Vertrag zur Auftragsverarbeitung für Caltrix Start

Fassung 2026-11-02, Entwurf. Die rechtliche Prüfung dieser Fassung steht noch aus.

Präambel

Zwischen

Auftraggeber (Verantwortlicher): dem Unternehmen, das sich zu Caltrix Start anmeldet, mit Firma, Anschrift und Vertretung aus der Anmeldung (nachfolgend „Auftraggeber“),

und

Auftragnehmer (Auftragsverarbeiter): der 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 nach Art. 28 DSGVO geschlossen. Er konkretisiert den Vertrag über Caltrix Start nach den Allgemeinen Geschäftsbedingungen für Caltrix Start (nachfolgend „Hauptvertrag“). Geschlossen wird er mit der Anmeldung im elektronischen Format (Art. 28 Abs. 9 DSGVO), und er gilt, sobald der Hauptvertrag zustande kommt. Der Auftragnehmer hält fest, welche Fassung der Auftraggeber angenommen hat und zu welchem Zeitpunkt.

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

---

§ 1 Gegenstand und Dauer

(1) Gegenstand. Der Auftragnehmer betreibt für den Auftraggeber die Plattform Caltrix im Umfang von Caltrix Start (Hauptvertrag, Ziffer 3) auf einer Installation, die sich mehrere Auftraggeber teilen, mit einer eigenen Datenbank je Auftraggeber. Die Verarbeitung umfasst das Speichern, Anzeigen, Auswerten und Löschen der in **Anlage 1** beschriebenen Daten zu den dort genannten Zwecken. Welche dieser Datenarten tatsächlich anfallen, hängt davon ab, welche Teile der Plattform der Auftraggeber nutzt und ob er Pay dazugebucht hat.

(2) Dauer. Die Laufzeit entspricht der des Hauptvertrags, die ersten beiden Wochen eingeschlossen. Der Vertrag endet mit dem Hauptvertrag, frühestens aber mit der vollständigen Rückgabe oder Löschung der Daten nach § 8.

---

§ 2 Art, Umfang und Zweck der Verarbeitung

Art, Umfang, Zweck, Datenarten und Kategorien betroffener Personen ergeben sich abschließend aus **Anlage 1**. Zu eigenen Zwecken verarbeitet der Auftragnehmer keine Daten des Auftraggebers. Insbesondere verwendet er sie **nicht** zum Training von KI-Modellen, zur Profilbildung über Auftraggeber hinweg oder für Vergleichswerte.

---

§ 3 Weisungsrecht

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

(2) Der Hauptvertrag, dieser Vertrag und die Einstellungen und Funktionen, die der Auftraggeber in der Plattform selbst nutzt, etwa eine Frist oder eine Löschung, sind dokumentierte Weisungen. Weitere Weisungen erteilt der Auftraggeber in Textform, etwa per E-Mail an kontakt@caltrix.de; mündliche Weisungen bestätigt er unverzüglich in Textform.

(3) Hält der Auftragnehmer eine Weisung für rechtswidrig, teilt er das 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 sinkt, und teilt wesentliche Änderungen dem Auftraggeber mit.

---

§ 5 Vertraulichkeit

Der Auftragnehmer setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet und mit den einschlägigen Vorschriften zum Datenschutz 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) Eine beabsichtigte Änderung teilt der Auftragnehmer dem Auftraggeber mindestens **30 Tage** im Voraus per E-Mail an die Adresse mit, die der Auftraggeber bei der Anmeldung angegeben oder später mitgeteilt hat. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem Grund widersprechen. Kommt keine Einigung zustande, kann er den Hauptvertrag ohne Frist zu dem Tag kündigen, an dem die Änderung wirksam würde.

(3) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter auf gleichwertige Pflichten zum Datenschutz.

(4) Nebenleistungen ohne Bezug zu den Daten des Auftraggebers, etwa Telekommunikation, Reinigung oder Wartung, sind keine Unterauftragsverhältnisse.

---

§ 7 Unterstützungspflichten

(1) Der Auftragnehmer unterstützt den Auftraggeber angemessen bei Anfragen betroffener Personen nach Art. 15 bis 21 DSGVO, bei Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 und 34 DSGVO und bei Datenschutz-Folgenabschätzungen nach Art. 35 und 36 DSGVO.

(2) Die Plattform stellt die Funktionen dafür bereit, sodass der Auftraggeber die meisten Anfragen **selbst und ohne Zutun des Auftragnehmers** beantworten kann (Anlage 2, Abschnitt 5). Unterstützung, die darüber hinausgeht, berechnet der Auftragnehmer zu den Sätzen der Support-Stunden (Hauptvertrag, Ziffer 5), es sei denn, der Anlass liegt in seinem Verantwortungsbereich.

(3) Eine Verletzung des Schutzes personenbezogener Daten meldet der Auftragnehmer dem Auftraggeber unverzüglich, spätestens **innerhalb von 24 Stunden**, nachdem er davon erfahren hat.

---

§ 8 Löschung und Rückgabe

(1) Export. Während der Laufzeit kann der Auftraggeber jederzeit in der Plattform selbst einen vollständigen Export in einem gängigen, maschinenlesbaren Format erstellen: jede Tabelle als JSON und CSV samt Beschreibung, dazu die abgelegten Dateien. Nach dem Ende des Hauptvertrags stellt der Auftragnehmer ihm diesen Export auf Anforderung bereit, und zwar **bis 30 Tage** nach dem Vertragsende.

(2) Löschung nach Vertragsende. Nach Ablauf dieser Frist löscht der Auftragnehmer die Daten **binnen weiterer 30 Tage**: zuerst die abgelegten Dateien des Auftraggebers (Unterlagen,

Belege, Anhänge, Videos), die in einem eigenen Ordner je Auftraggeber liegen, danach seine Datenbank, denn auch davon hat jeder Auftraggeber eine eigene. Die Löschung bestätigt der Auftragnehmer auf Wunsch in Textform.

(3) Sicherungen. Jeder Stand einer Sicherung wird höchstens **14 Tage** aufbewahrt (Anlage 2, Abschnitt 3). Gelöschte Daten verschwinden damit spätestens 14 Tage nach der Löschung auch aus den Sicherungen.

(4) Bei ausbleibender Zahlung. Stellt der Auftragnehmer den Mandanten nach dem Hauptvertrag (Ziffer 9) auf Nur-Lesen, verarbeitet er die Daten unverändert weiter und löscht deswegen nichts. Der Export nach Absatz 1 bleibt in dieser Zeit möglich. Gelöscht wird erst nach dem Ende des Hauptvertrags nach Absatz 1 bis 3.

(5) Gesetzliche Aufbewahrungspflichten bleiben unberührt.

(6) 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	6 Monate nach Abschluss des Verfahrens *(einstellbar)*	Absage oder Rückzug; der Lauf löscht Zeile **und** hochgeladene Datei
Talentpool	12 Monate *(einstellbar)*, jederzeit widerruflich	Einwilligung beim Eingang; der Widerruf holt die reguläre Frist zurück. Aufgenommen wird nur, wer selbst eingewilligt hat, und wessen Frist verstrichen ist, erscheint nicht mehr
Zeitaufzeichnungen	36 Monate *(einstellbar)*, **mindestens 24 Monate**	Der Lauf 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
Meldungen nach dem HinSchG	drei Jahre nach Abschluss	Löschung samt Verlauf, automatisch und ohne Vorankündigung an die Administration (§ 11 Abs. 5 HinSchG)

Datenart	Frist	Auslöser und Durchführung
Zustellprotokoll der E-Mails	6 Monate *(einstellbar)*	Zeitpunkt des Versands
Teilnahme an Befragungen	24 Monate nach dem Schließen einer Welle *(einstellbar)*	Die Person fällt aus der Zeile, die Zeile bleibt, denn sie trägt die Antwortquote der Welle. Die Antworten einer anonymen Befragung hängen an niemandem
Wochenstimmung	12 Monate *(einstellbar)*	Kalenderwoche der Angabe
Zwischenstände angefangener Eingaben	3 Monate *(einstellbar)*	Letztes Sichern; Abgabe und Speichern räumen sie ohnehin. Gespeichert wird verschlüsselt, was eine Person in einen laufenden Quizversuch, eine Reflexion oder eine Praxisaufgabe eingegeben und noch nicht abgeschickt hat
Quizversuche	unbegrenzt, bis der Auftraggeber eine Frist setzt *(einstellbar)*	Abgabe des Versuchs; der Lauf **anonymisiert**, Ergebnis und Antworten bleiben für die Bestehensquote
Zeitzugabe an Quizzen	24 Monate *(einstellbar, auch auf unbegrenzt)*	Letzte Verwendung; der Lauf **löscht** die Zugabe. Ein Grund wird nie gespeichert
Archiv der Aufbewahrung	**30 Tage**, nicht verkürzbar	Was der Lauf an Quizversuchen und Zeitzugaben anonymisiert oder löscht, liegt vorher verschlüsselt im Archiv und kann vom Auftraggeber zurückgeholt werden; danach löscht der Lauf es endgültig. Zurückholen und endgültige Löschung stehen im Audit-Log
Aufnahmen im Browser, nie übernommen	14 Tage	Abbruch oder fehlende Übernahme; bei einer Löschung der Person sofort
Ankommens-Checkliste	mit der Tilgung der Person	Sie hängt an der Person und fällt mit ihr
Supportanfragen	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. 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	mit der Tilgung der Person, sonst mit dem Projektteam	Die Mitgliedschaft samt Anteil wird gelöscht
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 Tabellen der einzelnen Module 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. Für das Rechenzentrum genügt der Nachweis über die Zertifizierung des Hosters nach ISO 27001 und dessen Vertrag zur Auftragsverarbeitung (Anlage 3).

(2) Der Auftraggeber darf sich nach Voranmeldung mit einer Frist von **14 Tagen** zu üblichen Geschäftszeiten von der Einhaltung überzeugen. Vor-Ort-Prüfungen finden höchstens einmal im Jahr statt, es sei denn, es gibt einen konkreten Anlass.

---

§ 10 Drittlandtransfer

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

---

§ 11 Schlussbestimmungen

(1) Änderungen dieses Vertrags bedürfen der Textform. Eine neue Fassung trägt eine eigene Fassungsnummer und gilt, sobald der Auftraggeber sie annimmt, etwa in der Anwendung; bis dahin gilt die Fassung, die er angenommen hat. Änderungen nach § 4 und § 6 bleiben davon unberührt.

(2) Widersprechen sich dieser Vertrag und der Hauptvertrag, gehen die Regelungen dieses Vertrags vor, soweit sie den Datenschutz betreffen.

(3) Ist eine Bestimmung unwirksam, bleiben die übrigen wirksam.

Anlage 1: Gegenstand der Verarbeitung

Zwecke

Personalverwaltung. 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, Betrieb des internen Meldekanals nach dem Hinweisgeberschutzgesetz und Erstellung des Exports an die Lohnabrechnung.

- **Arbeitszeit:** Aufzeichnung der Arbeitszeit einschließlich der Prüfung gegen die Grenzen des Arbeitszeitgesetzes und der Führung eines Zeitkontos.
- **Bewerbungen:** Ausschreibung von Stellen sowie Entgegennahme und Bearbeitung von Bewerbungen einschließlich der fristgebundenen Löschung.
- **Pay, soweit dazugebucht:** Angabe des Entgelts in der Ausschreibung, Auskunft über das Entgelt der Vergleichsgruppe nach der Richtlinie (EU) 2023/970, Einsicht der Person in ihr eigenes Entgelt und Gehaltsbänder.

Einarbeitung und Weitergabe. Einarbeitung neuer Beschäftigter über Lernpfade je Rolle mit Pate, Führungskraft und Frist, Zuweisung und Nachverfolgung von Lerninhalten, Wissensübergabe beim Austritt und die KI-Werkbank mit dem KI-Zugang des Auftraggebers.

Plattform. Organisation mit Abteilungen, Teams, Rollen und Rechten, Benachrichtigungen, Zusammenarbeit, Befragungen, Projektteams und Supportanfragen.

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 die Administration, Einladung oder Import
Administratoren des Auftraggebers	wie Beschäftigte
Freie Mitarbeitende	Anlage durch die Administration; Rahmenvertrag als Vertragsart
Bewerberinnen und Bewerber	eigene Eingabe über das Bewerbungsformular oder interne Bewerbung
Hinweisgebende Personen	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- und Nachname, E-Mail, Personalnummer, Eintritts- und Austrittsdatum. Die E-Mail kann fehlen; dann ist die Personalnummer der Schlüssel, und die Person meldet sich nicht an und bekommt keine Mail	Identifikation, Zeitanker der Lernpfade, Zählung nach dem Hauptvertrag
Organisationsdaten	Team, Abteilung, Position, Seniorität, Standort, Rolle im Team	Zuweisungsregeln, Sichtbarkeit, Auswertung
Zugangsdaten	Passwort-Hash, Zwei-Faktor-Geheimnis, Sitzungen, Anmeldeversuche	Anmeldung, Schutz vor Missbrauch
Anzeige-Vorlieben	die von der Person **selbst** im Profil gewählte Schriftgröße, „weniger Bewegung“ und „ruhigere Oberfläche“; die Administration kann sie weder setzen noch einsehen	Darstellung nach der Wahl der Person
Profilfoto	ein **freiwillig** von der Person selbst hochgeladenes Bild, gespeichert als zugeschnittene Fassung mit 256 Pixeln, ausgeliefert nur an angemeldete Personen desselben Auftraggebers; mit der Löschung der Person wird die Datei entfernt	Wiedererkennen in Listen und Gesprächen
Lerndaten	Zuweisungen, Fortschritt, Abschlüsse, Quiz-Ergebnisse, Abgaben, Reflexionen, eine Zeitzugabe an einem Quiz (Minuten und wer sie gewährt hat, nie ein Grund). Aus den Abschlüssen ein Hinweis „Andere in deiner Rolle haben das gemacht“, der nur die **Kopfzahl** nennt und erst oberhalb der Mindestgruppengröße erscheint. Führt der Auftraggeber ein eigenes Statusmodell, dazu je Teilnahme der Zustand samt Verlauf der Wechsel	Kern der Leistung, Orientierung der Belegschaft, Nachvollziehbarkeit des Bearbeitungsstands
Eigene Dateien der Medien-Registry	Videos, Tondateien und PDFs, die die Verwaltung als Lerninhalt hochlädt; ein Schulungsvideo kann **Bild und Stimme von Beschäftigten** zeigen. Ausgeliefert nur innerhalb der Plattform an Personen, die den Lernpfad sehen dürfen, gelöscht mit dem Inhalt	Bereitstellung eigener Lerninhalte
Aufnahmen im Browser	**Bild und Stimme** der aufnehmenden Person, der Bildschirm oder das Fenster, das sie freigibt, auf ihren Wunsch der Systemton, dazu Zeitpunkt und Fassung ihrer Zustimmung. Eine übernommene Aufnahme wird Inhalt des Auftraggebers; abgebrochene und nie übernommene Aufnahmen werden nach 14 Tagen gelöscht. Die Aufnahme ist freiwillig und kein Werkzeug zur Leistungskontrolle	Wissen erfahrener Beschäftigter als Lerninhalt sichern
Ankommens-Daten	die **Checkliste** des Eintritts, abgehakt allein von der Person, und die **Wochenstimmung**: einer von drei Werten je Kalenderwoche, ohne Freitext und freiwillig	Begleitung des Eintritts

Kompetenzdaten	Selbst- und Fremdeinschätzungen, Entwicklungsziele. Im Expertenverzeichnis erscheinen Name, Kompetenz und Stufe **nur nach Freischaltung durch die Person selbst**, jederzeit widerruflich	Entwicklungsplanung, Wissensaustausch im Unternehmen
Wissen weitergeben	wer eine Kompetenz an wen weitergibt, Kompetenz, Zielstufe, Frist, Beschreibung und Stand. Ob die Zielstufe erreicht ist, liest die Plattform aus den Kompetenzdaten. Die Kennzahl „Zeit bis zur Weitergabe“ ist ein Median über Vorgänge und erscheint erst ab der Mindestgruppengröße	Wissen weitergeben, bevor es fehlt, auch beim Austritt
Kommunikationsdaten	Benachrichtigungen samt den Namen, die eine Meldung nennt, Beiträge und Kommentare, Push-Abos und die Mail-Anlässe, die die Person selbst abbestellt hat	Zusammenarbeit, Beachtung der Wahl der Person
Supportanfragen	Betreff, Text, Klasse, Anhänge, Verlauf aus Rückfragen und Antworten, Bearbeitungsstand mit Zeitpunkten, Name und E-Mail der anfragenden Person. An den Support gehen per E-Mail und als Vorgang im Ticketsystem des Auftragnehmers Betreff, Text, Name, E-Mail und die Antworten, **nicht** die Anhänge	Bearbeitung von Störungen und Fragen
Protokolldaten	Audit-Log (wer hat wann was geändert), Server-Logs und die Störungsaufzeichnung des Betriebs: Zeitpunkt, Mandant, Pfad **ohne Abfrageteil**, Art und Fundstelle des Fehlers, Kennung der Anfrage und, wenn angemeldet, die Nummer der handelnden Person. **Kein Stacktrace, keine Eingaben**; die Meldung ist auf 200 Zeichen gekappt	Nachweisbarkeit, Fehlersuche
Zustelldaten	Empfängeradresse, Anlass, Betreff, Zeitpunkt und Status ausgehender E-Mails, **ohne Inhalt der Nachricht**	Auskunft über den Versand, Fehlersuche
Vertretungsdaten	vertretene Person, Vertretung, Zeitraum und ein Anlass-Vermerk wie „Urlaubsvertretung“, **kein Krankheitsgrund**	Weiterleitung offener Entscheidungen während einer Abwesenheit
Projektteam-Daten	Zugehörigkeit zu einem Projektteam quer zur Linie, Leitung, Zeitraum und ein optionaler Anteil der Arbeitszeit. Ein Projektteam erteilt **kein Recht** und begründet **keine Führungslinie**	Zusammenarbeit über Teamgrenzen

Befragungsdaten	bei einer **anonymen** Befragung die Antworten **ohne Personenbezug** und getrennt davon der Vermerk, **dass** jemand geantwortet hat, beide auf den Tag gerundet; zur Abgabe die Einordnung nach Team, Abteilung, Führungskraft und Zugehörigkeit als Band, soweit der Auftraggeber sie nicht abschaltet. Herausgegeben wird nur aggregiert und erst ab der Mindestgruppengröße	Standortbestimmung der Organisation
Meldungen nach dem HinSchG *(nur bei eingeschaltetem Meldekanal)*	Gegenstand, Betreff, Meldetext, Nachrichtenverlauf, Fristzeitpunkte; bei freiwilliger Namensnennung Name und Kontaktweg. Kein Verweis auf einen Personendatensatz, keine IP-Adresse, kein Gerätemerkmal. Betreff, Text und Nachrichten feldverschlüsselt	Erfüllung der Pflichten aus §§ 12, 16, 17 HinSchG
Vertragsdaten	Vertragsart, Wochenstunden, Arbeitszeitmuster, Befristung, Probezeit, Kündigungsfrist, Kostenstelle, Regelung zu Überstunden	Personalakte, Fristen, Nachweis nach dem NachwG
Berichtslinie	zugeordnete Führungskräfte, auch mehrere	Antragsweg, Organigramm
Personal-Unterlagen	hochgeladene Dokumente mit Kategorie, Schutzstufe, Aufbewahrungsfrist und wahlweise Ablaufdatum, auch Aufenthaltstitel und Arbeitserlaubnis als vertrauliche Kategorie	Personalakte, Erinnerung vor dem Ablauf eines Aufenthaltstitels
Antrags- und Vorgangsdaten	Urlaub, Homeoffice, Fortbildung, Stammdatenänderung samt Entscheidung und Begründung	Genehmigung, Nachweis des Ablaufs
Abwesenheitsdaten	Zeitraum, Zeitanteil und Herkunft (genehmigter Antrag oder von Hand), **ohne Angabe eines Grundes**	Prüfung auf Konflikte, Abgleich von Soll und Ist, Übersicht im Team
Urlaubskonto	Anspruch, Übertrag, Verbrauch, Hinweis auf den Verfall	§ 7 BUrlG, Hinweisobliegenheit
Austrittsdaten	Beendigungsart, Zugang der Kündigung, Frist, Freistellung, Rückgabeliste	Abwicklung des Austritts
Zeugnisdaten	Zeugnisart, Beurteilungsstufen, Textbausteine, Freigabe	§ 109 GewO
Entgeltdaten	Grundentgelt und weitere Bestandteile (Zulage, Sonderzahlung, Bonus, Sachleistung) mit Bezeichnung und Turnus, Anlass, Gehaltsband; alle Beträge **feldverschlüsselt**	Personalakte, Nachweis nach § 2 Abs. 1 Nr. 7 NachwG

Geschlecht *(nur mit Pay)*	weiblich, männlich, divers oder keine Angabe, **zweckgebunden** für die Entgeltauskunft	Art. 7 der Richtlinie (EU) 2023/970
Stellenbewertung *(nur mit Pay)*	Kriterium, Stufe, Punktzahl und Gewicht einer **Stelle** samt Vergleichsgruppe; **keine Angabe über eine Person**, denn bewertet wird die Tätigkeit	Art. 4 Abs. 4 der Richtlinie (EU) 2023/970, § 87 Abs. 1 Nr. 10 BetrVG
Herausnahme aus dem Gehaltsvergleich *(nur mit Pay)*	Grund aus einer festen Liste, Zeitraum und eine Begründung **feldverschlüsselt**	Auskunft ohne Personen, deren Entgelt sich nicht vergleichen lässt
Zeitdaten	Beginn, Ende, Dauer, Pausen, Kostenträger, Korrekturprotokoll	§ 16 Abs. 2 ArbZG, Zeitkonto
Bewerberdaten	Name, Kontakt, Anschreiben, Unterlagen, Verfahrensstand, Absagevermerk, Einwilligung in den Talentpool, Antworten auf Formularfragen je Stelle, freiwillig angegebener Kanal, Bewertungsbogen der Beteiligten (in der Auskunft ohne die Namen der Verfassenden), angebotene und gewählte Gesprächstermine	Auswahlverfahren, § 15 Abs. 4 AGG
Angabe zur Schwerbehinderung	**freiwillige** Angabe der bewerbenden Person, schwerbehindert oder gleichgestellt, sonst nichts. Sie teilt die Löschfrist der Bewerbung, wird bei einer Einstellung nicht übernommen und erscheint in keiner Liste und keiner Auswertung; jede Einsicht der Schwerbehindertenvertretung wird protokolliert	Art. 9 Abs. 2 Buchst. b DSGVO, § 164 Abs. 1 Satz 4 und § 178 Abs. 2 SGB IX

Besondere Kategorien nach Art. 9 DSGVO werden nicht planmäßig verarbeitet, mit **einer** benannten Ausnahme: der freiwilligen Angabe zur Schwerbehinderung in einer Bewerbung, die das SGB IX voraussetzt, damit Schwerbehindertenvertretung und Betriebsrat unterrichtet werden können. Im Übrigen ist das eine Entscheidung der Konstruktion: Die Plattform kennt in dieser Fassung **keine Krankmeldung**, eine Abwesenheit hat **kein Feld für einen Grund**, eine Zeitzugabe an einem Quiz trägt **keinen Grund**, und eine elektronische Arbeitsunfähigkeitsbescheinigung wird weder abgerufen noch gespeichert. 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 Abwesenheitsübersicht. 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 der Abwesenheit. Weitere Reichweiten und die Art schaltet der Auftraggeber selbst ein, und die Plattform übernimmt nie die Art eines Vorsystems. Krankheit ist nie eine Art. Ob er die Übersicht mit seinem Betriebsrat abstimmt,

bleibt seine Entscheidung als Verantwortlicher.

Die Wochenstimmung geht allein an die Führungskraft im eigenen Verwaltungsbereich, nicht an die Personalabteilung, und erscheint in keinem Export und keiner Auswertung. Sie ist freiwillig, eine fehlende Angabe wird nirgends ausgewiesen, und damit ist sie keine Verhaltens- oder Leistungskontrolle.

Befragungen messen nichts an einer Person und geben über keine Person etwas aus. Ob der Auftraggeber sie mit seinem Betriebsrat abstimmt, bleibt seine Entscheidung; die Auswertung nach Führungskraft lässt sich für alle Befragungen abschalten.

Der Meldekanal nach dem Hinweisgeberschutzgesetz. Zur hinweisgebenden Person wird **nichts** gespeichert, was sie identifiziert, auch keine Verknüpfung zu einem Konto, wenn sie bei der Meldung angemeldet ist. Der Rückkanal ist ein Postfach mit zufälliger Vorgangsnummer und selbst gewählter Kennung, von der allein ein Hash gespeichert wird. Einsicht hat allein die vom Auftraggeber benannte **Meldestelle** mit der eigenen, nicht vererbbaren Berechtigung `whistleblower.office`; die Personalverwaltung, die Führungskräfte und die Administration sehen weder die Vorgänge noch deren Anzahl. Meldevorgänge erscheinen nicht in „Meine Daten“, denn eine Auskunft, die den Vorgang offenlegt, ließe regelmäßig auf die hinweisgebende Person schließen (§ 8 HinSchG). Über Auskunftsersuchen in diesem Bereich entscheidet der Auftraggeber im Einzelfall und außerhalb der Plattform.

Art der Verarbeitung

Erheben, Erfassen, Organisieren, Speichern, Anpassen, Auslesen, Verwenden, Übermitteln (nur innerhalb der Instanz des Auftraggebers und an die in Anlage 3 genannten Stellen), Einschränken, Löschen und Vernichten, vollständig automatisiert über die Plattform.

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

Stand: 2026-11-02, für die gemeinsam genutzte Installation von Caltrix Start.

1. Vertraulichkeit

Zutrittskontrolle. Die Installation läuft auf einem Managed vServer des Hosters in einem Rechenzentrum in Deutschland (Anlage 3). Der Hoster ist für sein Unternehmen nach ISO 27001 zertifiziert und trägt die physische Sicherheit. Der Auftragnehmer selbst betreibt keine Serverräume.

Zugangskontrolle. Anmeldung mit E-Mail und Passwort, gespeichert als Hash nach dem aktuellen Standard des Frameworks (bcrypt oder argon2). Sperre nach wiederholten Fehlversuchen. Zwei-Faktor-Authentisierung (TOTP) steht jeder Person zur Verfügung; auf Weisung des Auftraggebers schaltet der Auftragnehmer sie für alle Konten oder für die Konten mit Verwaltungsrechten als Pflicht ein. Administrativer Zugang zum Server ausschließlich über SSH mit Schlüssel.

Zugriffskontrolle. Rollen- und rechtebasierte Steuerung mit Geltungsbereichen: Eine Rolle gilt für die ganze Organisation, für eine Abteilung samt Unterabteilungen oder für ein einzelnes Team. Die Berechtigungen sind im Code festgelegt, ihre Zuordnung zu Rollen stellt der Auftraggeber selbst ein.

Nicht vererbbare Berechtigungen. Die Rolle der Organisations-Administration nimmt zwei Schlüssel ausdrücklich **nicht** mit: die Einsicht in besonders geschützte Personal-Unterlagen und die Einsicht in Entgeltdaten samt Gehaltsbändern 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. So öffnet die Administration einer Plattform nicht nebenbei die Gehaltsliste des Unternehmens.

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, Zwei-Faktor-Geheimnisse, die Inhalte des Meldekanals und 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 lassen sich per Datei einspielen. Die hochgeladene Datei wird nach dem Lesen gelöscht, die temporäre Datei des Uploads eingeschlossen. Zwischen Prüfen und Übernehmen liegt der geprüfte Stand verschlüsselt in der Sitzung und verfällt nach 30 Minuten, beim Übernehmen oder Verwerfen sofort. Das Audit-Log nennt die Zahl der Zeilen und nie einen Betrag.

Trennungskontrolle. Eine eigene Datenbank je Auftraggeber, auch auf der gemeinsam genutzten Installation. Die Trennung ist damit keine Filterbedingung in einer Abfrage, sondern eine Grenze der Verbindung: Ein Programmierfehler in einer Abfrage kann keine Daten eines anderen Auftraggebers zutage fördern, weil sie nicht in derselben Datenbank liegen. Die abgelegten Dateien liegen in einem eigenen Ordner je Auftraggeber. Die Zuordnung von Adresse zu Mandant steht in einer zentralen Registry, deren Zugangsdaten verschlüsselt abgelegt sind.

Pseudonymisierung und Löschung. Nach dem Austritt einer Person werden ihre Stammdaten und persönlichen Inhalte nach einer einstellbaren Frist (Standard: 24 Monate) anonymisiert. Abschlussnachweise bleiben in anonymisierter Form erhalten.

2. Integrität

Weitergabekontrolle. Transport ausschließlich über TLS, HTTPS wird erzwungen. Ausgehende Aufrufe an Adressen, die der Auftraggeber hinterlegt (Link-Prüfung, KI-Webhook, OIDC-Discovery), laufen über eine zentrale Prüfung, die nur öffentlich erreichbare Ziele zulässt (Schutz vor SSRF). 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 wann was geändert hat. Der Auftraggeber sieht und filtert es in der Oberfläche.

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. Jede Datei, die eine Anfrage mitbringt, wird geprüft, bevor sie abgelegt oder gelesen wird. 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. Jede abgewiesene Datei steht mit Name, Größe, Grund und Herkunft im Audit-Log.

Schutz öffentlicher Formulare. Formulare ohne Anmeldung, etwa die Bewerbung, 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.

3. Verfügbarkeit und Belastbarkeit

Sicherungskonzept. Der Hoster sichert die Installation täglich, Datenbanken wie abgelegte Dateien, in seinen Rechenzentren in Deutschland. Zusätzlich sichert die Anwendung täglich die zentrale Datenbank **und jede einzelne Mandanten-Datenbank**, komprimiert und mit Prüfsummen-Manifest. Jeder Stand einer Sicherung wird **höchstens 14 Tage** aufbewahrt und danach überschrieben; eine Löschung ist damit spätestens nach 14 Tagen auch aus den Sicherungen verschwunden. Die in Abschnitt 1 genannten Felder liegen auch in den Sicherungen verschlüsselt, und der Anwendungsschlüssel wird getrennt von den Sicherungen verwahrt.

Wiederherstellung. Ein dokumentierter Ablauf zur Wiederherstellung steht in der Betriebsdokumentation. Wird eine Sicherung zurückgespielt, wiederholt der Auftragnehmer die

Löschungen, die seit ihrem Stand ausgelöst wurden.

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

4. Verfahren zur regelmäßigen Überprüfung

- Automatisierte Tests; kein Stand wird ohne grüne Tests ausgeliefert.
- Eine Betriebs-Checkliste als Befehl (`ops:preflight`) prüft den laufenden Zustand statt einer Liste im Kopf.
- Last- und Leistungsprüfung der Hauptseiten (`ops:smoke`) vor jeder größeren Auslieferung.
- Sicherheits-Durchgänge nach der Systematik von OWASP; Ergebnisse und die daraus bindenden Regeln sind in der Spezifikation der Plattform 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 Administration. Die Auskunft folgt dem **Bestand** und nicht der Buchung: Was gespeichert ist, wird beauskunftet. Unterlagen werden mit Kategorie, Name, Datum und Aufbewahrungsfrist **benannt**; Angaben über Dritte bleiben nach Art. 15 Abs. 4 draußen
Auskunft ohne eigenen Zugang	Wer keinen Zugang hat, etwa Bewerberinnen und Bewerber von außen, erreicht die Seite nicht. Für sie beantwortet der Auftraggeber die Anfrage auf dem üblichen Weg; die Plattform liefert die Angaben dafür aus Personal- und Bewerbungsakte
Berichtigung (Art. 16)	Profildaten ändert die Person selbst, Stammdaten die Administration
Löschung (Art. 17)	Anonymisierung mit dem Ablauf der Aufbewahrungsfrist nach dem Austritt oder auf Weisung sofort. **Die Löschung deckt denselben Umfang wie die Auskunft**, 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); ihr Freitext fällt
Datenübertragbarkeit (Art. 20)	Export in maschinenlesbarem Format
Widerspruch (Art. 21)	Freiwillige Funktionen, etwa Push-Benachrichtigungen oder der Eintrag im Expertenverzeichnis, laufen über eine ausdrückliche, jederzeit widerrufbare Einwilligung

---

Anlage 3: Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
Mittwald CM Service GmbH & Co. KG, Königsberger Straße 4–6, 32339 Espelkamp	Hosting der gemeinsam genutzten Installation von Caltrix Start auf einem Managed vServer: Anwendung, Datenbanken, abgelegte Dateien und deren tägliche Sicherung	Deutschland
Eid Hub GmbH, Am Steeg 4, 65239 Hochheim am Main (Muttergesellschaft des Auftragnehmers)	Bereitstellung des E-Mail-Versands und des Ticketsystems für Supportanfragen aus eigenem Vertrag mit dem Hoster	Deutschland
ALL-INKL.COM – Neue Medien Münnich, Friedrich-Ebert-Str. 12, 02826 Görlitz, als weiterer Unterauftragsverarbeiter der Eid Hub GmbH	Hosting von E-Mail-Versand und Ticketsystem	Deutschland

Zur Kette bei E-Mail und Ticketsystem: Den Vertrag mit ALL-INKL.COM hält die Eid Hub GmbH und stellt dem Auftragnehmer die Dienste 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).

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

Zur KI-Werkbank: 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, etwa über n8n oder Make, und die Plattform schickt die Anfrage signiert an die Adresse, die er hinterlegt. Der dabei eingesetzte Anbieter ist **Unterauftragsverarbeiter des Auftraggebers** und nicht des Auftragnehmers, und der Auftraggeber schließt den Vertrag mit ihm selbst. Fragen- und Schlagwort-Vorschläge übermitteln allein den Text eines Inhalts. Das Transkript per KI übermittelt dagegen die Tonspur eines Videos und damit die **Stimmen der Sprechenden**; es hat einen eigenen Schalter, der ab Werk aus ist, und die Plattform löscht die bereitgestellte Tonspur, sobald das Ergebnis zurück ist, spätestens nach sieben Tagen.

Zu weiteren Anbindungen: Verbindet der Auftraggeber ein Fremdsystem, etwa einen Kalender über ein Abo, verarbeitet dieses Daten in seinem Auftrag und auf seine Verantwortung.