bereitgestellter und zentral verwalteter Endgeräte durch Mitarbeiter für die Verarbeitung von Kundendaten.
- Vergabe von Benutzerkonten nach dem Prinzip der minimalen Rechtevergabe.
- Regelmäßige Sicherheitsschulungen für Mitarbeiter, um das Bewusstsein für Phishing und andere Bedrohungen zu schärfen.

1.3 Zugriffskontrolle

Logicc wird angemessene Maßnahmen treffen, um sicherzustellen, dass die zur Benutzung der Datenverarbeitungssysteme Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, und dass Kundendaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Hierzu trifft Logicc folgende Vorkehrungen:

- Technische Maßnahmen:
- Implementierung eines differenzierten Berechtigungskonzepts, das den Zugriff auf Kundendaten auf das notwendige Minimum beschränkt.
- Einsatz von Netzwerk- und Anwendungsfiltern, einschließlich einer Web Application Firewall für öffentlich erreichbare Anwendungsendpunkte.
- Umfassende Protokollierung aller Zugriffe auf Kundendaten in manipulationssicheren Audit-Logs nach festgelegten Aufbewahrungsfristen.
- Gesonderte Protokollierung sicherheitsrelevanter Datenbankzugriffe.
- Administrativer Zugriff auf die Hosting-Infrastruktur ausschließlich über verschlüsselte und zugangsgeschützte Verbindungen.
- Zentrale, verschlüsselte Verwaltung von Produktionsgeheimnissen und kryptografischen Schlüsseln; Zugriffe und Bereitstellung werden auf die jeweils erforderlichen Personen und Dienste beschränkt.
- Verschlüsselung von Kundendaten im Ruhezustand unter Verwendung starker, dem Stand der Technik entsprechender Verschlüsselungsverfahren.
- Organisatorische Maßnahmen:
- Richtlinie zur Vergabe und Entziehung von Zugriffsrechten, die sich am "Need-to-know"-Prinzip orientiert.
- Regelmäßige und anlassbezogene Überprüfung von Zugriffsberechtigungen, insbesondere für privilegierte Zugänge.
- Besondere Autorisierung für den Zugriff auf besonders sensible Datenkategorien.
- Beschränkung privilegierter Zugriffe auf einen kleinen, betrieblich erforderlichen Personenkreis nach dem Prinzip der minimalen Rechtevergabe.
- Mitarbeiter, die bei ihrer Tätigkeit Kenntnis von Kundendaten erlangen können, werden vor dem Zugriff in Textform zur Vertraulichkeit und zur Wahrung fremder Geheimnisse gemäß § 203 StGB verpflichtet.

1.4 Trennungskontrolle

Logicc wird angemessene Maßnahmen treffen, um sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Kundendaten getrennt verarbeitet werden können. Hierzu trifft Logicc folgende Vorkehrungen:

- Technische Maßnahmen:
- Strikte logische Mandantentrennung innerhalb der zentralen Datenbank durch den Einsatz von Row-Level Security (RLS).
- Sicherstellung der Mandantentrennung auf Anwendungsebene, um den Zugriff auf Daten anderer Mandanten zu unterbinden.
- Getrennte Umgebungen für Entwicklung, Tests und Produktion.
- Ein differenziertes Berechtigungskonzept, das den Zugriff regelt.
- Organisatorische Maßnahmen:
- Richtlinie zur Datenklassifizierung und zur getrennten Verarbeitung von Daten verschiedener Mandanten und Zwecke.
- Regelmäßige Kontrolle der technischen und organisatorischen Maßnahmen zur Datentrennung.

2. Integrität

2.1 Weitergabekontrolle

Logicc wird angemessene Maßnahmen treffen, um das Risiko zu reduzieren, dass Kundendaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Hierzu trifft Logicc folgende Vorkehrungen:

- Technische Maßnahmen:
- Konsequente Verschlüsselung sämtlicher Übertragungen von Kundendaten über externe oder öffentliche Netze unter Verwendung von mindestens TLS 1.3.
- Nutzung freigegebener, zugangsgeschützter Übertragungswege und Cloud-Dienste für den Austausch und die Bereitstellung von Kundendaten.
- Organisatorische Maßnahmen:
- Richtlinie zur sicheren Übertragung und Weitergabe von Kundendaten, die die Nutzung unsicherer Kanäle untersagt.
- Sensibilisierung der Mitarbeiter für die Risiken unsicherer Datenübertragung.
- Klare Regelungen zur Nutzung von Cloud-Diensten und zur Übermittlung von Daten an Dritte.
- Dokumentierte Übersicht über regelmäßige Abruf- und Übermittlungsverfahren.

2.2 Eingabekontrolle

Logicc wird angemessene Maßnahmen treffen, um sicherzustellen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem Kundendaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Hierzu trifft Logicc folgende Vorkehrungen:

- Technische Maßnahmen:
- Umfassende Protokollierung aller Eingaben, Änderungen und Löschungen von Kundendaten in manipulationssicheren Audit-Logs nach festgelegten Aufbewahrungsfristen.
- Gesonderte Protokollierung sicherheitsrelevanter Datenbankzugriffe.
- Plausibilitäts- und Validierungsprüfungen bei der Dateneingabe.

- Nachvollziehbarkeit von Änderungen durch Zeitstempel oder Versionierung, soweit dies für den jeweiligen Verarbeitungsvorgang technisch vorgesehen ist.
- Organisatorische Maßnahmen:
- Klare Zuständigkeiten für die Dateneingabe und -pflege.
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf der Grundlage eines Berechtigungskonzepts.
- Regelmäßige und anlassbezogene Überprüfung sicherheitsrelevanter Protokolle.

3. Verfügbarkeit und Belastbarkeit

Logicc wird angemessene Maßnahmen treffen, um sicherzustellen, dass Kundendaten gegen zufällige Zerstörung oder Verlust geschützt sind. Hierzu trifft Logicc folgende Vorkehrungen:

- Technische Maßnahmen:
- Hosting der Anwendung und Kundendaten in ISO/IEC 27001-zertifizierten Rechenzentren.
- Tägliche Sicherung produktiver Kundendaten sowie der für den sicheren Betrieb erforderlichen Systeme und Konfigurationen.
- Speicherung der Sicherungen innerhalb der Europäischen Union und Verschlüsselung mit AES-256.
- Reguläre Aufbewahrung der Sicherungen für 14 Tage; gelöschte Sicherungen bleiben durch eine Soft-Delete-Funktion für 90 Tage wiederherstellbar.
- Gelöschte Sicherungen werden während der Soft-Delete-Frist ausschließlich für Zwecke der Notfallwiederherstellung vorgehalten, nicht produktiv genutzt und nach Ablauf der Frist automatisch endgültig gelöscht.
- Überwachung der Sicherungsprozesse sowie regelmäßige Kontrolle und Dokumentation der Sicherungsergebnisse.
- Regelmäßige und anlassbezogene Tests der Wiederherstellbarkeit von Sicherungen, mindestens einmal pro Quartal.
- Technische Maßnahmen zur Erkennung und Abwehr von Schadsoftware und sonstigen Sicherheitsbedrohungen.
- Physische Schutz- und Redundanzmaßnahmen der Rechenzentrumsbetreiber, insbesondere für Stromversorgung, Klimatisierung, Brandschutz und Speichersysteme.
- Organisatorische Maßnahmen:
- Dokumentiertes Sicherungs- und Wiederherstellungskonzept, das sich an der Kritikalität der Daten und Systeme orientiert und Verantwortlichkeiten, Eskalationswege sowie automatisierungsunterstützte Wiederherstellungsschritte festlegt.
- Notfallpläne für relevante Ausfallszenarien, die regelmäßig überprüft, aktualisiert und erprobt werden.
- Benannte interne Verantwortliche für Notfälle, technische Sicherheitsvorfälle und erforderliche Wiederherstellungsmaßnahmen.
- Nutzung der vertraglich vereinbarten Standardverfügbarkeiten und Supportleistungen der Hosting-Anbieter.
- Informationssicherheitsrichtlinie mit Vorgaben zur Verfügbarkeit, Wiederherstellung und zum Notfallbetrieb.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Logicc implementiert Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

4.1 Datenschutz-Management

- Es wurde ein externer Datenschutzbeauftragter bestellt. Dieser wird durch den Geschäftsführer und einen dedizierten Mitarbeiter, die als interne Datenschutzkoordinatoren fungieren, bei der Umsetzung der Datenschutzmaßnahmen im Unternehmen unterstützt.
- Implementierung eines Datenschutz-Managementsystems (DSMS) in Anlehnung an bewährte Standards (z.B. ISO 27701, BSI IT-Grundschutz), angepasst an die Größe und Komplexität des Unternehmens.
- Regelmäßige interne Überprüfungen der Datenschutzmaßnahmen und -prozesse, mindestens einmal jährlich.
- Dokumentation und Bearbeitung von Datenschutzvorfällen gemäß einem definierten internen Prozess.
- Regelmäßige Schulungen der Mitarbeiter zum Datenschutz, mindestens einmal jährlich.
- Prozesse bezüglich Informationspflichten gemäß Artikel 13 und 14 DSGVO umgesetzt.
- Formalisiertes Verfahren für Auskunftsersuchen von betroffenen Personen eingerichtet.
- Datenschutz-Checkpoints, soweit möglich und sinnvoll, in die Risikobewertung integriert.
- Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf für neue Verarbeitungstätigkeiten mit voraussichtlich hohem Risiko durchgeführt.
- Datenschutzaspekte sind Teil des allgemeinen Risikomanagements des Unternehmens.

4.2 Incident-Response-Management

- Einsatz eines auf technische Fehler- und Performanceinformationen beschränkten Monitorings mit Maßnahmen zur Vermeidung der Erfassung von Prompts, Modellantworten, Dokumentinhalten, Authentifizierungstoken und vollständigen Request-Bodies.
- Dokumentierter Incident-Response-Prozess für die Erkennung, Meldung, Analyse, Reaktion und Nachbereitung von Sicherheitsvorfällen und Datenschutzverletzungen, einschließlich der Prüfung gesetzlicher Meldepflichten.
- Benannte interne Incident-Response-Gruppe und Einbindung der technischen Leitung in die Koordination und Bearbeitung von Sicherheitsvorfällen und Datenschutzverletzungen.
- Zentrale Dokumentation und Nachverfolgung von Sicherheitsvorfällen und Datenschutzverletzungen.
- Einsatz einer Web Application Firewall zum Schutz öffentlich erreichbarer Anwendungsendpunkte.
- Nutzung zentraler Spam-, Phishing- und Malware-Schutzmechanismen für die geschäftliche E-Mail-Kommunikation.
- Regelmäßige Schulung der Mitarbeiter im Umgang mit Sicherheitsvorfällen und Phishing-Versuchen.
- Regelmäßige Überprüfung und Weiterentwicklung des Incident-Response-Verfahrens.

4.3 Sichere Softwareentwicklung und Schwachstellenmanagement

- Geschützte Entwicklungszweige sowie geregelte Merge-, Freigabe- und Release-Prozesse für Änderungen am Anwendungscode.
- Prüfung von Änderungen in einer vom Produktivbetrieb getrennten Testumgebung vor der Produktivsetzung.

- In den Entwicklungsprozess integrierte sowie regelmäßig ausgeführte Sicherheits-, Abhängigkeits- und Schwachstellenscans.
- Festgestellte Schwachstellen werden nach Schweregrad und tatsächlicher Betroffenheit priorisiert und zeitnah behoben.