CALTRIX®

ANLAGE 2 ZUM VERTRAG ZUR AUFTRAGSVERARBEITUNG · STAND 09.11.2026

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Wie die Plattform Caltrix personenbezogene Daten schützt: Vertraulichkeit, Integrität, Verfügbarkeit, regelmäßige Überprüfung und die Rechte der betroffenen Personen.

Stand: 28.10.2026

1. Vertraulichkeit

Zutrittskontrolle. Die Server stehen in einem Rechenzentrum des Hosters in Deutschland (siehe Anlage 3 zum Vertrag zur Auftragsverarbeitung, die Liste der Unterauftragsverarbeiter). Der Auftragnehmer selbst betreibt keine Serverräume, und die physische Sicherheit obliegt dem Hoster.

Zugangskontrolle. Anmeldung mit E-Mail und Passwort (Hashing nach dem aktuellen Laravel-Standard, bcrypt/argon2). Sperre nach wiederholten Fehlversuchen. Zwei-Faktor-Authentisierung (TOTP) steht jeder Person zur Verfügung. Pflicht ist sie in der Ausbaustufe Compliance, und auf Weisung des Auftraggebers schaltet der Auftragnehmer die Pflicht in jeder Ausbaustufe ein oder ab. Eingeschaltet gilt sie entweder für alle Konten des Mandanten oder nur für die Konten mit Verwaltungsrechten, also für jede Person, die Rollen oder Personen verwaltet, Personalakte, Entgelt oder besonders geschützte Unterlagen einsieht, das Audit-Log liest, Integrationen und API-Token einrichtet oder die Meldestelle und vertrauliche Mentorings öffnet, und zwar auch dann, wenn das Recht nur für ein Team oder eine Abteilung gilt. Diese Liste ist fest und nicht je Mandant änderbar. Erhält eine Person ein solches Recht, verlangt die Anwendung den zweiten Faktor mit ihrer nächsten Anfrage. Optional Single Sign-On über OpenID Connect oder SAML 2.0 gegen das Verzeichnis des Auftraggebers. Administrativer Serverzugang ausschließlich über SSH mit Schlüssel.

Zugriffskontrolle. Rollen- und rechtebasierte Steuerung (RBAC) mit Geltungsbereichen: eine Rolle gilt organisationsweit, für eine Abteilung samt Unterabteilungen oder für ein einzelnes Team. Berechtigungen sind im Code definiert, die Zuordnung zu Rollen pro Mandant konfigurierbar.

Nicht vererbbare Berechtigungen. Zwei Schlüssel nimmt die Rolle des Organisations-Administrators ausdrücklich **nicht** mit: die Einsicht in besonders geschützte Personal-Unterlagen und die Einsicht in Entgeltdaten samt Gehaltsbändern, Entgeltbericht und dem Nachweis nach dem NachwG. Wer sie haben soll, bekommt sie einzeln über eine eigene Rolle, sichtbar in der Rechte-Matrix und mit Eintrag im Audit-Log. Das verhindert, dass die Administration einer Plattform nebenbei die Gehaltsliste der Firma öffnet.

Aggregierte Auswertung der Entgelte. Der Entgeltbericht und die daneben stehende **Lückenanalyse** rechnen auf ein Berichtsjahr, und zwar aus dem Bestand, den die Personalverwaltung ohnehin führt, und seit dem 04.10.2026 aus dem **Ist-Entgelt je Jahr**, sofern der Auftraggeber es aus seinem Lohnjournal einspielt. Diese Ablage ist die einzige Angabe, die allein für den Bericht geführt wird; sie ist verschlüsselt wie das Entgelt und wird mit Ablauf des vierten Jahres nach dem Berichtsjahr gelöscht. Beide geben nur Kennzahlen über Gruppen heraus, nie eine Zeile über eine Person, und sie greifen erst oberhalb der Mindestgruppengröße. Die liegt hier bei sechs Beschäftigten der Vergleichstätigkeit (§ 12 Abs. 3 EntgTranspG) oder bei der höheren allgemeinen Mindestgruppengröße des

Auftraggebers und lässt sich anheben, nicht senken; sie gilt je Merkmal und nicht nur für die Gruppe im Ganzen. Weil die Gruppen einer Aufteilung den Bestand vollständig aufteilen, fällt zusätzlich die kleinste sichtbare Gruppe weg, sobald genau eine unterdrückt wäre, denn sonst ergäbe sie sich als Differenz zur Gesamtzahl. Dieselbe Vorsicht trägt das bereinigte Gefälle: Es mittelt nur die Gruppen, die auch ausgewiesen sind. Zu den Angaben, die Art. 9 Abs. 1 der Richtlinie verlangt, gehören seit dem 09.09.2026 auch der Median, die variablen Bestandteile getrennt samt dem Anteil ihrer Empfänger und die Verteilung der Merkmale über die vier Entgeltquartile. Auch dafür wird nichts zusätzlich erhoben. Die **Grenzen zwischen den Quartilen** werden nicht ausgewiesen, denn eine solche Grenze ist der Betrag einer bestimmten Person; herausgegeben wird allein, wie viele Köpfe je Merkmal in einem Viertel stehen, und das ist eine Aussage über eine Spanne und über keinen Betrag. **Die drei Aufteilungen** nach Vergleichsgruppe, Seniorität und Team **lassen sich nicht kombinieren**, und es führt kein Weg von einer Kennzahl zu den Personen dahinter; zwei Merkmale zusammen wären in den meisten Firmen eine einzelne Person. Die eigene Auskunft nach Art. 15 bleibt davon unberührt und nennt das eigene Entgelt vollständig.

Verschlüsselung einzelner Felder. Über die Verschlüsselung des Transports hinaus liegen besonders sensible Felder **verschlüsselt in der Datenbank**: Entgeltbeträge samt jedem weiteren Bestandteil und Notiz, der Text des Nachweises der Vertragsbedingungen (er enthält das Entgelt im Fließtext), Zwei-Faktor-Geheimnisse sowie hinterlegte Zugangsdaten zu Fremdsystemen. Ein Auszug der Datenbank ohne den Anwendungsschlüssel gibt diese Werte nicht preis. Aus demselben Grund nennt das Audit-Log bei Entgeltänderungen den Vorgang und nie den Betrag.

Import von Entgeltdaten. Entgeltstände, Geschlecht und das Ist-Entgelt je Jahr lassen sich seit dem 04.10.2026 per Datei oder über die Schnittstelle einspielen. Die hochgeladene Datei wird nach dem Lesen gelöscht, die temporäre Datei des Uploads eingeschlossen, und an keiner Stelle aufbewahrt. Zwischen Prüfen und Übernehmen liegt der geprüfte Stand verschlüsselt mit dem Schlüssel der Installation in der Sitzung und verfällt nach 30 Minuten, beim Übernehmen oder Verwerfen sofort. Über die Schnittstelle wird nichts abgelegt, und eine Antwort nennt nur Zahlen. Das Schreiben verlangt dieselben Rechte wie die Pflege von Hand, ein Schnittstellen-Token eine eigene Berechtigung, die nur anlegen kann, wer das Entgelt selbst einsehen darf. Das Audit-Log nennt die Zahl der Zeilen und nie einen Betrag.

Entgelt aus Personio. Seit dem 04.10.2026 kann der Auftraggeber Vertragsstand, Entgelt und Geschlecht aus Personio übernehmen lassen, und zwar nur mit Staff und Pay und nur auf einen eigenen Schalter in der Einrichtung. Seit 2.5 liest sie der Konnektor (nächster Absatz) und schreibt sie über die Public API mit denselben Prüfungen wie ein Import von Hand. Gelesen werden die Vergütungen der Beschäftigten vier Jahre zurück, je mit Art, Betrag, Turnus, Beginn und Wochenstunden, dazu das Geschlecht aus dem Personendatensatz. Sie landen in denselben Tabellen und mit derselben Verschlüsselung wie von Hand gepflegtes Entgelt; je Stand ist die Herkunft vermerkt. Zwischengespeichert wird die Antwort von Personio weder in der Plattform noch im Konnektor, und im Protokoll eines Laufs steht kein Betrag, sondern nur, wie viele Stände angelegt, nachgezogen oder unverändert sind. Vom Entgelt geht nichts zurück nach Personio; zurück gehen allein die Nachweise, die die Plattform selbst zustellt.

Konnektor. Seit 2.5 kann eine eigene Instanz je Mandant Daten aus einem Personal- oder Lohnsystem des Auftraggebers lesen und über die Public API in genau diesen Mandanten schreiben. Sie läuft auf demselben Server wie die Instanz des Auftraggebers, mit eigenem Token, eigenem Prozess und eigenem Schlüsselpaar. Zugangsdaten zum Fremdsystem werden bei der Eingabe an den öffentlichen Schlüssel der Instanz versiegelt und nur so gespeichert; weder der Auftragnehmer noch eine Kopie der Datenbank kann sie öffnen. Dateien holt der Konnektor von einem SFTP-Server, den der Auftraggeber stellt und dessen Schlüssel vor jeder Anmeldung geprüft wird; sie werden nur während des Laufs verarbeitet und danach gelöscht. Log und Laufzustand enthalten weder Beträge noch Namen. Was der Konnektor für eine Person liefert, ist in der Plattform gegen Änderung gesperrt, damit beide Systeme nicht auseinanderlaufen; gesperrt wird nur, was er tatsächlich liefert, und nur, solange er eingerichtet ist.

Trennungskontrolle. Eine eigene Datenbank je Mandant. Die Trennung ist damit keine Filterbedingung in einer Abfrage, sondern eine Verbindungsgrenze: ein Programmierfehler in einer Abfrage kann keine Daten eines anderen Mandanten zutage fördern, weil sie nicht in derselben Datenbank liegen. Die Zuordnung Domain → Mandant erfolgt in einer zentralen Registry; deren Zugangsdaten sind verschlüsselt abgelegt.

Pseudonymisierung und Löschung. Nach dem Austritt einer Person werden deren Stammdaten und persönliche Inhalte nach einer konfigurierbaren Frist (Standard: 24 Monate) anonymisiert. Abschlussnachweise bleiben in anonymisierter Form erhalten, damit der Compliance-Nachweis nicht verloren geht.

2. Integrität

Weitergabekontrolle. Transport ausschließlich über TLS (HTTPS erzwungen). Ausgehende Aufrufe an vom Auftraggeber hinterlegte Adressen (Link-Prüfung, KI-Webhook, OIDC-Discovery) laufen über eine zentrale Prüfung, die nur öffentlich routbare Ziele zulässt (SSRF-Schutz). Die öffentliche API arbeitet mit Zugriffs-Token mit enger Rechtebindung, Ablaufdatum und sofortigem Widerruf; ausgehende Webhooks werden signiert.

Eingabekontrolle. Vollständiges Audit-Log über administrative und sicherheitsrelevante Vorgänge: wer hat wann was geändert. Für den Auftraggeber in der Oberfläche einsehbar und filterbar.

Schutz vor Schadcode und Manipulation. Strikte Content-Security-Policy ohne Inline-Skripte, CSRF-Schutz an jedem Schreibpfad, Ratenbegrenzung nach Zweck an Anmeldung, Import und API, Obergrenzen für Anfragekörper.

Prüfung hochgeladener Dateien. Seit dem 15.10.2026 wird jede Datei, die eine Anfrage mitbringt, geprüft, bevor sie abgelegt oder gelesen wird, gleich an welchem Formular. Abgewiesen werden ausführbare Programme und Skripte (am Inhalt erkannt, nicht nur am Namen), gesperrte Dateiendungen auch hinter einer zweiten Endung, Office-Dokumente mit Makros und PDF-Dateien, die beim Öffnen etwas ausführen. Wo der Auftraggeber es verlangt und die Installation es trägt, prüft zusätzlich ein Virenscanner (ClamAV); ist er dann nicht erreichbar, wird die Datei abgewiesen und nicht ungeprüft abgelegt. Jede abgewiesene Datei steht mit Name, Größe, Grund und Herkunft im Audit-Log, und dieser Eintrag lässt sich nicht abschalten.

Schutz öffentlicher Formulare. Formulare ohne Anmeldung (Bewerbung, Anmeldung zu Veranstaltungen, auch als Widget auf der Website des Auftraggebers) tragen neben der Ratenbegrenzung ein verstecktes Köderfeld und eine Rechenaufgabe, die der Browser im Hintergrund löst. Dafür wird kein Dienst eines Dritten eingebunden und kein Cookie gesetzt; geprüft wird auf dem eigenen Server.

3. Verfügbarkeit und Belastbarkeit

Sicherungskonzept. Tägliche Sicherung der zentralen Datenbank **und jeder einzelnen Mandanten-Datenbank**, komprimiert, mit Prüfsummen-Manifest und automatischer Rotation: Jeder Satz wird **30 Tage** aufbewahrt. Die Sätze selbst sind nicht verschlüsselt, doch die in Abschnitt 1 genannten Felder liegen auch darin verschlüsselt. Ein eigener Befehl prüft einen Satz gegen sein Manifest. Der Anwendungsschlüssel, an dem diese Felder und die Registry-Geheimnisse hängen, wird bewusst getrennt von den Sicherungen verwahrt. Die abgelegten Dateien (Unterlagen, Belege, Anhänge, Videos) sichert beim Betrieb durch den Auftragnehmer die tägliche Datei-Sicherung des Rechenzentrums. Wo eine Instanz ohne sie betrieben wird, sichert die Anwendung ihre Dateien samt der Datenbank-Sätze täglich, inkrementell und verschlüsselt auf ein zweites Ziel in Deutschland und bewahrt jeden Tagesstand **30 Tage** auf, die Dateien jedes Mandanten als eigenen Stand, sodass einer allein zurückkommt und nach seiner Löschung nach 30 Tagen auch aus der Sicherung verschwindet. Verschlüsselt wird mit einem eigenen Sicherungsschlüssel und nicht mit dem Anwendungsschlüssel, damit eine Sicherung allein ohne Wert ist; beide werden getrennt von den Sicherungen verwahrt. Ob eine Instanz gesichert wird, prüft die Betriebsüberwachung: Ohne eigene Sicherung und ohne festgehaltene Sicherung des Rechenzentrums meldet sie einen Befund.

Wiederherstellung. Ein dokumentierter Wiederherstellungsablauf steht in der Betriebsdokumentation und wird vor Aufnahme des Produktivbetriebs einmal vollständig durchgespielt.

Überwachung. Stündliche automatische Prüfung von Hintergrundverarbeitung, Warteschlange, Sicherung und Erreichbarkeit jeder Mandanten-Datenbank; Störungen gehen an eine hinterlegte Alarm-Adresse. Ergänzend eine externe Erreichbarkeitsprüfung.

4. Verfahren zur regelmäßigen Überprüfung

- Automatisierte Testabdeckung; kein Auslieferungsstand ohne grüne Tests.

- Betriebs-Checkliste als Befehl (`ops:preflight`) gegen den laufenden Zustand statt gegen eine Liste im Kopf.
- Last- und Leistungsprüfung der Hauptseiten (`ops:smoke`) vor jeder größeren Auslieferung.
- Sicherheits-Durchgänge nach OWASP-Systematik; die Ergebnisse und die daraus bindenden Regeln sind in der Plattform-Spezifikation dokumentiert.

5. Betroffenenrechte in der Plattform

Recht	Umsetzung
Auskunft (Art. 15)	Jede Person sieht unter „Meine Daten" ihren vollständigen Datenbestand und lädt ihn als Export herunter, ohne Antrag und ohne Administrator. Die Auskunft umfasst **beide Produktlinien und jedes Zusatzmodul**: neben Lernangaben, Lernaktivität, Kompetenzstand, Anmeldungen, Rollen, Anträgen, Benachrichtigungen und E-Mails auch Vertragsstände, Unterlagen der Personalakte, Abwesenheiten, Urlaubskonto, Austritt, Arbeitszeugnis, Nachweise nach dem NachwG, Entgeltstände, das Ist-Entgelt je Jahr, Zeitbuchungen und Bewerbungen, dazu Feedbackgespräche, Mentoring-Sitzungen samt Notizen, Schulungen, externe Nachweise, Prüfungsversuche, Übergaben und die Meldungen des angebundenen Personalsystems. Sie folgt dem **Bestand** und nicht der Buchung: Ein abbestelltes Produkt lässt seine Tabellen stehen, und was steht, wird beauskunftet. Unterlagen und hochgeladene Nachweise werden dabei mit Kategorie, Name, Datum und Aufbewahrungsfrist **benannt**; die Datei selbst gibt die Auskunft nicht heraus, dafür bleibt die Freigabe an der Akte maßgeblich. Interne Notizen über eine Person gehören zur Kopie nach Art. 15 Abs. 3, Angaben über Dritte bleiben nach Art. 15 Abs. 4 draußen. Seit 20.09.2026 nennt die Auskunft zusätzlich die **Erwähnungen in den Meldungen anderer**, und zwar mit Art und Zeitpunkt, ohne die empfangende Person und ohne den Text: Das Postfach gehört jemand anderem, und der Text benennt womöglich einen weiteren Dritten
Auskunft ohne eigenen Zugang	Wer **noch keinen oder keinen Zugang** hat, erreicht die Seite nicht: Bewerberinnen und Bewerber von außen, Personen im Preboarding vor dem ersten Arbeitstag und Gäste an einem einzelnen Lernpfad. Für sie beantwortet der Verantwortliche die Anfrage auf dem üblichen Weg; die Plattform liefert die Angaben dafür aus der Personalakte und der Bewerbungsakte
Berichtigung (Art. 16)	Profildaten selbst änderbar, Stammdaten über die Administration
Löschung (Art. 17)	Anonymisierung, entweder mit dem Ablauf der Aufbewahrungsfrist nach dem Austritt oder auf Weisung sofort. Der Weg dorthin steht auf jeder Personenseite und gehört zu jedem gebuchten Umfang, denn ein Recht der betroffenen Person richtet sich nicht danach, was die Organisation gebucht hat. **Die Löschung deckt denselben Umfang wie die Auskunft**: Was die eine nennt, räumt die andere, und beide Richtungen sind durch Tests aneinander gebunden. Erhalten bleiben allein Zeilen, die eine Aussage über die Organisation tragen (Abschlüsse, Nachweise, entschiedene Vorgänge, Audit-Log, die Teilnahme an vergangenen Terminen); ihr Freitext fällt. Anmeldungen an künftigen Terminen werden abgemeldet, und der Platz geht an die Warteliste, das Zustellprotokoll der E-Mails verliert Adresse, Name und Betreff. Seit 20.09.2026 erreicht die Löschung auch die Benachrichtigungen **anderer** Menschen, die die betroffene Person beim Namen nennen: Die Meldung bleibt als Aufzeichnung der empfangenden Person stehen, der Name darin wird durch die Bezeichnung der gelöschten Person ersetzt. Gefunden wird sie über einen Verweis an der Zeile und nicht über eine Suche nach dem Namen; benennt eine Meldung mehrere Menschen, fällt allein der Name der gelöschten
Datenübertragbarkeit (Art. 20)	Export in maschinenlesbarem Format
Widerspruch (Art. 21)	Optionale Funktionen (etwa Push-Benachrichtigungen oder der Eintrag im Expertenverzeichnis) laufen über eine ausdrückliche, jederzeit widerrufbare Einwilligung

Caltrix Software UG (haftungsbeschränkt) · Am Steeg 4 · 65239 Hochheim am Main · Amtsgericht Wiesbaden HRB 37080 · Geschäftsführer Patric Eid · kontakt@caltrix.de
Eine Tochtergesellschaft der Eid Hub GmbH. Das Caltrix-Logo ist eine eingetragene Wort-/Bildmarke der Eid Hub GmbH (DPMA 30 2026 245 801).