CALTRIX®

MUSTERVERTRAG · STAND 09.11.2026

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Für die Nutzung der Plattform Caltrix, mit Anlage 1 (Gegenstand der Verarbeitung), Anlage 2 (technische und organisatorische Maßnahmen) und Anlage 3 (Unterauftragsverarbeiter).

Präambel

Zwischen

Auftraggeber (Verantwortlicher):

Firma, Anschrift, vertreten durch

(nachfolgend „Auftraggeber“)

und

Auftragnehmer (Auftragsverarbeiter): Caltrix Software UG (haftungsbeschränkt), Am Steeg 4, 65239 Hochheim am Main, eingetragen beim Amtsgericht Wiesbaden unter HRB 37080, vertreten durch den Geschäftsführer Patric Eid (nachfolgend „Auftragnehmer“)

wird der folgende Vertrag zur Auftragsverarbeitung geschlossen. Er konkretisiert den zwischen den Parteien geschlossenen Hauptvertrag über die Nutzung der Plattform **Caltrix** (nachfolgend „die Plattform"). Die Plattform umfasst je nach Buchung die Lern- und Entwicklungsanwendung (**Caltrix Campus**) und die Personalverwaltung (**Caltrix Staff** samt der Bausteine Time, Hire und Pay). Welche Teile gebucht sind, ergibt sich aus dem Hauptvertrag; **Anlage 1** weist die Datenarten je Teil aus.

Der Auftraggeber bleibt Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich weisungsgebunden.

§ 1 Gegenstand und Dauer

(1) Gegenstand. Der Auftragnehmer betreibt für den Auftraggeber eine mandantenfähige Lern- und Personalverwaltungsplattform. Die Verarbeitung umfasst das Speichern, Anzeigen, Auswerten und Löschen der in **Anlage 1** beschriebenen Daten zu den dort genannten Zwecken. Welche der dort genannten Datenarten tatsächlich anfallen, hängt davon ab, welche Teile der Plattform der Auftraggeber gebucht hat.

(2) Dauer. Die Laufzeit entspricht der des Hauptvertrags. Sie endet mit dessen Beendigung, spätestens mit der vollständigen Rückgabe oder Löschung der Daten nach § 8.

(3) On-Premises. Betreibt der Auftraggeber die Plattform auf eigener Infrastruktur (On-Premises-Lizenz), findet **keine** Auftragsverarbeitung statt, denn der Auftragnehmer erhält keinen Zugriff auf personenbezogene Daten. Dieser Vertrag gilt dann nicht; für Support-Fälle mit Datenzugriff ist eine gesonderte Vereinbarung zu schließen.

§ 2 Art, Umfang und Zweck der Verarbeitung

Art, Umfang, Zweck, Datenarten und Kategorien betroffener Personen ergeben sich abschließend aus **Anlage 1**. Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt. Insbesondere werden die Daten des Auftraggebers **nicht** zum Training von KI-Modellen, zur Profilbildung über Mandanten hinweg oder zur Erstellung von Benchmarks verwendet.

§ 3 Weisungsrecht

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaates zur Verarbeitung verpflichtet.

(2) Weisungen erfolgen in Textform. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Hält der Auftragnehmer eine Weisung für rechtswidrig, teilt er dies dem Auftraggeber unverzüglich mit und darf die Ausführung bis zur Bestätigung aussetzen.

§ 4 Technische und organisatorische Maßnahmen

Der Auftragnehmer unterhält die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Er darf sie fortschreiben, solange das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen teilt er dem Auftraggeber mit.

§ 5 Vertraulichkeit

Der Auftragnehmer setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet und mit den einschlägigen Datenschutzvorschriften vertraut gemacht wurden (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO).

§ 6 Unterauftragsverhältnisse

(1) Der Auftraggeber stimmt dem Einsatz der in **Anlage 3** genannten Unterauftragsverarbeiter zu.

(2) Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen mindestens **30 Tage** im Voraus in Textform. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem Grund widersprechen; kommt keine Einigung zustande, steht ihm ein Sonderkündigungsrecht zu.

(3) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter auf gleichwertige Datenschutzpflichten.

(4) Als Unterauftragsverhältnis gelten **nicht** Nebenleistungen ohne Bezug zu den Daten des Auftraggebers (Telekommunikation, Reinigung, Wartung).

§ 7 Unterstützungspflichten

Der Auftragnehmer unterstützt den Auftraggeber angemessen bei

- Anfragen betroffener Personen nach Art. 15 bis 21 DSGVO,
- Meldungen von Datenschutzverletzungen nach Art. 33, 34 DSGVO,
- Datenschutz-Folgenabschätzungen nach Art. 35, 36 DSGVO.

Die Plattform stellt die zugehörigen Funktionen bereit, sodass der Auftraggeber die meisten Anfragen **selbst und ohne Zutun des Auftragnehmers** beantworten kann (siehe Anlage 2, Abschnitt „Betroffenenrechte").

Meldung von Datenschutzverletzungen: Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch **innerhalb von 24 Stunden** nach Kenntniserlangung.

§ 8 Löschung und Rückgabe

(1) Während der Laufzeit kann der Auftraggeber jederzeit einen vollständigen Datenexport in einem gängigen, maschinenlesbaren Format (JSON/CSV je Tabelle samt Beschreibung, dazu die abgelegten Dateien) in der Plattform selbst erstellen. Nach Beendigung des Hauptvertrags stellt der Auftragnehmer ihm diesen Export auf Wunsch bereit, und zwar bis **30 Tage** nach Vertragsende, sofern der Hauptvertrag keine andere Frist bestimmt.

(2) Nach Ablauf dieser Frist löscht der Auftragnehmer die Daten binnen weiterer **30 Tage**: die abgelegten Dateien des Auftraggebers (Unterlagen, Belege, Anhänge, Videos), die in einem eigenen Ordner je Mandant liegen, und danach seine Datenbank, denn auch davon hat jeder Mandant eine eigene. Die Löschung bestätigt der Auftragnehmer auf Wunsch schriftlich.

(3) Sicherungskopien werden im Rahmen des regulären Rotationszyklus überschrieben; die maximale Nachlaufzeit ergibt sich aus Anlage 2 (Sicherungskonzept) und beträgt **längstens 30 Tage**.

(4) Gesetzliche Aufbewahrungspflichten bleiben unberührt.

(5) Löschung im laufenden Betrieb. Unabhängig vom Vertragsende löscht die Plattform fristgebunden von selbst. Maßgeblich ist die folgende Übersicht; wo eine Frist einstellbar ist, kann der Auftraggeber sie verkürzen, eine gesetzliche Untergrenze aber nicht unterschreiten.

Datenart	Frist	Auslöser und Durchführung
Stammdaten und persönliche Inhalte ausgeschiedener Personen	24 Monate *(einstellbar)*	Austritt; Anonymisierung über den Tilgungslauf, Abschlussnachweise bleiben anonymisiert erhalten
Personal-Unterlagen	je Kategorie hinterlegte Aufbewahrungsfrist	Ablauf der Frist am einzelnen Dokument
Bewerbungen *(Hire)*	6 Monate nach Abschluss des Verfahrens *(einstellbar)*	Absage oder Rückzug; der Lauf `staff:prune-applications` löscht Zeile **und** hochgeladene Datei
Talentpool *(Hire)*	12 Monate *(einstellbar)*, jederzeit widerruflich	Einwilligung beim Eingang; der Widerruf holt die reguläre Frist zurück. Seit 01.09.2026 ist der Pool als Liste einsehbar (Personal → Recruiting → Talentpool, Recht `hire.manage`): **aufgenommen wird niemand von dort**, denn die Einwilligung erteilt nur, wen sie betrifft; entfernen kann die Verwaltung jederzeit, und wessen Frist verstrichen ist, erscheint gar nicht mehr
Zeitaufzeichnungen *(Time)*	36 Monate *(einstellbar)*, **mindestens 24 Monate**	Der Lauf `time:prune` erzwingt die Untergrenze aus § 16 Abs. 2 ArbZG selbst
Entgelt-, Zeugnis- und Nachweisdaten	mit der Tilgung der Person	Vollständige Löschung; die Tatsache einer Aushändigung bleibt nur im Audit-Log ohne Inhalt

Datenart	Frist	Auslöser und Durchführung
Ist-Entgelt je Jahr *(nur mit Pay)*	mit Ablauf des vierten Jahres nach dem Berichtsjahr, spätestens mit der Tilgung der Person	Vollständige Löschung; feste Frist, denn die Werte braucht der Bericht im Folgejahr, und nachgewiesen werden muss er, solange daraus Ansprüche entstehen können (Art. 21 der Richtlinie (EU) 2023/970: mindestens drei Jahre)
Zustellprotokoll der E-Mails	6 Monate *(einstellbar)*	Zeitpunkt des Versands; der Lauf `privacy:apply-retention` löscht die Zeilen
Teilnahme an Befragungen	24 Monate nach dem Schließen einer Welle *(einstellbar)*	Der Lauf `privacy:apply-retention` nimmt die **Person aus der Zeile** und löscht sie nicht, denn sie trägt zugleich die Antwortquote der Welle, und die ist eine Aussage über die Organisation. Die Antworten selbst altern nicht, weil sie bei einer anonymen Befragung an niemandem hängen
Wochenstimmung	12 Monate *(einstellbar)*	Kalenderwoche der Angabe; der Lauf `privacy:apply-retention` löscht die Zeilen
Zwischenstände angefangener Eingaben *(seit 16.10.2026)*	3 Monate *(einstellbar)*	Letztes Sichern; Abgabe und Speichern räumen sie ohnehin. Der Lauf `privacy:apply-retention` löscht die Zeilen. Gespeichert wird verschlüsselt, was die Person in einen laufenden Quizversuch, eine Reflexion oder eine Praxisaufgabe eingegeben und noch nicht abgeschickt hat
Teilnahme an Terminen (Schulungen, Veranstaltungen) *(seit 02.10.2026)*	unbegrenzt, bis der Auftraggeber eine Frist setzt *(einstellbar unter Verwaltung › System › Aufbewahrung)*	Ende des Termins, bei einer Serie ihr letzter Termin. Der Lauf `privacy:apply-retention` **anonymisiert**: Person, Name und Adresse eines Gasts, Ticket und Newsletter-Wunsch fallen, ebenso die Adresse im Anwesenheitsprotokoll, der Name an einer Frage aus dem Live-Webinar und der Verweis vom Anmeldeantrag auf die Teilnahme. Status und Zeitpunkte bleiben für Auslastung und Anwesenheitsquote; die anonymisierte Zeile trägt keine Organisationseinheit mehr
Quizversuche *(seit 02.10.2026)*	unbegrenzt, bis der Auftraggeber eine Frist setzt *(einstellbar)*	Abgabe des Versuchs. Der Lauf **anonymisiert**: Die Person fällt, Ergebnis und Antworten bleiben für die Bestehensquote des Quiz
Schulungsnachweise, die nicht mehr gelten *(seit 02.10.2026)*	unbegrenzt, bis der Auftraggeber eine Frist setzt *(einstellbar)*	Widerruf oder Ablauf; der Lauf **löscht** den Nachweis. Ein gültiger Nachweis altert nicht

Datenart	Frist	Auslöser und Durchführung
Zeitzugabe an Quizzen ***(seit 2.4)***	24 Monate *(einstellbar, auch auf unbegrenzt)*	Letzte Verwendung, also der Beginn des letzten Versuchs der Person an dem Quiz, ohne Versuch das Gewähren oder Ändern der Zugabe; der Lauf **löscht** die Zugabe. Ein Grund wird nie gespeichert. Mit der Löschung der Person fällt sie ohnehin
Archiv der Aufbewahrung ***(seit 02.10.2026)***	**30 Tage**, nicht verkürzbar	Was der Lauf an den vorigen Datenarten ab der Teilnahme an Terminen anonymisiert oder löscht, liegt vorher verschlüsselt im Archiv und kann vom Auftraggeber (Recht `retention.manage`) zurückgeholt werden; danach löscht der Lauf es endgültig. Ein zurückgeholter Datensatz bleibt ohne Inhalt als Vermerk stehen, und der Lauf erfasst ihn nicht wieder. Jedes Zurückholen und jede endgültige Löschung steht im Audit-Log. Vor jeder Frist meldet die Plattform den Org-Admins und den Inhabern dieses Rechts die Zahl der fälligen Datensätze
Ankommens-Checkliste	mit der Tilgung der Person	Sie hängt an der Person und fällt mit ihr
Supportanfragen ***(seit 16.10.2026)***	mit der Tilgung der Person, eine noch offene Anfrage mit ihrem Abschluss	Eine abgeschlossene Anfrage wird samt Verlauf und Anhängen gelöscht. Eine offene bleibt ohne Personenbezug stehen, denn sie betrifft den Betrieb des Auftraggebers, und lässt sich an eine andere Person übertragen; der Name fällt auch aus Antworten, die jemand für die Person gab. Der Vorgang im Ticketsystem des Auftragnehmers wird auf Weisung gelöscht
Vertretungen	mit der Tilgung der Person	Beide Richtungen werden gelöscht; dass jemand in Vertretung gehandelt hat, bleibt nur im Audit-Log
Projektteams ***(seit 02.10.2026)***	mit der Tilgung der Person, sonst mit dem Projektteam	Die Mitgliedschaft samt Anteil wird gelöscht, ein geleitetes Projektteam verliert seine Leitung. Ein beendetes Projektteam bleibt stehen, bis der Auftraggeber es löscht; wer drin war, steht dann nur noch im Audit-Log
Audit-Log	für die Dauer des Vertrags	Anonymisiert mit der Tilgung der Person

Auf Wunsch einer betroffenen Person löscht der Auftraggeber vorzeitig über die Tilgungsfunktion der Plattform; sie räumt dabei auch die Modul-Tabellen und die zugehörigen Dateien.

§ 9 Nachweise und Kontrollrechte

(1) Der Auftragnehmer weist die Einhaltung der Pflichten aus diesem Vertrag auf Anforderung nach, insbesondere durch Vorlage der Anlage 2 im jeweils aktuellen Stand.

(2) Der Auftraggeber ist berechtigt, sich nach Voranmeldung mit einer Frist von **14 Tagen** zu üblichen Geschäftszeiten von der Einhaltung zu überzeugen. Vor-Ort-Prüfungen erfolgen höchstens einmal jährlich, es sei denn, es besteht ein konkreter Anlass.

§ 10 Drittlandtransfer

Eine Verarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums findet **nicht** statt. Sollte sie künftig erforderlich werden, setzt sie eine vorherige Vereinbarung nach Kapitel V DSGVO voraus.

§ 11 Schlussbestimmungen

(1) Änderungen bedürfen der Textform.

(2) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags vor, soweit sie den Datenschutz betreffen.

(3) Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt.

Ort, Datum, Unterschrift Auftraggeber	Ort, Datum, Unterschrift Auftragnehmer

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).

Anlage 1: Gegenstand der Verarbeitung

Zwecke

Caltrix Campus (Lernen und Entwicklung). Onboarding neuer Beschäftigter, Zuweisung und Nachverfolgung von Lerninhalten, Nachweis von Pflichtschulungen, Organisation von Veranstaltungen und Schulungen, Mentoring, Kompetenzverwaltung sowie die zugehörigen Auswertungen.

Caltrix Staff (Personalverwaltung), soweit gebucht. Führung der Personalakte samt Vertragshistorie, Abbildung der Berichtslinie, Verwaltung von Unterlagen mit Aufbewahrungsfristen, Bearbeitung von Anträgen (Urlaub, Homeoffice, Fortbildung, Stammdatenänderung) einschließlich des Urlaubsanspruchs, Erfassung von Abwesenheiten, Abwicklung von Eintritt und Austritt samt Kündigungsfristen und Rückgabeliste, Erstellung von Arbeitszeugnissen und des Nachweises der wesentlichen Vertragsbedingungen nach dem Nachweisgesetz.

- **Time**, soweit gebucht: Aufzeichnung der Arbeitszeit einschließlich der Prüfung gegen die Grenzen des Arbeitszeitgesetzes und der Führung eines Zeitkontos.
- **Hire**, soweit gebucht: Ausschreibung von Stellen sowie Entgegennahme und Bearbeitung von Bewerbungen einschließlich der fristgebundenen Löschung.
- **Pay**, soweit gebucht: Auskunft über das Entgelt der Vergleichsgruppe und Auswertung des geschlechtsspezifischen Entgeltgefälles nach der Richtlinie (EU) 2023/970.

Die Verarbeitung dient jeweils der Erfüllung des Beschäftigungsverhältnisses und der rechtlichen Pflichten des Auftraggebers als Arbeitgeber; die Rechtsgrundlage bestimmt der Auftraggeber als Verantwortlicher.

Kategorien betroffener Personen

Kategorie	Herkunft
Beschäftigte des Auftraggebers	Anlage durch Administratoren, Einladung, HRIS-Schnittstelle, Konnektor zu einem Personal- oder Lohnsystem (etwa Personio) oder SCIM
Externe Gäste von Veranstaltungen	Selbst-Anmeldung über einen öffentlichen Link (Double-Opt-In)
Externe Gäste von Schulungen und Lernpfaden	Selbst-Registrierung mit Code (Double-Opt-In), Freischaltung durch Administratoren, Eintrag an einer Schulung durch Administratoren
Externe Trainer und Mentoren	Anlage durch Administratoren
Administratoren des Auftraggebers	wie Beschäftigte
Bewerberinnen und Bewerber *(nur mit Hire)*	Eigene Eingabe über das Bewerbungsformular oder interne Bewerbung
Freie Mitarbeitende *(nur mit Staff)*	Anlage durch Administratoren; Rahmenvertrag als Vertragsart
Hinweisgebende Personen *(nur mit Staff)*	Eigene Eingabe über den Meldekanal nach dem HinSchG, in der Regel **anonym**; ein Konto entsteht dabei nicht

Kategorien personenbezogener Daten

Datenart	Beispiele	Zweck
Stammdaten	Vor-/Nachname, E-Mail, Personalnummer, Eintritts-/Austrittsdatum; seit 04.10.2026 kann die E-Mail fehlen, dann ist die Personalnummer der Schlüssel, und die Person meldet sich nicht an und bekommt keine Mail	Identifikation, Zeitanker der Lernpfade
Organisationsdaten	Team, Abteilung, Position, Seniorität, Standort, Team-Rolle	Zuweisungsregeln, Sichtbarkeit, Auswertung
Zugangsdaten	Passwort-Hash, Zwei-Faktor-Geheimnis, Sitzungen, Anmeldeversuche. Bei **Gästen eines Lernpfads** tritt an die Stelle der Sitzung ein signiertes **Zutritts-Cookie** (`caltrix_guest`), das vier Stunden gilt und sich bei jedem Aufruf erneuert. Seit 30.09.2026 kommt ein zweites Cookie dazu, das allein festhält, **dass** die Begrüßung des Zugangs in diesem Browser schon angezeigt wurde (`caltrix_guest_intro_<Nummer des Zugangs>`, Wert „1", kein Name). Es gilt bis zum Ablauf des Zugangs und höchstens ein Jahr, denn es überdauert den Zugang nicht. Beide Cookies gelten nur im Gast-Bereich (`/gast`) und sind für den Browser-Skriptzugriff gesperrt	Anmeldung, Missbrauchsschutz; beim Begrüßungs-Merker: die Begrüßung beim zweiten Besuch zugeklappt zeigen
Meldungen nach dem HinSchG *(nur mit Staff, nur bei eingeschaltetem Meldekanal)*	Gegenstand, Betreff, Meldetext, Nachrichtenverlauf, Fristzeitpunkte; bei freiwilliger Namensnennung Name und Kontaktweg der hinweisgebenden Person. Kein Verweis auf einen Personendatensatz, keine IP-Adresse, kein Gerätemerkmal. Betreff, Text und Nachrichten feldverschlüsselt; Einsicht nur mit `whistleblower.office`; Löschung drei Jahre nach Abschluss	Erfüllung der Pflicht aus §§ 12, 16, 17 HinSchG
Anzeige-Vorlieben *(seit 24.09.2026)*	Die **von der betroffenen Person selbst** im Profil gewählte Schriftgröße, „weniger Bewegung" und „ruhigere Oberfläche". Voreinstellung: nichts gewählt. Weil eine größere Schrift auf eine Sehbeeinträchtigung hindeuten kann, gibt es **keinen Weg für die Administration**, die Wahl zu setzen oder einzusehen; sie steht allein in der Selbstauskunft der Person und geht mit der Löschung	Darstellung der Oberfläche nach der Wahl der Person
Profilfoto	Ein **freiwillig** von der betroffenen Person selbst hochgeladenes Bild. Es gibt keinen Weg, jemandem ein Foto zu geben oder zu entziehen: Hochladen und Entfernen stehen allein auf der eigenen Profilseite, die Voreinstellung ist „kein Foto", und wer keines hinterlegt, erscheint mit seinem Namenskürzel. Gespeichert wird nicht die hochgeladene Datei, sondern eine quadratisch zugeschnittene, auf 256 Pixel gerechnete Fassung; ausgeliefert wird sie **nur an angemeldete Personen desselben Mandanten** und nie im offenen Netz. Sichtbar ist sie dort, wo ohnehin der Name steht (Kopfzeile, Team-Cockpit, Betreuungsliste, Community, Personenseite). Mit der Löschung der Person wird die Datei entfernt	Wiedererkennen von Menschen in Listen und Gesprächen

Datenart	Beispiele	Zweck
Lerndaten	Zuweisungen, Fortschritt, Abschlüsse, Quiz-Ergebnisse, Abgaben, Reflexionen. Seit 2.4 dazu die **Zeitzugabe an einem Quiz**: Minuten und wer sie gewährt hat, nie ein Grund; sie altert ab ihrer letzten Verwendung (Fristentabelle oben). Aus den Abschlüssen entsteht zusätzlich ein **Empfehlungs-Hinweis für die Belegschaft** („Andere in deiner Rolle haben das gemacht"): Er nennt allein die **Kopfzahl** der Abschlüsse innerhalb derselben Rollenbezeichnung, **keinen Namen, keinen Anteil und keine Gruppengröße**, und er erscheint erst oberhalb der Mindestgruppengröße (Voreinstellung fünf, `CALTRIX_MIN_GROUP_SIZE`, vom Auftraggeber anhebbar). Wo nichts abgeschlossen wurde, erscheint **kein** Hinweis; eine Aussage darüber, wer etwas **nicht** absolviert hat, ist damit ausgeschlossen. Führt der Auftraggeber ein **eigenes Statusmodell**, kommt je Teilnahme der von ihm benannte Zustand hinzu (etwa „in Bearbeitung", „ausgesetzt") samt einem **Verlauf** der Wechsel mit Zeitpunkt, auslösendem Ereignis und, bei einer Umschaltung von Hand, der handelnden Person und ihrem Vermerk. Die Zustände und ihre Bezeichnungen setzt allein der Auftraggeber; ohne gepflegtes Modell entsteht kein einziger Datensatz. Der Verlauf steht in der Selbstauskunft „Meine Daten" und geht mit der Löschung der Person unter. Bei **Gästen eines Lernpfads** im Nachweis-Modus entstehen dieselben Lerndaten an ihrer Gast-Person, seit 24.09.2026 auch abgehakte Checklisten und Antworten auf Reflexionsfragen, die allein der Gast sieht; sie stehen in seiner Selbstauskunft und gehen mit seinen übrigen Gast-Daten. Im offenen Modus entsteht nichts davon. Verlangt ein Inhalt eine **Lesebestätigung** (seit 01.10.2026, Add-on Pflichtunterweisungen), wird je Person und Fassung die **Kenntnisnahme** festgehalten: Inhalt, Titel zum Zeitpunkt der Bestätigung, Fassung und Zeitpunkt. Sie ist keine Signatur, steht in der Selbstauskunft und bleibt wie die Abschlüsse als Nachweis an der gelöschten Person stehen, die danach keinen Namen mehr trägt	Kern der Leistung; beim Hinweis zusätzlich: Orientierung der Belegschaft bei der eigenen Auswahl; beim Statusmodell: Nachvollziehbarkeit des Bearbeitungsstands
Nachweise	Zertifikate, Gültigkeitsdaten, hochgeladene Belege	Compliance-Nachweis
Supportanfragen ***(seit 16.10.2026)***	Betreff, Text, vorgeschlagene und bestätigte Klasse, Anhänge (etwa ein Bildschirmfoto), der Verlauf aus Rückfragen und Antworten, Bearbeitungsstand mit Zeitpunkten (Eingang, erste Reaktion, Wiederherstellung, Erledigung), Name und E-Mail der anfragenden Person. Die Anfrage verlässt den Mandanten als E-Mail an den Support und als Vorgang im Ticketsystem des Auftragnehmers; dorthin gehen Betreff, Text, Name, E-Mail und die Antworten der Person, **nicht** die Anhänge, die in der Ablage des Mandanten bleiben und nur über die Betriebskonsole mit Protokoll abgerufen werden. Aus dem Ticketsystem kommen Stand, Bearbeiter und die für den Kunden freigegebenen Antworten zurück. Einsicht und Antwort hat die anfragende Person und, wer beim Auftraggeber `support.manage` trägt; dort steht dann der eigene Name. Eine Anfrage lässt sich an eine andere Person des Auftraggebers übertragen	Bearbeitung von Störungen und Fragen; Nachweis zugesagter Reaktions- und Wiederherstellungszeiten

Datenart	Beispiele	Zweck
Personio *(seit 30.09.2026; Abruf seit 2.5 über den Konnektor)*	**Herein**, nur mit Staff und nur bei eingerichtetem Konnektor (Zeile „Konnektor zu Personal- und Lohnsystemen"): Name, Rufname, E-Mail, Personalnummer, Eintritts- und Austrittsdatum, Position, Team, Abteilung, Führungskraft, ob die Person in Personio inaktiv ist, wahlweise Standort und Seniorität aus einem Zusatzfeld, die Vertragsstände und der **Zeitraum genehmigter Abwesenheiten** samt einer Art aus Urlaub, Bildung oder „abwesend", **ohne Grund und ohne Kommentar**; eine Krankheit wird nie als solche übernommen. Mit Pay und nur auf einen eigenen Schalter zusätzlich die **Vergütungen der letzten vier Jahre und das Geschlecht** (siehe „Entgelt aus Personio" in Anlage 2). Gespeichert wird je Datensatz nur die Herkunft (Konnektor) und je Abwesenheit ihre Kennung in Personio, damit eine dort gelöschte Abwesenheit beim nächsten Lauf storniert wird; einen Prüfwert, eine Kopie der Antwort von Personio oder deren weitere Angaben wie Geburtstag oder Profilbild gibt es nicht. Was der Konnektor führt, ist in der Plattform gegen Änderung gesperrt und wird in Personio geändert. **Hinaus**, nur mit Integrationen und auf ausdrücklichen Schalter: abgeschlossene Lernpfade, Schulungsnachweise und externe Nachweise als PDF in der Personio-Akte, samt einem Vermerk je Nachweis mit Titel, Zeitpunkt und der Kennung des Dokuments in Personio; ein widerrufener Nachweis wird dort gelöscht. Die Person in Personio findet der erste Versand über ihre E-Mail-Adresse, und ihre Kennung dort wird gespeichert. **Nie** übermittelt werden Fortschritt, Stimmung oder Kompetenzstufen. Personio ist dabei ein vom Auftraggeber verbundenes Fremdsystem (siehe unten); das Zugangspaar für die Nachweise liegt verschlüsselt, die Kennung in Personio wird mit der Löschung der Person entfernt	Führung der Stammdaten im System des Auftraggebers ohne doppelte Pflege; Anhalten der Lernfristen während einer Abwesenheit; Ablage der Nachweise in der Personalakte des Auftraggebers
Konnektor zu Personal- und Lohnsystemen *(mit Staff, nur bei eingerichteter Instanz, seit 2.5)*	Personen, Vertragsstände, Abwesenheiten (Zeitraum und Art, kein Grund) und mit Pay das Entgelt aus dem vom Auftraggeber benannten System, übermittelt über die Public API in genau diesen Mandanten. Die Instanz läuft auf demselben Server wie die Instanz des Auftraggebers und speichert keine Entgelt- oder Personendaten, sondern nur Laufzustand mit Zahlen; Dateien, die sie vom SFTP-Server des Auftraggebers holt, liegen nur für die Dauer eines Laufs auf dem Server und werden danach gelöscht. In der Plattform steht an Person, Vertrags- und Entgeltstand, dass der Konnektor sie führt, und welche Felder er zuletzt geliefert hat	Führung der Stammdaten und des Entgelts ohne doppelte Pflege
Veranstaltungsdaten	Anmeldungen, Warteliste, Anwesenheit, Gast-Name/-E-Mail; bei einer Live-Übertragung zusätzlich die gestellten Fragen, die abgegebenen Ja/Nein-Stimmen, bei einer bereitgestellten Datei der Vermerk, dass eine Anmeldung sie heruntergeladen hat, sowie **zwei Zeitstempel je Anmeldung** (erste Öffnung des Players und letztes Lebenszeichen), aus denen sich die Anwesenheit ergibt, beim Webinar auf Abruf dazu ein **pseudonymes Sitzungsmerkmal**, das allein dazu dient, dem Zuschauer seine eigenen Fragen wieder anzuzeigen	Organisation von Terminen, Durchführung der Übertragung, Anwesenheitsnachweis
Kompetenzdaten	Selbst- und Fremdeinschätzungen, Entwicklungsziele, Karriereziele. Im **Expertenverzeichnis** („Wer kann was?") sind Name, Kompetenz und Stufe zusätzlich für die übrige Belegschaft sichtbar, jedoch **nur nach ausdrücklicher Freischaltung durch die betroffene Person** und jederzeit widerruflich; die Voreinstellung ist „nicht gelistet", das Verzeichnis weist keine fehlenden Kompetenzen aus	Entwicklungsplanung, betrieblicher Wissensaustausch

Datenart	Beispiele	Zweck
Wissen, das an einer Person hängt ***(ab der Ausbaustufe Entwicklung, seit 01.10.2026)***	**Abgeleitet und nicht gespeichert**: welche Kompetenz im Umfeld einer Person (eigene Teams und Teams derselben Abteilung) nur sie auf ihrer Stufe trägt. Gerechnet wird bei jedem Aufruf aus den Kompetenzdaten, gespeichert wird allein die Einstellung des Auftraggebers (aus, ohne Namen, mit Namen) und jeder Wechsel im Audit-Log. **Ohne Namen** nennt die Sicht Kompetenz, Stufe und Team, ein Team aber erst ab der Mindestgruppengröße, sonst die Abteilung oder den ganzen Bereich. **Mit Namen** zusätzlich die Person, und die Person sieht in ihrem Profil, dass und mit welchen Kompetenzen sie dort steht. Sichtbar für die Führungskraft im eigenen Verwaltungs-Scope und für Inhaber einer eigenen, nicht vererbten Berechtigung. **Nie** einbezogen werden Alter, Eintrittsdatum, Nähe zum Ruhestand oder Austrittsdatum, und eine Bewertung der Person entsteht nicht	Wissenssicherung und Nachfolgeplanung im Team, bevor jemand ausfällt
Wissen weitergeben ***(mit dem Zusatzmodul Wissensübergabe, seit 12.10.2026)***	Wer eine Kompetenz an wen weitergibt, die Kompetenz, die Zielstufe, eine Frist und eine Beschreibung, dazu der Stand (offen, vermittelt, angekommen) und wann die Zielstufe erreicht war. Ob sie erreicht ist, liest die Plattform aus den Kompetenzdaten; ein Häkchen von Hand gibt es nicht. Beide beteiligten Personen sehen den Vorgang und werden beim Anlegen benachrichtigt. Die Kennzahl „Zeit bis zur Weitergabe“ ist ein Median über Vorgänge und erscheint erst ab der Mindestgruppengröße, insgesamt wie je Kompetenz	Wissen im Team verteilen, bevor es fehlt
Kommunikationsdaten	Benachrichtigungen samt den Namen, die eine Meldung nennt (seit 20.09.2026 trägt jede Zeile dafür einen Verweis auf die benannten Personen, damit Auskunft und Löschung sie finden, ohne nach einem Namen zu suchen), Community-Beiträge, Kommentare, Push-Abos sowie die Mail-Anlässe, die die betroffene Person **selbst** in ihrem Profil abbestellt hat (Voreinstellung: keiner; abbestellbar sind nur Erinnerungen und Zusammenfassungen). Bei **Gästen einer Schulung** seit 18.09.2026 zusätzlich ihre Beiträge, Antworten, Reaktionen und Meldungen in der Diskussionsrunde dieser Schulung samt dem Namen, den sie dafür selbst bestätigt haben; sichtbar allein im Kreis der Schulung (Teilnehmende, Trainer:in, Verwaltung, Moderation), enthalten in der Selbstauskunft des Gasts und gelöscht mit seinen übrigen Gast-Daten	Zusammenarbeit; bei den Mail-Anlässen: Beachtung der Wahl, welche Mails die Person bekommt; bei Gästen: Praxistransfer nach einer Schulung
Schulungsunterlagen ***(nur mit Training)***	Dateien, die die Verwaltung zu einer Schulung hochlädt, etwa Handout oder **Fotoprotokoll**. Ein Fotoprotokoll kann **Abbildungen der Teilnehmenden** enthalten. Ausgeliefert wird eine Datei allein an den Kreis der Schulung, also an Teilnehmende einschließlich eingetragener Gäste, Trainer:in und Verwaltung, nie an die übrige Belegschaft und nie ins offene Netz; gelöscht wird sie mit der Unterlage oder der Schulung. Ob Fotos aufgenommen und so verteilt werden, klärt der Auftraggeber mit den Abgebildeten	Bereitstellung der Unterlagen an die Teilnehmenden, Praxistransfer
Eigene Dateien der Medien-Registry ***(nur mit Learning, seit 2.4)***	Videos, Tondateien und PDFs, die die Verwaltung als Lerninhalt hochlädt. Ein Schulungsvideo kann **Bild und Stimme von Beschäftigten** zeigen. Ausgeliefert wird eine Datei nur innerhalb der Plattform an Personen, die den Lernpfad sehen dürfen, einschließlich eingetragener Gäste dieses Pfads, nie über eine offene Adresse; gelöscht wird sie mit dem Inhalt, eine ersetzte Datei bleibt bis dahin als frühere Fassung im Verlauf. Gespeichert wird in der Ablage des Mandanten auf der Instanz, und umgewandelt wird nichts. An Dritte geht nichts, außer der Auftraggeber lässt zu einem Video ein **Transkript per KI** erstellen: Dann geht dessen Tonspur an den KI-Ablauf, den er selbst eingerichtet hat (Abschnitt „Zur KI-Funktion“ in Anlage 3). Ob Beschäftigte gefilmt und so gezeigt werden, klärt der Auftraggeber mit den Abgebildeten	Bereitstellung eigener Lerninhalte

Datenart	Beispiele	Zweck
Aufnahmen im Browser ***(nur mit Learning, seit 2.4)***	**Bild und Stimme** der aufnehmenden Person, dazu der Bildschirm oder das Fenster, das sie freigibt, und auf ihren Wunsch der Systemton. Gespeichert wird schon während der Aufnahme in Stücken in der Ablage des Mandanten auf der Instanz; nach dem Stopp setzt ffmpeg die Stücke ohne Neukodierung zusammen. An jeder Aufnahme steht, wann die Person der Übertragung an den Auftraggeber zugestimmt hat und unter welcher Fassung des Hinweises. Eine **übernommene** Aufnahme wird eine eigene Datei der Medien-Registry (Zeile darüber) und bleibt nach dem Austritt und einer Löschung der Person, denn sie ist dann Inhalt des Auftraggebers; abgebrochene und nie übernommene Aufnahmen werden nach 14 Tagen gelöscht, bei einer Löschung der Person sofort. Dazu die Bitten um eine Aufnahme mit Thema, Frist und Stand. Die Aufnahme ist freiwillig und kein Werkzeug zur Leistungskontrolle. Hat der Auftraggeber das **Transkript per KI** eingeschaltet (Abschnitt „Zur KI-Funktion“ in Anlage 3), kann er aus der Tonspur über seinen eigenen Ablauf ein Transkript und Untertitel erstellen lassen; der Hinweis vor der Aufnahme nennt das dann in einer eigenen Fassung, und wer zuvor nur der Grundfassung zugestimmt hat, bestätigt ihn vor der nächsten Aufnahme neu. Darüber hinaus geht an Dritte nichts	Wissen erfahrener Beschäftigter als Lerninhalt sichern
Protokolldaten	Audit-Log (wer hat wann was geändert), Server-Logs sowie die **Störungsaufzeichnung** des Betriebs: Zeitpunkt, Mandant, aufgerufener Pfad **ohne Abfrageteil**, Art des Fehlers samt Meldung, Fundstelle im Quelltext, Kennung der Anfrage und, sofern angemeldet, die Nummer der handelnden Person. **Kein Stacktrace, keine Eingaben, keine Suchbegriffe**; die Meldung ist auf 200 Zeichen gekappt und kann in seltenen Fällen einen Wert aus der gescheiterten Abfrage zitieren. Sie ist allein dem Betrieb zugänglich, umfasst die letzten 200 Vorfälle und wird von diesem verworfen, sobald die Störung abgearbeitet ist	Nachweisbarkeit, Fehlersuche, Erkennen einer Störung ohne Meldung des Kunden
Zustelldaten	Zustellprotokoll der ausgehenden E-Mails: Empfängeradresse, Anlass, Betreff, Zeitpunkt und Zustellstatus, bei einer angehaltenen Mail der Grund (etwa, dass die Person den Anlass abbestellt hat), **ohne Inhalt der Nachricht**	Auskunft über den Versand, Fehlersuche bei Zustellproblemen
Vertretungsdaten	vertretene Person, Vertretung, Zeitraum und ein **Anlass-Vermerk** wie „Urlaubsvertretung", **kein Krankheitsgrund**	Weiterleitung offener Entscheidungen und Bestätigungen während einer Abwesenheit
Projektteam-Daten ***(seit 02.10.2026)***	Zugehörigkeit zu einem Projektteam quer zur Linie, die **Leitung** des Teams, Zeitraum der Mitgliedschaft und ein optionaler **Anteil** in Prozent der eigenen Arbeitszeit. Gepflegt von der Verwaltung, der Leitung des Teams oder einem angebundenen Projektwerkzeug (factro, Public API); die betroffene Person wird bei jeder Aufnahme in der Plattform benachrichtigt. Namen, Linie und Leitung sehen die übrigen Mitglieder, den Anteil nur Leitung und Verwaltung. Ein Projektteam erteilt **kein Recht** und begründet **keine Führungslinie**	Zusammenarbeit über Teamgrenzen; Planung in einem Projektwerkzeug des Auftraggebers
Mentoring-Daten	Tandem (wer begleitet wen), Termine und Dauer der Sitzungen, gebuchte Sprechstunden. Private Notizen und Feedback der Beteiligten sind **nur für diese** sichtbar und stehen keiner Verwaltung offen	Durchführung der Begleitung, Nachweis geleisteter Stunden

Datenart	Beispiele	Zweck
Befragungsdaten	Bei einer **anonymen** Befragung: die Antworten **ohne jeden Personenbezug**, daneben getrennt der Vermerk, **dass** eine Person geantwortet hat, damit die Erinnerung endet. Zwischen beiden besteht keine Verbindung, auch nicht über den Zeitstempel, denn beide werden auf den Tag gerundet. Zur Abgabe wird die **Einordnung** festgehalten (Team, Abteilung, Führungskraft, Zugehörigkeit als Band, nie als Eintrittsdatum), soweit der Auftraggeber die jeweilige Aufteilung nicht abgeschaltet hat. Bei einer **namentlichen** Befragung tragen die Antworten die Person. Herausgegeben wird ausschließlich aggregiert und erst ab der Mindestgruppengröße; unterhalb davon erscheinen auch **keine Freitexte**	Standortbestimmung der Organisation, Entwicklung über die Zeit, Erkennen von Unterschieden zwischen Bereichen
Ankommens-Daten	Die **Checkliste** des Eintritts (Wortlaut der Punkte, gesetzt von der Personalabteilung, abgehakt allein von der betroffenen Person) und die **Wochenstimmung**: einer von drei Werten je Kalenderwoche, **ohne Freitext**, **freiwillig** und jederzeit änderbar. Die Stimmung erscheint allein im Cockpit der Führungskraft im eigenen Verwaltungs-Scope, nicht in der Personalverwaltung, in keinem Export und in keiner Auswertung; angezeigt wird höchstens die Vorwoche, und die Frage wird nur gestellt, solange eine Einarbeitung läuft	Begleitung des Eintritts; frühzeitiges Gespräch statt später Kündigung

Zusätzlich, **soweit Caltrix Staff gebucht ist**:

Datenart	Beispiele	Zweck
Vertragsdaten	Vertragsart, Wochenstunden, Arbeitszeitmuster, Befristung, Probezeit, Kündigungsfrist, Kostenstelle, Regelung zu Überstunden	Führung der Personalakte, Fristen, Nachweis nach dem NachwG
Berichtslinie	zugeordnete Führungskräfte (auch mehrere, etwa bei geteilter Leitung)	Antragsweg, Organigramm
Personal-Unterlagen	hochgeladene Dokumente mit Kategorie, Schutzstufe, Aufbewahrungsfrist und wahlweise Ablaufdatum; seit 04.10.2026 auch Aufenthaltstitel und Arbeitserlaubnis als vertrauliche Kategorie mit Pflicht zum Ablaufdatum	Personalakte; Erinnerung vor dem Ablauf eines Aufenthaltstitels an die Personalverwaltung und die Person
Antrags- und Vorgangsdaten	Urlaub, Homeoffice, Fortbildung, Stammdatenänderung samt Entscheidung und Begründung	Genehmigungsverfahren, Nachweis des Ablaufs
Abwesenheitsdaten	Zeitraum und Zeitanteil, **ohne Angabe eines Grundes**	Konfliktprüfung, Soll-Ist-Abgleich; seit 02.10.2026 auch ein **Hinweis an die Verantwortlichen eines betroffenen Termins** (Verwaltung der Schulung, Ausrichtende der Veranstaltung, die andere Seite eines Mentoring-Tandems), der Name, Termin und „abwesend gemeldet" nennt und nie einen Grund, sowie der Teilnahmestatus „entschuldigt" statt „nicht erschienen"

Datenart	Beispiele	Zweck
Abwesenheitsübersicht ***(nur mit Caltrix Staff, seit 02.10.2026)***	Zu jeder Abwesenheit ihre **Herkunft** (genehmigter Urlaubsantrag, genehmigter Bildungsurlaub, von Hand, Vorsystem), **kein Grund**. Daraus leitet die Übersicht, wo der Auftraggeber es einschaltet, eine **Art** ab (Urlaub, Bildung, sonst „abwesend"); Krankheit ist nie eine Art, auch wenn ein Vorsystem sie liefert. Je Person die **Reichweiten, in denen sie ihre Abwesenheit teilt** (eigenes Team, gemeinsame Projektteams, Abteilung, Unternehmen), als Einwilligung mit Audit, und eine Fassungsnummer ihrer Kalender-Abos. Sichtbar wird eine Abwesenheit nur nach der Einstellung des Auftraggebers je Reichweite (aus, freiwillig, für alle); unabhängig davon für die Führungskraft im eigenen Verwaltungs-Scope und für die Personalverwaltung, nie für eine Projektleitung allein wegen der Leitung. An Projektwerkzeuge des Auftraggebers gehen über die Public API nur Zeiträume ohne Art, die Feiertage und der Anteil im Projektteam, die vereinbarten Wochenstunden erst nach einem eigenen Schalter	Planung im Team, Vertretung, die Frage, ob jemand erreichbar ist; Kapazitätsplanung im Projektwerkzeug des Auftraggebers
Urlaubskonto	Anspruch, Übertrag, Verbrauch, Verfallshinweis	§ 7 BUrlG, Hinweisobliegenheit
Austrittsdaten	Beendigungsart, Zugang der Kündigung, Frist, Freistellung, Rückgabeliste	Abwicklung des Austritts
Zeugnisdaten	Zeugnisart, Beurteilungsstufen, Textbausteine, Freigabe	§ 109 GewO
Entgeltdaten ***(Staff)***	Grundentgelt und weitere Bestandteile (Zulage, Sonderzahlung, Bonus, Sachleistung) je mit Bezeichnung und Turnus, bei einer Einmalzahlung mit dem Tag der Auszahlung, Anlass, Gehaltsband, Herkunft (von Hand oder über den Konnektor); alle Beträge **feldverschlüsselt**	Personalakte, Nachweis nach § 2 Abs. 1 Nr. 7 NachwG
Personalakte als Abschrift ***(mit Pay, seit 12.10.2026)***	Führt der Auftraggeber die Personalakte in einem anderen System, verarbeitet Caltrix nur eine Abschrift: Person mit Personalnummer, Position, Team und Abteilung, Vertragsstand mit Wochenstunden, Entgelt samt Bestandteilen, Entgeltgruppe, Geschlecht und Ist-Entgelt, eingespielt per Datei, Schnittstelle oder Konnektor. Unterlagen, Abwesenheiten, Anträge, Austritt, Zeugnis und Nachweis werden in diesem Modus nicht erhoben; was aus einer früheren vollen Akte schon vorliegt, bleibt unverändert gespeichert und unterliegt seinen Löschfristen	Entgelttransparenz nach der Richtlinie (EU) 2023/970
Ist-Entgelt je Jahr ***(nur mit Pay)***	je Person und Kalenderjahr: Art (Grundentgelt oder Bestandteil), Bezeichnung, Betrag **feldverschlüsselt**, bezahlte Stunden; eingespielt aus dem Lohnjournal	Entgeltbericht nach Art. 9 der Richtlinie (EU) 2023/970, der auf das Ist eines Berichtsjahres rechnet
Geschlecht ***(nur mit Pay)***	weiblich / männlich / divers / keine Angabe; **zweckgebunden** allein für den Entgeltbericht und die daraus gerechnete Lückenanalyse	Art. 9 der Richtlinie (EU) 2023/970
Herausnahme aus dem Gehaltsvergleich ***(nur mit Pay, seit 29.10.2026)***	Grund aus einer festen Liste, Zeitraum und eine Begründung **feldverschlüsselt**; gesetzt von der Personalabteilung, ausgewiesen in den Auswertungen nur als Zahl je Grund	Entgeltbericht und Auskunft nach Art. 7 und 9 der Richtlinie (EU) 2023/970 ohne Personen, deren Entgelt sich nicht vergleichen lässt
Stellenbewertung ***(nur mit Pay)***	Kriterium, Stufe, Punktzahl, Gewicht und Gesamtsumme einer **Stelle**, dazu die vorgeschlagene und die bestätigte Vergleichsgruppe. **Keine Angabe über eine Person**: Bewertet wird die Tätigkeit, und die Tabellen tragen keine Personenspalte. In der Selbstauskunft erscheint die Bewertung der eigenen Stelle über die Stellenbezeichnung; gelöscht wird sie mit der Person nicht, denn die Stelle bleibt	Art. 4 Abs. 4 der Richtlinie (EU) 2023/970, § 87 Abs. 1 Nr. 10 BetrVG

Datenart	Beispiele	Zweck
Zeitdaten *(nur mit Time)*	Beginn, Ende, Dauer, Pausen, Kostenträger, Korrekturprotokoll	§ 16 Abs. 2 ArbZG, Zeitkonto
Bewerberdaten *(nur mit Hire)*	Name, Kontakt, Anschreiben, hochgeladene Unterlagen, Verfahrensstand, Absagevermerk, Talentpool-Einwilligung; seit 04.09.2026 zusätzlich die **Antworten auf je Stelle konfigurierte Formularfragen**, der **freiwillig angegebene Aufmerksamkeits-Kanal** (etwa „Jobbörse", allein für die Auswertung, welcher Kanal trägt), der **Bewertungsbogen** der am Verfahren Beteiligten (Einschätzung 1 bis 5 samt Begründung; in der Auskunft ohne die Namen der Verfassenden, Art. 15 Abs. 4 DSGVO) sowie die **angebotenen und gewählten Gesprächstermine**. Alles davon teilt die Löschfrist der Bewerbung	Auswahlverfahren, § 15 Abs. 4 AGG
Angabe zur Schwerbehinderung *(nur mit Hire, seit 01.10.2026)*	**freiwillige** Angabe der bewerbenden Person: schwerbehindert oder gleichgestellt, sonst nichts. Ein Gesundheitsdatum nach Art. 9 DSGVO. Sie steht an der Bewerbung und teilt deren Löschfrist, wird bei einer Einstellung nicht in die Personalakte übernommen, erscheint in keiner Liste, keinem Filter und keiner Auswertung, und die Meldungen an Schwerbehindertenvertretung und Betriebsrat tragen keinen Namen. Einsehen darf sie die Personalverwaltung der Stelle in der Vorgangsansicht und die Schwerbehindertenvertretung, diese nur solange das Verfahren läuft und mit Protokoll jeder Einsicht. Ebenso protokolliert wird die Unterrichtung, nie die Art der Angabe	Art. 9 Abs. 2 Buchst. b DSGVO, § 164 Abs. 1 Satz 4 und § 178 Abs. 2 SGB IX
Supportanfragen	Name und Adresse der anfragenden Person, Betreff und Text der Anfrage, Mandant, Zeitpunkt	Erbringung der vertraglichen Leistung. **Seit 01.09.2026 wird die Anfrage zusätzlich zur E-Mail als Aufgabe im Ticketsystem des Auftragnehmers angelegt**, damit sie nachverfolgbar bleibt; betrieben wird es von der Eid Hub GmbH als Unterauftragsverarbeiter (Anlage 3). Übermittelt wird, was zur Bearbeitung nötig ist, also Name und Adresse für die Antwort sowie der Text der Anfrage. Eine Rückkopplung findet nicht statt: Caltrix speichert nur die Kennung der Aufgabe. Der Auftraggeber wirkt daran mit, indem er keine besonderen Kategorien in den Freitext schreibt.

Besondere Kategorien nach Art. 9 DSGVO werden nicht planmäßig verarbeitet, auch mit Caltrix Staff nicht, mit **einer** benannten Ausnahme: der freiwilligen Angabe zur Schwerbehinderung in einer Bewerbung (Zeile oben), die das SGB IX voraussetzt, damit Schwerbehindertenvertretung und Betriebsrat unterrichtet werden können. Im Übrigen ist das eine Konstruktionsentscheidung und keine Zusicherung auf Zuruf: Die Plattform kennt **keine Krankmeldung**, eine Zeitzugabe an einem Quiz trägt **keinen Grund** (auch wenn sie auf einen deuten kann und deshalb als einzige Lerndatenart nach 24 Monaten fällt), die Abwesenheit hat **kein Feld für einen Grund**, der Anlass-Vermerk einer Vertretung sagt, wofür jemand einspringt, und nicht, warum jemand fehlt, und eine elektronische Arbeitsunfähigkeitsbescheinigung wird weder abgerufen noch gespeichert. Ein Entgelt ist keine besondere Kategorie. Der Auftraggeber stellt sicher, dass er keine solchen Daten in Freitextfelder einträgt; für Unterlagen mit Gesundheitsbezug steht die Schutzstufe „besonders geschützt" bereit, deren Einsicht eine eigene, nicht vererbbare Berechtigung verlangt und protokolliert wird.

Die Wochenstimmung, und warum sie keine Leistungskontrolle ist. Die Frage „wie läuft deine Woche" ist die persönlichste, die die Plattform stellt, und sie ist deshalb so schmal wie möglich gebaut: drei Werte, eine je Kalenderwoche, kein Freitext, keine Verlaufskurve innerhalb der Woche. Sie ist **freiwillig** und wird nicht angemahnt; eine fehlende Angabe wird nirgends als solche ausgewiesen, und es gibt keine Auswertung über Antwortquoten. Sie geht **allein** an die Führungskraft im eigenen Verwaltungs-Scope, nicht an die Personalabteilung, und sie erscheint in keinem Export, in keiner Analytik und in keinem Bericht. Damit ist sie keine Verhaltens- oder Leistungskontrolle im Sinne des § 87 Abs. 1 Nr. 6 BetrVG; ob der Auftraggeber sie gleichwohl mit seinem Betriebsrat abstimmt, bleibt seine Entscheidung als Verantwortlicher. Eine Angabe zur Gesundheit ist sie nicht: Sie sagt nichts über eine Ursache und lässt keinen Rückschluss auf eine Diagnose zu.

Die Abwesenheitsübersicht, und warum die Art keine Gesundheitsangabe werden darf. Eine Übersicht darüber, wer wann fehlt, ist eine Auswertung über Beschäftigte und kann eine technische Einrichtung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG sein. **Voreingestellt ist sie nur im eigenen Team eingeschaltet und dort ohne Art** (seit 03.10.2026): Wer zusammenarbeitet, sieht, wer abwesend ist, und nicht mehr. Abteilung, Projektteam und Unternehmen schaltet der Auftraggeber selbst ein. Auch das eigene Team kann er abschalten, etwa bis eine Vereinbarung mit dem Betriebsrat steht, und die Einstellung sagt das selbst. Die Art ist eine Ableitung aus der Herkunft und kein gespeicherter Grund; ihr Risiko ist die Restklasse: Erfasst ein Unternehmen Urlaub nur über den Antrag und alles andere von Hand, heißt „abwesend" dort „krank", und eine sichtbare Art wäre eine Angabe zur Gesundheit. Die Plattform zeigt die Art darum nur, wo der Auftraggeber sie je Reichweite einschaltet, warnt an der Einstellung davor und übernimmt die Art eines Vorsystems nie. **Ob die Restklasse beim Auftraggeber gemischt bleibt, kann nur er beurteilen, und ob er die Übersicht mit seinem Betriebsrat abstimmt, bleibt seine Entscheidung als Verantwortlicher.** Wer bei „freiwillig" nicht teilt, fehlt in der Übersicht ganz und erscheint auch nicht als „da". Ein Kalender-Abo ist an die Person gebunden, fragt bei jedem Abruf dieselbe Freigabe und lässt sich jederzeit durch Erneuern entwerten. Für die Übersicht selbst gibt es keine eigene Löschfrist, denn gespeichert wird außer Herkunft, Freigabe und Einstellung nichts; die Freigabe fällt mit der Löschung des Personenbezugs weg, und die Selbstauskunft nennt beides.

Wissen, das an einer Person hängt, und warum der Auftraggeber die Stufe wählt. Die Sicht ist eine stehende Auswertung über Beschäftigte und kann damit eine technische Einrichtung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG sein, auch wenn sie keine Leistung misst: Sie sagt, wo Wissen ungleich verteilt ist, und nichts darüber, wie gut jemand arbeitet. Deshalb entscheidet der Auftraggeber über die Stufe, und die Plattform sagt das an der Einstellung selbst. Die Stufe **ohne Namen** ist nicht anonym im Sinne des Erwägungsgrunds 26 DSGVO, denn die Führungskraft kennt ihr Team; sie hält aber die Mindestgruppengröße ein, und zwar gezählt im Kreis dessen, der die Liste ansieht, sodass eine Zeile nie auf eine Gruppe unter der Schwelle zeigt. Die Stufe **mit Namen** gehört nach unserer Einschätzung in eine Betriebsvereinbarung; die Plattform sorgt dafür, dass die betroffene Person davon weiß, verhindert die Stufe aber nicht. **Ob und wie der Auftraggeber die Sicht mit seinem Betriebsrat abstimmt, bleibt seine Entscheidung als Verantwortlicher.** Weil nichts davon gespeichert wird, gibt es für die Sicht keine eigene Löschfrist; die Selbstauskunft nennt die zugrunde liegenden Kompetenzdaten.

Wissen weitergeben ist Aufgabenverteilung. Ein Vorgang hält fest, dass eine Person einer anderen eine Kompetenz bis zu einer Stufe und einem Datum beibringt. Das ist eine Verteilung von Aufgaben und keine Leistungs- oder Verhaltenskontrolle: Es gibt keine Bewertung der beteiligten Personen, die Frist ist ein Ziel und kein Maßstab, und angekommen ist der Vorgang allein über die Kompetenzdaten, die ohnehin geführt werden. Eine aktive Mitbestimmung löst er nach unserer Einschätzung deshalb nicht aus. Beide Beteiligten sehen den Vorgang selbst, die tragende Person ist an der Vermittlung beteiligt und nicht ihr Gegenstand. Die einzige Auswertung, die Zeit bis zur Weitergabe, zählt Vorgänge und nicht Menschen und erscheint erst ab der Mindestgruppengröße. Der Vorgang wird mit der Löschung des Personenbezugs einer der beiden Beteiligten entfernt, denn ohne sie gibt es nichts mehr weiterzugeben, und die Selbstauskunft nennt ihn für beide.

Mitarbeitendenbefragungen, und was an ihnen anonym ist. Anonym heißt hier nicht, dass die Oberfläche keinen Namen anzeigt, sondern dass die Abgabe keinen Personenbezug trägt: kein Fremdschlüssel, kein Kennzeichen des Geräts, keine Sitzung. Getrennt davon steht der Vermerk, **dass** jemand geantwortet hat, denn sonst wüsste keine Erinnerung, wer noch fehlt. Zwischen beiden Beständen gibt es keine Spalte, und weil zwei Zeilen mit derselben

Sekunde über den Zeitstempel wieder zusammenzuführen wären, werden bei einer anonymen Befragung beide Seiten auf den Tag gerundet. Damit ist der Bezug nicht bloß verborgen, sondern nicht vorhanden (Erwägungsgrund 26 DSGVO), und genau deshalb nennt die Selbstauskunft die Teilnahme und nie die Antworten.

Für die **Auswertung nach Gruppen** wird zur Abgabe die Einordnung festgehalten, also Team, Abteilung, Führungskraft und die Zugehörigkeit als Band, und zwar **nur die Aufteilungen, die der Auftraggeber für die Befragung gewählt hat**. Er kann jede der vier je Befragung abschalten und für alle Befragungen zusammen ausschließen; eine abgeschaltete Aufteilung wird bei der Abgabe nicht gespeichert, und wer sie für alle Befragungen ausschließt, löscht damit auch die bereits festgehaltenen Werte. Herausgegeben wird daraus nur ein Ergebnis über mindestens so viele Abgaben, wie die Mindestgruppengröße verlangt; darunter erscheinen auch keine Freitexte, denn in einer Vierergruppe verrät ein Satz seinen Verfasser. Weil die Gruppen den Bestand vollständig aufteilen, fällt zusätzlich die kleinste sichtbare Gruppe weg, sobald genau eine unterdrückt wäre: Sonst ergäbe sie sich als Differenz zur Gesamtzahl. Stehen mehrere Aufteilungen nebeneinander, werden sie seit dem 20.10.2026 zusammen geprüft, denn eine Abteilung minus ihre sichtbaren Teams ergäbe sonst die verborgenen. Es fallen so lange weitere Gruppen weg, bis jede solche Differenz null ist oder mindestens die Mindestgruppengröße erreicht und mehr als eine verborgene Gruppe umfasst. Dieselbe Schwelle gilt für jede einzelne Frage, auch für eine freiwillige, und Freitexte erscheinen sortiert statt in der Reihenfolge der Abgabe.

Wer die Auswertung sieht, legt der Auftraggeber über die Rollenverwaltung fest. Das Recht, Befragungen zu verwalten, gilt nur für die ganze Organisation. Das Leserecht lässt sich auf ein Team oder eine Abteilung beschränken; dann rechnet die Auswertung nur über die Abgaben aus diesem Bereich, und die Mindestgruppengröße gilt für genau diese Abgaben. Im Bereich nennt sie keine Zahl der Eingeladenen, die Zahl der Antworten erst ab der Mindestgruppengröße und Inhalte erst, wenn die Welle geschlossen ist. Die Auswertung nach Führungskraft sieht nur, wer die Auswertung für die ganze Organisation liest, eine Führungskraft also auch nicht die Zahl über sich selbst. Eine Auswertung je Person gibt es nicht, auch nicht bei einer namentlichen Befragung.

Die Mindestgruppengröße setzt der Auftraggeber mit, aber nur nach oben. Seit dem 20.10.2026 kann er sie unter „Verwaltung › System › Datenschutz“ anheben, etwa auf die Zahl aus seiner Betriebsvereinbarung, höchstens auf 50. Unter die Vorgabe der Plattform lässt sie sich nicht senken, und es gibt sie nur einmal: für Befragungen, Onboarding-Analytik, die Sicht auf Wissen an einer Person, die Wissensübergabe, die Zeiterfassung von Führungskraft und Betriebsrat und die Hinweise an Paten gleichermaßen, eine Schwelle je Befragung oder je Auswertung gibt es nicht. Sie wirkt beim Lesen, also ab dem Speichern auch für vergangene Wellen und Auswertungen; gespeichert wird allein der eingestellte Wert, und jede Änderung steht mit altem und neuem Wert im Audit-Log. Einstellen kann sie nur, wer das Recht dazu für die ganze Organisation trägt; an einer Rolle für ein Team oder eine Abteilung wirkt es nicht. Für den Entgeltbericht gilt das Höhere aus diesem Wert und seiner eigenen Mindestgröße.

Der **Exit-Bogen** ist derselbe Mechanismus mit einer anderen Zielgruppe: Er geht an Beschäftigte, deren Austritt eingetragen ist, solange ihr Zugang besteht. Auch er ist freiwillig, auch er wird anonym erhoben, und auch aus ihm wird nichts unterhalb der Mindestgruppengröße herausgegeben. Das ist bei ihm die wichtigere Zusage als bei jedem anderen Bogen: In einem Quartal mit drei Austritten weiß jeder in der Firma, wer gemeint sein könnte, und deshalb schweigt die Auswertung dort ganz. Die Antwort bleibt nach dem Ausscheiden bestehen, denn sie trägt keinen Personenbezug mehr; die Einladung selbst fällt mit der Frist unten oder früher mit der Tilgung der Person.

Eine Befragung ist keine Verhaltens- oder Leistungskontrolle, denn sie misst nichts an einer Person und gibt über keine Person etwas aus. Sie berührt gleichwohl § 87 Abs. 1 Nr. 1 BetrVG, wo sie Fragen zur Ordnung des Betriebs stellt, und die Auswertung nach Führungskraft ist eine Aussage über Vorgesetzte. Wer sie nicht will, schaltet sie für alle Befragungen ab, und dann wird die Zuordnung zur Führungskraft weder gespeichert noch ausgegeben. **Ob und wie der Auftraggeber sie mit seinem Betriebsrat abstimmt, bleibt seine Entscheidung als Verantwortlicher**; die Plattform erzwingt hier anders als bei der Zeiterfassung keinen Freigabeweg, denn eine Befragung ist freiwillig und erhebt keine Daten über einzelne Beschäftigte.

Die Anwesenheit in einer Live-Übertragung. Die Plattform hält je Anmeldung zwei Zeitstempel fest, die erste Öffnung des Players und das letzte Lebenszeichen, und leitet daraus die Anwesenheit ab: Wer eine halbe Minute zusieht, gilt als anwesend, so wie er es beim Einlass an der Tür durch einen Scan wäre. Was daraus entsteht, ist ein **Ja oder Nein zur Teilnahme** und keine Aufmerksamkeitsmessung: Es wird keine Sehdauer ausgewertet, keine Kurve über die Sendung geführt und kein Verlassen und Wiederkommen gezählt. Der Moderation wird während der Sendung

allein die **Anzahl** der Zuschauer angezeigt, nie eine namentliche Liste derer, die gerade zusehen. Ein Lebenszeichen ist nach kurzer Zeit veraltet und damit ohne Aussage über eine Person; aufbewahrt wird es mit der Anmeldung und mit ihr gelöscht.

Downloads aus einer Live-Übertragung. Stellt die Moderation eine Datei bereit, etwa eine Vorlage am Ende der Sendung, hält die Plattform je Anmeldung einmal fest, dass sie heruntergeladen wurde, samt dem Zeitpunkt des ersten Abrufs. Der Moderation wird allein die **Anzahl** angezeigt, keine Liste der Personen, und ein wiederholter Abruf wird nicht gezählt. Der Vermerk wird mit der Anmeldung und mit der bereitgestellten Datei gelöscht.

Mentoring als Grenzfall, und wie er behandelt wird. Setzt der Auftraggeber das Mentoring für ein Angebot zur psychischen Gesundheit ein, etwa zur Burnout-Prävention, so ist zwar keine Diagnose gespeichert, doch die Teilnahme selbst kann einen Rückschluss auf die Gesundheit zulassen. Die Plattform hält dafür das Kennzeichen **vertraulich** bereit, das an der beratenden Person oder am einzelnen Termin gesetzt wird. Ist es gesetzt, erscheint die teilnehmende Person weder in der Aufsicht des Produkts noch im Export noch in der Team-Terminliste ihrer Führungskraft, die nur einen belegten Zeitraum ohne Titel sieht; die zugehörigen Audit-Einträge bleiben erhalten, sind aber gesondert markiert. Einsicht verlangt in beiden Fällen eine eigene, **nicht vererbbare** Berechtigung (`mentoring.confidential` beziehungsweise `audit.confidential`). Der Auftraggeber entscheidet als Verantwortlicher, wer sie erhält, und stellt sicher, dass die Bezeichnung eines Angebots keine Angaben zur Gesundheit einer bestimmten Person enthält.

Der Meldekanal nach dem Hinweisgeberschutzgesetz. Betreibt der Auftraggeber den internen Meldekanal (§ 12 HinSchG), so verarbeitet die Plattform dort Meldungen samt ihrem Verlauf. Gespeichert werden Gegenstand, Betreff, Meldetext, die Nachrichten zwischen Meldestelle und hinweisgebender Person sowie die Zeitpunkte von Eingang, Bestätigung, Rückmeldung und Abschluss. Betreff, Meldetext und Nachrichten liegen **feldverschlüsselt**.

Zur hinweisgebenden Person wird **nichts** gespeichert, was sie identifiziert: keine IP-Adresse, kein Gerätemerkmal, keine Sitzungskennung, und vor allem keine Verknüpfung zu einem Benutzerkonto, auch dann nicht, wenn sie zum Zeitpunkt der Meldung angemeldet ist. Der Meldevorgang trägt technisch **keinen Verweis** auf einen Personendatensatz. Nennt die hinweisgebende Person freiwillig ihren Namen, steht dieser verschlüsselt als Angabe **in** der Meldung und nicht als Verbindung zu einem Konto. Der Rückkanal ist ein Postfach, das über eine zufällige Vorgangsnummer und eine selbst gewählte Kennung geöffnet wird; von der Kennung wird allein ein Hash gespeichert, und sie lässt sich nicht zurücksetzen, weil dafür eine Kontaktangabe nötig wäre.

Einsicht hat allein die vom Auftraggeber benannte **Meldestelle**, erkennbar an der eigenen, **nicht vererbbaren** Berechtigung `whistleblower.office`. Die Personalverwaltung, die Führungskräfte und die Administration haben keinen Zugriff, auch nicht auf die Anzahl der Vorgänge; die Handlungen der Meldestelle werden als vertrauliche Audit-Einträge protokolliert, für die zusätzlich `audit.confidential` nötig ist. Der Auftraggeber kann die Meldestelle nach § 14 Abs. 1 HinSchG bei einem Dritten ansiedeln; diese Person erhält dann einen Zugang ohne Personalakte und ausschließlich diese Berechtigung.

Zur Auskunft nach Art. 15 DSGVO gilt hier eine Besonderheit, und sie ist gewollt: Meldevorgänge erscheinen **nicht** in „Meine Daten". Zur hinweisgebenden Person gibt es keine Verknüpfung, über die sie auffindbar wären, und ihr eigener Zugang zu ihren Angaben ist das Postfach. Zur in einer Meldung **benannten** Person wird ebenfalls keine Auskunft über den Bestand erteilt: Das Vertraulichkeitsgebot des § 8 HinSchG schützt die Identität der hinweisgebenden Person, und eine Auskunft, die den Vorgang offenlegt, ließe regelmäßig auf sie schließen. Der Auftraggeber entscheidet als Verantwortlicher über Auskunftsersuchen in diesem Bereich im Einzelfall und außerhalb der Plattform.

Aufbewahrung: Ein abgeschlossener Vorgang wird samt seinem Verlauf **drei Jahre nach Abschluss** gelöscht (§ 11 Abs. 5 HinSchG). Die Löschung läuft automatisch und **ohne Vorankündigung an die Administration**, denn schon die Zahl der anstehenden Löschungen wäre eine Aussage über den Bestand.

Art der Verarbeitung

Erheben, Erfassen, Organisieren, Speichern, Anpassen, Auslesen, Verwenden, Übermitteln (nur innerhalb der Instanz des Auftraggebers), Einschränken, Löschen und Vernichten, vollständig automatisiert über die Plattform.

Anlage 2: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Stand: 28.10.2026

1. Vertraulichkeit

Zutrittskontrolle. Die Server stehen in einem Rechenzentrum des Hosters in Deutschland (siehe Anlage 3). 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

Anlage 3: Unterauftragsverarbeiter

Welche der beiden Listen gilt, richtet sich nach dem Betrieb, den der Hauptvertrag festlegt. Im **geteilten Betrieb** läuft die Plattform für mehrere Kunden auf einer gemeinsamen Installation, jeder Kunde mit einer eigenen Datenbank. Bei einer **eigenen Instanz** läuft sie für einen einzigen Kunden auf einem eigenen, verwalteten Server.

Geteilter Betrieb

Name	Sitz	Leistung	Ort der Verarbeitung
Eid Hub GmbH (Muttergesellschaft des Auftragnehmers)	Am Steeg 4, 65239 Hochheim am Main	Bereitstellung der Hosting-Umgebung aus eigenem Vertrag mit dem Hoster; Ticketsystem des Auftragnehmers: je Supportanfrage ein Vorgang mit Betreff, Text, Name und Adresse der anfragenden Person und den Antworten, die Anhänge bleiben in der Plattform	Deutschland
ALL-INKL.COM, Neue Medien Münnich, als weiterer Unterauftragsverarbeiter der Eid Hub GmbH	Hauptstraße 68, 02742 Friedersdorf	Hosting der Plattform (Anwendung, Datenbank, Dateien, E-Mail-Versand) und des Ticketsystems	Deutschland

Zur Kette beim Hosting: Den Vertrag mit ALL-INKL.COM hält die Eid Hub GmbH, und sie stellt dem Auftragnehmer die Umgebung daraus bereit. Sie ist damit selbst Unterauftragsverarbeiter, und ALL-INKL.COM ist es eine Stufe weiter unten. Der Auftragnehmer gibt seine Pflichten aus diesem Vertrag an die Eid Hub GmbH weiter, und diese gibt sie an ALL-INKL.COM weiter (Art. 28 Abs. 4 DSGVO, § 6 Abs. 3).

Eigene Instanz

Name	Sitz	Leistung	Ort der Verarbeitung
Mittwald CM Service GmbH & Co. KG	Königsberger Straße 4-6, 32339 Espelkamp	Rechenzentrum und verwalteter Server der Instanz: Anwendung, Datenbank, Dateien, Sicherungen und der Mailserver, über den die Plattform ihre Mails versendet	Deutschland
Eid Hub GmbH (Muttergesellschaft des Auftragnehmers)	Am Steeg 4, 65239 Hochheim am Main	Ticketsystem des Auftragnehmers: je Supportanfrage ein Vorgang mit Betreff, Text, Name und Adresse der anfragenden Person und den Antworten; die Anhänge bleiben auf dem Server der Instanz	Deutschland
ALL-INKL.COM, Neue Medien Münnich, als weiterer Unterauftragsverarbeiter der Eid Hub GmbH	Hauptstraße 68, 02742 Friedersdorf	Hosting des Ticketsystems	Deutschland
Tutao GmbH je nach Vereinbarung	Deisterstr. 17a, 30449 Hannover	Postfach des Auftragnehmers für eine eigene Support-Adresse der Instanz: Mails an den Support, auch die Meldungen aus dem Supportformular der Plattform, mit Name und Adresse der anfragenden Person, Betreff, Text und Antworten	Deutschland

Name	Sitz	Leistung	Ort der Verarbeitung
ebuero AG je nach Vereinbarung	Hauptstraße 8, 10827 Berlin	Telefondienst, wenn eine Hotline vereinbart ist: Annahme von Anrufen in den Servicezeiten; Name, Rufnummer und Anliegen der anrufenden Person werden notiert und an den Auftragnehmer weitergeleitet. Zugriff auf die Plattform hat ebuero nicht	Deutschland; der Auftragnehmer beauftragt ebuero nur mit vertraglich zugesicherter Speicherung in Deutschland
TÜV Rheinland Akademie GmbH je nach Vereinbarung	Alboinstraße 56, 12103 Berlin	Kurse des Kurspakets, wenn es gebucht ist: Die SCORM-Pakete laden ihre Inhalte beim Start vom Server des Anbieters und melden dorthin den Lernstand, also Fortschritt, Ergebnis und Abschluss. Statt Name und Personalnummer übergibt die Plattform dabei ein Pseudonym	Deutschland (Bestätigung des Anbieters angefragt)

Die Einträge „je nach Vereinbarung“ gelten nur, wenn der Hauptvertrag die jeweilige Leistung vorsieht.

Zur Kette beim Ticketsystem: Die Eid Hub GmbH betreibt das Ticketsystem für den Auftragnehmer bei ALL-INKL.COM. Der Auftragnehmer gibt seine Pflichten aus diesem Vertrag an die Eid Hub GmbH weiter, und diese gibt sie an ALL-INKL.COM weiter (Art. 28 Abs. 4 DSGVO, § 6 Abs. 3).

Der Mailversand läuft bei einer eigenen Instanz über den Mailserver von mittwald, der zur Leistung in der ersten Zeile gehört. Einen weiteren Versanddienstleister setzt der Auftragnehmer nicht ein; die Mails gehen von dort unmittelbar an die Mailserver der Empfänger.

Für beide Fälle

Keine weiteren. Insbesondere werden **nicht** eingesetzt: externe Analyse- oder Tracking-Dienste, externe CAPTCHA-Dienste, Content Delivery Networks, externe KI-Anbieter, externe Videodienste.

Änderungen an dieser Liste kündigt der Auftragnehmer mindestens 30 Tage im Voraus in Textform an; der Auftraggeber kann innerhalb dieser Frist aus wichtigem Grund widersprechen (§ 6 Abs. 2).

Zur KI-Funktion: Die Plattform hält **keinen** eigenen Schlüssel für einen KI-Anbieter. Nutzt der Auftraggeber die KI-Funktionen, richtet er selbst einen Ablauf bei einem Anbieter seiner Wahl ein; die Plattform schickt die Anfrage signiert an die von ihm hinterlegte Adresse. Der dabei eingesetzte Anbieter ist damit **Unterauftragsverarbeiter des Auftraggebers**, nicht des Auftragnehmers, und von ihm selbst zu vertragen.

Fragen- und Schlagwort-Vorschläge übermitteln allein den Text eines Inhalts und keine personenbezogenen Daten. **Anders das Transkript per KI** (seit 2.4): Es übermittelt die Tonspur eines Videos oder einer Tondatei und damit die **Stimmen der Sprechenden**. Die Funktion hat einen eigenen Schalter, der ab Werk aus ist, und arbeitet nur über den Ablauf des Auftraggebers. Die Plattform trennt dafür allein die Tonspur des gezeigten Ausschnitts ab, stellt sie unter einer signierten, 24 Stunden gültigen Adresse bereit, vermerkt jeden Abruf im Audit-Log und löscht sie, sobald das Ergebnis zurück ist, die Anforderung endgültig scheitert, spätestens aber nach sieben Tagen. Transkript und Untertitel werden erst nach Prüfung durch einen Menschen am Inhalt gespeichert. Ob die Sprechenden in diese Übermittlung einbezogen werden dürfen, klärt der Auftraggeber mit ihnen, so wie die Aufnahme selbst. Bei einer Aufnahme im Browser nennt der Hinweis, dem die Person vor der Aufnahme zustimmt, das Transkript, solange der Schalter an ist; eine Aufnahme, deren Person nur dem Hinweis ohne diesen Absatz zugestimmt hat, wird nicht transkribiert. Wird der Schalter ausgeschaltet oder der Inhalt gelöscht, löscht die Plattform die Tonspuren offener Anforderungen sofort.

Zu Kalender- und HR-Anbindungen: Verbindet der Auftraggeber ein Fremdsystem (Microsoft 365, Personio, Workday, ein iPaaS-Werkzeug), verarbeitet dieses Daten in seinem Auftrag und auf seine Verantwortung. Das gilt auch für den SFTP-Server, von dem der Konnektor Dateien abholt: Er liegt in der Sphäre des Auftraggebers oder seines Lohnbüros und wird vom Auftraggeber bereitgestellt; der Auftragnehmer speichert die abgeholten Dateien nicht. Der Konnektor selbst läuft auf dem Server, auf dem auch die Instanz des Auftraggebers betrieben wird, und begründet keinen weiteren Unterauftragsverarbeiter.