

Kundeninformation

Datenschutz und Datensicherheit bei Tajo

Stand: 21. Mai 2025

Tajo unterstützt Unternehmen bei der digitalen Zusammenarbeit mit sensiblen Unternehmens- und Personaldaten. Datenschutz und Datensicherheit sind deshalb fester Bestandteil unserer Produktgestaltung und unserer Zusammenarbeit mit Kunden.

Unser Anspruch ist, Daten nur im vereinbarten Rahmen zu verarbeiten, Zugriffe nachvollziehbar zu begrenzen und die Anwendung durch angemessene technische und organisatorische Maßnahmen zu schützen. Die vertraglichen Einzelheiten stellen wir Ihnen transparent zur Prüfung zur Verfügung – insbesondere unseren Auftragsverarbeitungsvertrag (AVV) und unsere technischen und organisatorischen Maßnahmen (TOMs).

Kurz gesagt: Tajo kombiniert verschlüsselte Übertragung, geschützte Benutzerkonten, rollenbasierte Zugriffsrechte, Mandantentrennung und abgesicherte Schnittstellen. AVV und TOMs schaffen den vertraglichen und organisatorischen Rahmen.

Unsere Datenschutzprinzipien

- **Zweckgebundene Verarbeitung:** Daten werden für die vereinbarten Zwecke und im Rahmen der beauftragten Leistung verarbeitet.
- **Zugriff nach Bedarf:** Nutzer erhalten nur die Rechte, die sie für ihre jeweilige Rolle und ihren Organisationsbereich benötigen.
- **Trennung von Kundendaten:** Zugriffe werden der jeweiligen Unternehmensmitgliedschaft zugeordnet und auf den betreffenden Mandanten begrenzt.
- **Schutz sensibler Informationen:** Verbindungen, Konten, Sitzungen, Schnittstellen und Protokolle werden mit geeigneten Schutzmechanismen abgesichert.
- **Transparenz und Prüfbarkeit:** AVV und TOMs können in Ihre Vertrags- und Datenschutzprüfung einbezogen werden.

Wie Tajo Daten schützt

Sichere Übertragung und Sitzungen

Die Kommunikation mit Tajo wird in der Produktionsumgebung über verschlüsselte HTTPS-Verbindungen abgesichert. Zusätzliche Browserschutzmechanismen und sichere Sitzungscookies reduzieren das Risiko, dass Verbindungen oder Sitzungsinformationen unbefugt genutzt werden.

Geschützte Benutzerkonten

Zugriff erhalten nur aktive Benutzerkonten, die einer gültigen Unternehmensmitgliedschaft zugeordnet sind. Passwörter werden nicht im Klartext gespeichert, sondern mit einem etablierten Verfahren geschützt. Passwort-Zurücksetzungen sind zeitlich begrenzt; wiederholte Anmeldeversuche werden limitiert.

Rollen und Berechtigungen

Tajo verfügt über ein rollenbasiertes Berechtigungssystem. Rechte können differenziert vergeben und unter anderem auf Organisationsbereiche sowie direkte und indirekte Teams begrenzt werden. So lässt sich der Zugriff am tatsächlichen Aufgabenbereich einer Person ausrichten.

Mandantentrennung

Unternehmenszugriffe werden an die jeweilige Mitgliedschaft im Unternehmen gebunden. Die Datenzugriffe der Anwendung sind darauf ausgerichtet, Informationen im Kontext des jeweils ausgewählten Unternehmens zu verarbeiten. Damit wird verhindert, dass reguläre Nutzer auf Daten eines anderen Kundenmandanten zugreifen.

Abgesicherte Schnittstellen

API-Zugriffe erfordern einen unternehmensbezogenen Schlüssel. Diese Schlüssel werden geschützt gespeichert, können widerrufen werden und unterliegen einer Begrenzung der Anfragen. Dadurch lassen sich Integrationen kontrolliert betreiben und bei Bedarf gezielt deaktivieren.

Datenschutzfreundliche Protokollierung

Sensible Werte – darunter Passwörter, E-Mail-Adressen, Tokens, Schlüssel und Sozialversicherungsnummern – werden aus den Anwendungsprotokollen gefiltert. Das reduziert das Risiko, dass vertrauliche Inhalte unbeabsichtigt in technischen Logs erscheinen.

Dateispeicherung in der EU

Produktivdateien werden in einem S3-Speicher in der Region **eu-central-1 (Frankfurt)** abgelegt. Zugangsdaten werden nicht im Anwendungscode hinterlegt, sondern über eine geschützte Konfiguration verwaltet. Angaben zur Datenresidenz weiterer Systeme, etwa Datenbank und Backups, stellen wir im Rahmen der Vertrags- und Datenschutzprüfung nach Bestätigung durch den Betrieb bereit.

Datenschutz ist eine gemeinsame Aufgabe

Tajo stellt die technische Plattform und die vereinbarten Schutzmaßnahmen bereit. Kunden steuern insbesondere, welche Daten eingestellt werden, welche Nutzer Zugang erhalten und welche Rollen und Berechtigungen vergeben werden.

Wir empfehlen daher:

1. Benutzerkonten regelmäßig zu prüfen und nicht mehr benötigte Zugänge zeitnah zu deaktivieren,
2. Rollen nach dem Prinzip der geringsten erforderlichen Berechtigung zu vergeben,

3. API-Schlüssel nur autorisierten Personen und Systemen zugänglich zu machen und bei Bedarf zu widerrufen,
4. interne Aufbewahrungs- und Löschvorgaben festzulegen sowie
5. Beschäftigte für den sicheren Umgang mit Zugangsdaten und personenbezogenen Informationen zu sensibilisieren.

Für Ihre Vertrags- und Datenschutzprüfung

Auf Anfrage bzw. im Rahmen der Beauftragung stellen wir folgende Unterlagen und Angaben bereit:

- **Auftragsverarbeitungsvertrag (AVV)** mit der vertraglichen Einordnung der Verarbeitung,
- **technische und organisatorische Maßnahmen (TOMs)** mit einer detaillierteren Beschreibung der Schutzmaßnahmen,
- Informationen zu Hosting und eingesetzten Unterauftragnehmern/Subprozessoren, soweit für die Prüfung erforderlich,
- **Angaben zu Löschung und Aufbewahrung** entsprechend der vereinbarten Leistung und den betrieblich bestätigten Verfahren sowie
- **Ansprechpartner und Zuständigkeiten** für Datenschutz- und Sicherheitsfragen.

Konkrete Angaben zu Hosting weiterer Systembestandteile, Datenbank- und Backup-Standorten, Wiederherstellung, Verschlüsselung ruhender Daten, Schlüsselmanagement, Zertifizierungen, Penetrationstests, Sicherheitsvorfällen, SSO/MFA oder personenbezogener Zugriffsauditierung werden nur aufgenommen oder zugesagt, wenn sie durch die zuständigen Fachbereiche bestätigt und dokumentiert sind.

Häufige Fragen

Ist Tajo DSGVO-konform?

Die DSGVO-Konformität hängt nicht allein von einer Software ab, sondern auch vom konkreten Einsatzzweck, der Konfiguration und den Prozessen des verantwortlichen Unternehmens. Tajo unterstützt eine datenschutzgerechte Nutzung durch technische Schutzmechanismen sowie durch AVV und TOMs. Die abschließende Bewertung erfolgt im Rahmen Ihrer konkreten Verarbeitung und Datenschutzprüfung.

Können Mitarbeiter anderer Kunden unsere Daten sehen?

Reguläre Nutzerzugriffe sind an eine aktive Mitgliedschaft im jeweiligen Unternehmen gebunden. Die Anwendung ist auf eine mandantenbezogene Verarbeitung ausgerichtet. Welche internen Administrator- oder Supportzugriffe im Ausnahmefall bestehen und wie diese organisatorisch geregelt sind, ergibt sich aus den vereinbarten Unterlagen und Zuständigkeiten.

Werden Daten verschlüsselt?

Die Übertragung zur Anwendung erfolgt in Produktion verschlüsselt über HTTPS. Passwörter und API-Schlüssel werden geschützt verarbeitet beziehungsweise gespeichert. Aussagen zur vollständigen Verschlüsselung sämtlicher ruhender Daten und Backups werden nach Bestätigung des konkreten Hosting- und Schlüsselmanagements bereitgestellt.

Wo werden unsere Daten gespeichert?

Produktivdateien liegen in der AWS-Region eu-central-1 in Frankfurt. Die bestätigten Speicherorte weiterer Systembestandteile, insbesondere Datenbank und Backups, sowie Angaben zu Unterauftragnehmern stellen wir für die Vertrags- und Datenschutzprüfung bereit.

Was passiert bei einem Sicherheitsvorfall?

Die maßgeblichen Meldewege, Verantwortlichkeiten und Fristen werden im AVV, in den TOMs und den betrieblich bestätigten Prozessen beschrieben. Sofern Sie hierzu weitergehende Nachweise benötigen, stimmen wir den erforderlichen Prüfungsumfang mit Ihnen ab.

Können Zugriffe gezielt eingeschränkt werden?

Ja. Rollen und Berechtigungen können differenziert vergeben und auf Organisationsbereiche und Teams begrenzt werden. API-Schlüssel können zudem widerrufen werden.

Unser Angebot: transparente Prüfung statt pauschaler Versprechen

Datenschutz und Sicherheit verdienen konkrete Antworten. Deshalb stellen wir belegbare Schutzmaßnahmen und vertragliche Unterlagen transparent dar und stimmen offene Detailfragen mit den zuständigen Fachbereichen ab. Gerne begleiten wir Ihre Datenschutz-, IT-Sicherheits- oder Einkaufsprüfung und stellen die dafür erforderlichen Unterlagen zusammen.

Hinweis zur Verwendung: Diese Unterlage ist eine allgemeine Kundeninformation und ersetzt weder die individuellen vertraglichen Vereinbarungen noch eine rechtliche Prüfung. Maßgeblich sind der abgeschlossene Vertrag, der AVV, die vereinbarten TOMs und die für den konkreten Einsatz bestätigten Angaben.