Auftragsverarbeitungsvertrag für den geteilten SaaS-Betrieb von Skillent

Dieser Vertrag wird bei der Registrierung eines Betriebsmandanten einbezogen und gilt zwischen

SoftwareGenie24 UG (haftungsbeschränkt), Mauernstraße 33, 38100 Braunschweig, Amtsgericht Braunschweig HRB 211248, vertreten durch den Geschäftsführer Julien Giesemann — nachfolgend **Auftragsverarbeiter** —

und dem bei der Registrierung angegebenen Betrieb — nachfolgend **Verantwortlicher**.

Kontakt für Weisungen, Datenschutzanfragen und Vertragsfragen: support@softwaregenie24.de. Kontakt für Sicherheitsmeldungen: security@softwaregenie24.de.

§ 1 Gegenstand, Rollen und Geltung

1. Der Auftragsverarbeiter betreibt Skillent als geteilte Installation unter einer gemeinsamen Adresse. Jeder Betrieb arbeitet darin in einem eigenen Mandanten. Der Verantwortliche nutzt diesen Mandanten für die Verwaltung seiner Berufsausbildung.
2. Soweit der Auftragsverarbeiter dabei personenbezogene Daten verarbeitet, die der Verantwortliche oder dessen Benutzer in den Mandanten einstellen, handelt er als Auftragsverarbeiter nach Art. 28 DSGVO. Dieser Vertrag regelt diese Verarbeitung.
3. Nicht von diesem Vertrag erfasst sind:
    - die Daten, die der Auftragsverarbeiter zur Begründung und Abwicklung des Nutzungsverhältnisses selbst benötigt, insbesondere die bestätigte Kontaktadresse der registrierenden Person, Tarif, Verbrauch und Abrechnungsdaten. Dafür ist der Auftragsverarbeiter eigener Verantwortlicher; die Verarbeitung ist in seiner Datenschutzerklärung beschrieben;
    - die Mandanten von Auszubildenden ohne Betrieb. Für sie gibt es keinen Verantwortlichen auf Kundenseite; der Auftragsverarbeiter ist dort selbst Verantwortlicher, und die Verarbeitung ist in seiner Datenschutzerklärung beschrieben;
    - der Self-Hosted-Betrieb und das Managed Hosting von Skillent. Dafür gilt die gesonderte Auftragsverarbeitungsvereinbarung von SoftwareGenie24.
4. Grundlage des Nutzungsverhältnisses sind die Nutzungsbedingungen für die geteilte Installation. Bei Widersprüchen zu Datenschutzfragen hat dieser Vertrag Vorrang. Wird später eine unterzeichnete Auftragsverarbeitungsvereinbarung über denselben Gegenstand geschlossen, tritt sie an die Stelle dieses Vertrags.

§ 2 Weisungsgebundenheit

1. Der Auftragsverarbeiter verarbeitet die Daten ausschließlich zu den in Anlage 1 genannten Zwecken und nach den Weisungen des Verantwortlichen.
2. Die Einstellungen, die der Verantwortliche in seinem Mandanten vornimmt, und die Nutzung der bereitgestellten Funktionen sind Weisungen. Weitere Weisungen erteilt der Verantwortliche in Textform über die oben genannte Kontaktadresse. Weisungsberechtigt sind die Personen, die der Verantwortliche in seinem Mandanten als Organisationsadministrator geführt oder dem Auftragsverarbeiter benannt hat.
3. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies mit und darf ihre Ausführung aussetzen, bis der Verantwortliche sie bestätigt oder ändert. Eine Weisung, deren Ausführung gegen die Datenschutz-Grundverordnung oder andere Datenschutzvorschriften verstößt, führt er auch nach einer Bestätigung nicht aus.

4. Eine Weisung, die die Trennung der übrigen Mandanten aufheben, den Betrieb der geteilten Installation beeinträchtigen oder Daten anderer Verantwortlicher betreffen würde, kann der Auftragsverarbeiter nicht ausführen. Er teilt dies mit und benennt, soweit möglich, einen anderen Weg.
5. Verarbeitungen, zu denen den Auftragsverarbeiter das Unionsrecht oder das Recht eines Mitgliedstaats verpflichtet, bleiben zulässig. Er unterrichtet den Verantwortlichen vorher über die rechtliche Anforderung, sofern das Recht dies nicht verbietet.

§ 3 Art, Umfang, Zweck und Dauer

1. Art, Umfang und Zweck der Verarbeitung, die Datenarten, die Kategorien betroffener Personen und der Verarbeitungsort ergeben sich aus Anlage 1.
2. Der Vertrag beginnt mit der Bestätigung der Registrierung. Er gilt bis zur vollständigen Erfüllung der Rückgabe- und Löschpflichten nach § 12. Seine Schutzpflichten gelten auch für Daten und Sicherungskopien fort, die nach der Beendigung des Mandanten noch aufbewahrt werden.
3. Der Verantwortliche kann den Mandanten jederzeit beenden. Die Folgen regelt § 12.

§ 4 Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung, die Rechtsgrundlage und die Information der betroffenen Personen verantwortlich. Dazu gehört die Information der Auszubildenden und der übrigen Benutzer über die Verarbeitung in seinem Mandanten.
2. Der Verantwortliche vergibt die Rollen und Berechtigungen in seinem Mandanten selbst, hält sie aktuell und entzieht sie bei Wegfall des Bedarfs.
3. Zu den im Auftrag verarbeiteten Angaben gehören Gesundheitsdaten in dem in Anlage 1 beschriebenen, begrenzten Umfang, insbesondere die Abwesenheitsart „krank“ mit ihrem Zeitraum, die daraus gebildeten Kontingente und Kennzahlen, die Anwesenheitsangabe „krank“ in den Einträgen des Berichtshefts und, bei eingeschaltetem Modul, die Daten der Untersuchungen nach dem Jugendarbeitsschutzgesetz. Diagnosen, ärztliche Befunde und Arbeitsunfähigkeitsbescheinigungen sind nicht als Eingabefeld und nicht als vorgesehener Upload Bestandteil des Dienstes. Der Verantwortliche prüft für die von ihm veranlasste Verarbeitung die erforderlichen Rechtsgrundlagen einschließlich Art. 9 DSGVO und § 26 Abs. 3 BDSG. Weitere besondere Kategorien sind nicht Zweck der Verarbeitung; der Verantwortliche weist seine Benutzer darauf hin, solche Angaben nicht in die vorhandenen Freitextfelder einzutragen, und begrenzt sie auf das Erforderliche.
4. Werden Daten von Minderjährigen verarbeitet, trifft der Verantwortliche die dafür erforderlichen Festlegungen; das gilt auch für die Angaben zum Jugendarbeitsschutz.
5. Setzt der Verantwortliche Beurteilungen, Noten oder das Feedback aus mehreren Perspektiven ein, prüft er selbst die dafür geltenden Anforderungen, insbesondere die Erforderlichkeit, die Information der betroffenen Personen und etwaige Beteiligungsrechte der Arbeitnehmervertretung.
6. Der Verantwortliche sichert die Zugangsdaten seiner Benutzer gegen unbefugte Nutzung und meldet den Verlust eines administrativen Zugangs unverzüglich.
7. Der Verantwortliche ist für die Sicherung der von ihm benötigten Daten mitverantwortlich, soweit ihm die Exportfunktionen zur Verfügung stehen.

§ 5 Technische und organisatorische Maßnahmen

1. Der Auftragsverarbeiter setzt die in Anlage 2 beschriebenen Maßnahmen nach Art. 32 DSGVO um und hält sie während der Vertragslaufzeit aufrecht.

2. Er darf die Maßnahmen fortentwickeln, solange das vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen teilt er in Textform mit.
3. Die geteilte Installation wird für alle Mandanten einheitlich betrieben. Kundenspezifische Abweichungen von Anlage 2 sind in diesem Betriebsmodell nicht möglich; sie setzen Self-Hosted oder Managed Hosting voraus.

§ 6 Vertraulichkeit

1. Der Auftragsverarbeiter setzt für die Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet und über die einschlägigen Datenschutzpflichten unterrichtet sind. Die Verpflichtung gilt über das Ende der Tätigkeit hinaus.
2. Der Zugriff wird auf die Personen begrenzt, die ihn für die beauftragte Leistung benötigen.

§ 7 Unterauftragsverarbeiter

1. Der Verantwortliche genehmigt den Einsatz der in Anlage 3 genannten Unterauftragsverarbeiter.
2. Vor dem Einsatz eines neuen oder ausgetauschten Unterauftragsverarbeiters unterrichtet der Auftragsverarbeiter den Verantwortlichen mindestens vier Wochen vorher in Textform unter Angabe von Unternehmen, Leistung und Verarbeitungsort.
3. Der Verantwortliche kann innerhalb von zwei Wochen nach der Unterrichtung aus nachvollziehbaren datenschutzrechtlichen Gründen widersprechen. Bei einem fristgerechten Widerspruch wird der neue Unterauftragsverarbeiter für die Daten dieses Verantwortlichen bis zur Klärung nicht eingesetzt. Die Parteien suchen eine geeignete Alternative. Ist sie nicht möglich, kann der Verantwortliche den Mandanten mit Wirkung zum geplanten Wechsel beenden; die Exportfrist nach § 12 bleibt ihm erhalten und wird ohne Einsatz des beanstandeten Unternehmens erfüllt.
4. Der Auftragsverarbeiter bindet Unterauftragsverarbeiter vertraglich mit Pflichten ein, die den Pflichten dieses Vertrags entsprechen, und gibt diese Pflichten auf jeder weiteren Stufe der Verarbeitungskette weiter. Für die Erfüllung bleibt er dem Verantwortlichen gegenüber verantwortlich.
5. Eine Verarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums findet nicht statt.

§ 8 Unterstützung des Verantwortlichen

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Beantwortung von Anträgen betroffener Personen. Der Verantwortliche kann Auskunft, Export, Berichtigung und Löschung im Regelfall selbst in seinem Mandanten vornehmen; dafür stehen ihm die Funktionen der Anwendung zur Verfügung.
2. Wendet sich eine betroffene Person mit einem Antrag, der den Mandanten des Verantwortlichen betrifft, an den Auftragsverarbeiter, leitet dieser den Antrag weiter und beantwortet ihn nicht selbst.
3. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO, insbesondere mit den Angaben, die für eine Datenschutz-Folgenabschätzung oder eine vorherige Konsultation zum Betrieb der geteilten Installation erforderlich sind.

§ 9 Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die dessen Mandanten betrifft, unverzüglich nach Bekanntwerden an die im Mandanten hinterlegte Kontaktadresse.
2. Die Meldung enthält, soweit bekannt, eine Beschreibung des Vorfalls, die betroffenen Datenarten und Personengruppen, den Zeitraum, die wahrscheinlichen Folgen und die getroffenen oder

vorgeschlagenen Maßnahmen. Fehlende Angaben werden nachgereicht.

3. Betrifft ein Vorfall die geteilte Installation als Ganzes, unterrichtet der Auftragsverarbeiter alle betroffenen Verantwortlichen. Angaben zu anderen Mandanten enthält die Meldung nicht.
4. Die Bewertung der Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO obliegt dem Verantwortlichen.

§ 10 Nachweise und Kontrollen

1. Der Auftragsverarbeiter weist die Einhaltung seiner Pflichten durch Auskünfte, die vorliegenden Dokumente zu den technischen und organisatorischen Maßnahmen, die Angaben zur Verarbeitungskette sowie durch Prüf- und Betriebsnachweise nach, soweit sie vorhanden und für die beauftragte Leistung einschlägig sind.
2. Der Auftragsverarbeiter ermöglicht und unterstützt die zur Kontrolle der beauftragten Verarbeitung erforderlichen Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten, zur Vertraulichkeit verpflichteten Prüfer. Vorrangig werden Auskünfte, Unterlagen und Fernprüfungen genutzt, soweit sie den konkreten Prüfzweck erfüllen. Ist eine weitergehende Prüfung erforderlich, werden Umfang, Zeitpunkt und sichere Durchführung abgestimmt.
3. Prüfungen werden mit angemessener Vorlaufzeit abgestimmt und auf das Erforderliche begrenzt. Daten anderer Verantwortlicher und Betriebsgeheimnisse werden dabei durch geeignete Maßnahmen geschützt, etwa durch begleitete Einsicht, geschwärzte Unterlagen oder Prüfungen an Testdaten; der erforderliche Nachweis darf dadurch nicht vereitelt werden. Bei einem Sicherheitsvorfall, einem begründeten Verdacht auf einen erheblichen Verstoß oder einer behördlichen Anforderung wird eine erforderliche kurzfristige Prüfung ermöglicht. Der Auftragsverarbeiter betreibt im Rechenzentrum keine eigenen Räume; die erforderlichen Nachweise zur Infrastruktur stellt er über die vertragliche Verarbeitungskette zur Verfügung. Befugnisse von Aufsichtsbehörden bleiben unberührt.
4. Eine Zertifizierung des Dienstes oder ein externer Prüfbericht liegt nicht vor. Der Auftragsverarbeiter legt solche Nachweise nur vor, wenn sie tatsächlich vorhanden sind.

§ 11 Supportzugriff des Auftragsverarbeiters

1. Der Auftragsverarbeiter greift nicht auf die Inhalte des Mandanten zu, um ihn zu unterstützen, solange der Organisationsadministrator des Mandanten den Zugriff nicht freigegeben hat. Die Freigabe ist befristet und widerruflich; Erteilung, Nutzung, Ablauf und Widerruf stehen mit Person und Zeitpunkt im Auditprotokoll des Mandanten. Die Freigabe ist die Weisung für diesen Zugriff; sie wird in der Anwendung erteilt und gilt nach Wahl des Administrators für 24 Stunden, drei oder sieben Tage.
2. Die Freigabe öffnet den Mandanten für die lesende Einsicht in nahezu alle Bereiche, so wie sie ein Administrator des Mandanten hat, einschließlich der Inhalte des Berichtshefts, der Bewertungen und der hochgeladenen Dateien. Verändern kann der Auftragsverarbeiter dabei nichts; die Anwendung lässt nur lesende Zugriffe zu. Auch lesend ausgenommen sind die Freigabe selbst, Export und Beendigung des Mandanten, Auskunfts- und Löschvorgänge sowie die Verwaltung der Schnittstellenschlüssel. Der Verantwortliche erteilt die Freigabe deshalb nur für den Zweck und die Dauer, die die Unterstützung erfordert.
3. Konten des Betreibers bestehen außerhalb der Kundenmandanten. Sie erhalten in Kundenmandanten keine Rechte, und sie werden bei der Anlage eines Mandanten nicht in ihn kopiert.
4. Betriebsmaßnahmen an Datenbank, Speicher und Sicherungen können technisch eine Einsicht in Daten ermöglichen. Eine gezielte Einsichtnahme in Inhalte eines Mandanten unterbleibt ohne Freigabe nach Absatz 1.

§ 12 Löschung und Rückgabe

1. Nach Wahl des Verantwortlichen werden die Auftragsdaten nach dem Ende der Leistung zurückgegeben oder gelöscht. Für die Rückgabe stehen die Exportfunktionen der Anwendung zur Verfügung, die der Verantwortliche während der Vertragslaufzeit jederzeit nutzen kann. Dazu gehört ein vollständiges Archiv des Mandanten mit den Datenbankinhalten, den hochgeladenen Dateien und einem Verzeichnis, das die enthaltenen Tabellen, die Prüfwerte je Datei und die ausgelassenen Felder nennt; ein Organisationsadministrator kann es selbst erzeugen und herunterladen. Welche Felder aus Sicherheitsgründen ausgelassen werden, nennt Anlage 1. Ist die Nutzung der Exportfunktionen aus Gründen, die der Auftragsverarbeiter zu verantworten hat, nicht möglich, stellt er einen gleichwertigen sicheren Rückgabeweg bereit.
2. Nach dem Ende des Nutzungsverhältnisses bleibt der Datenbestand 30 Kalendertage ausschließlich zur Ansicht und zum Export abrufbar (Exportfrist). Der Verantwortliche kann die Löschung ohne Ablauf der Fristen verlangen; sie wird dann unverzüglich ausgeführt.
3. Nach Ablauf der Exportfrist wird der Mandant beendet; der Zugang zur Anwendung endet damit. Nach Ablauf weiterer 30 Tage wird er mit seinen Daten, Dateien und Protokollen unverzüglich physisch gelöscht. Eine Kennung des gelöschten Mandanten verhindert, dass er durch die Wiederherstellung eines einzelnen Mandanten zurückkehrt. Der einmal vergebene Adressabschnitt einer öffentlichen Karriereseite bleibt gesperrt und wird keinem anderen Mandanten zugeteilt.
4. Ein vom Verantwortlichen gesetzter Sperrvermerk hindert die Beendigung und die Löschung des Mandanten sowie die endgültige Entfernung der von ihm erfassten Datensätze nach Absatz 6, solange er gilt. Er betrifft ausschließlich die darin bezeichneten Daten und den dokumentierten Aufbewahrungszweck und verlängert weder die Laufzeit noch die Zahlungspflicht eines bestellten Tarifs. Der Auftragsverarbeiter kann ihn nicht aufheben; das bleibt dem Verantwortlichen vorbehalten. Nach dem Ende des regulären Zugangs erfolgen die Aufhebung, erforderliche Abrufe und Auskünfte über einen gesicherten Weg, der nach einer Prüfung der Berechtigung zugänglich ist; die Zuständigkeit eines dann nicht mehr anmeldbaren Organisationsadministrators genügt dafür nicht. Nach der Aufhebung werden die gehaltenen Daten gelöscht, sobald die für sie ursprünglich geltenden Fristen abgelaufen sind; bereits abgelaufene Fristen beginnen dadurch nicht erneut.
5. Sicherungskopien, die den Mandanten oder gelöschte Daten noch enthalten, laufen nach dem vereinbarten Sicherungszyklus aus und werden nicht einzeln bearbeitet. Bis dahin sind sie verschlüsselt und gegen Zugriff geschützt. Der Sicherungszyklus ist in Anlage 2 angegeben.
6. Löschungen innerhalb eines bestehenden Mandanten nimmt der Verantwortliche selbst vor. Auf Weisung löscht der Auftragsverarbeiter einzelne Datenbestände; sieht die Anwendung dafür keine Funktion vor, führt er die Löschung auf einem anderen Weg aus. Gelöschte Daten sind sofort nicht mehr zugänglich und werden unverzüglich, spätestens nach sieben Kalendertagen, endgültig aus der Datenbank entfernt (Art. 28 Abs. 3 Buchstabe g DSGVO); der Vorgang wird im Auditprotokoll des Mandanten festgehalten. Absatz 4, Absatz 5 und Absatz 8 bleiben unberührt.
7. Endet eine vom Verantwortlichen bestellte Zusatzbuchung, löscht der Auftragsverarbeiter die Daten des betroffenen Verarbeitungsteils nach Ablauf einer Abruffrist von 30 Kalendertagen unverzüglich (Art. 28 Abs. 3 Buchstabe g DSGVO). Innerhalb der Abruffrist bleiben die Daten zur Ansicht und zum Export abrufbar; der Auftragsverarbeiter teilt dem Verantwortlichen den letzten Abruftag und den Tag der Löschung mit und erinnert sieben Tage vor der Löschung. Wird die Zusatzbuchung vor dem Tag der Löschung erneut bestellt, entfällt die Löschung. Absatz 4 gilt entsprechend; nach dem Ende eines Sperrvermerks werden die gehaltenen Daten frühestens am siebten Tag gelöscht, und der Auftragsverarbeiter teilt auch dafür den letzten Abruftag und den Tag der Löschung mit. Absatz 6 bleibt für Löschungen innerhalb des bestehenden Mandanten unberührt.
8. Dokumentationen, die der Auftragsverarbeiter aufgrund gesetzlicher Pflichten aufbewahren muss, bleiben davon unberührt.
9. Gesetzliche Rechte des Verantwortlichen auf Wechsel des Anbieters, auf einen Übergangszeitraum und auf den Abruf seiner Daten gehen den Fristen dieses Paragrafen vor. Daten werden nicht

gelöscht, bevor die dafür maßgeblichen Abrufzeiträume abgelaufen sind, es sei denn, der Verantwortliche verlangt eine frühere Löschung. Der Ablauf und die abrufbaren Daten ergeben sich aus den Nutzungsbedingungen.

§ 13 Haftung und Schlussbestimmungen

1. Für die Haftung gelten die Nutzungsbedingungen für die geteilte Installation. Art. 82 DSGVO bleibt unberührt.
2. Änderungen dieses Vertrags bedürfen einer Vereinbarung in Textform. Der Auftragsverarbeiter kann ihn einseitig nur ändern, soweit Rechtsänderungen oder Entscheidungen von Aufsichtsbehörden es erfordern; er teilt die Änderung mindestens vier Wochen vorher unter Benennung der betroffenen Bestimmungen mit. Widerspricht der Verantwortliche, kann jede Partei den Mandanten zum Wirksamwerden der Änderung beenden. Neue Verarbeitungszwecke, wesentlich neue Datenarten und ein niedrigeres Schutzniveau als das vereinbarte werden auf diesem Weg nicht zulässig; sie bedürfen einer Vereinbarung. Schweigen und die weitere Nutzung gelten nicht als Zustimmung.
3. Es gilt deutsches Recht.
4. Ist eine Bestimmung unwirksam, bleibt der übrige Vertrag wirksam.

Anlage 1: Beschreibung der Verarbeitung

Zweck. Bereitstellung und Betrieb von Skillent für die Verwaltung der Berufsausbildung des Verantwortlichen: Berichtsheft und Ausbildungsnachweise, Freigaben, Aufgaben, Bewertungen, Abwesenheiten, Entwicklungsgespräche, Zeugnisse, Dokumente, Benachrichtigungen und Exporte. Je nach Tarif und den vom Verantwortlichen eingeschalteten Modulen gehören dazu die Erfassung von Arbeitszeiten, die Einsatz- und Schichtplanung, Nachrichten zwischen den Benutzern eines Mandanten, das Onboarding neuer Auszubildender, das Prüfungspaket für die Kammer, automatisierte Abläufe und Auswertungen, die Übermittlung an Systeme des Verantwortlichen über Schnittstellen und Webhooks sowie die Verwaltung der Bewerbungen auf seine Ausbildungsstellen.

Art der Verarbeitung. Erheben, Speichern, Verändern, Auslesen, Übermitteln an die vom Verantwortlichen bestimmten Empfänger, Einschränken und Löschen innerhalb des Mandanten sowie die zum Betrieb erforderliche Sicherung, Wiederherstellung und Protokollierung.

Datenarten.

Gruppe	Angaben
Benutzer und Konten	Name, dienstliche Kontaktdaten, Benutzerkennung, Rollen, Berechtigungen, Anmeldedaten, Geheimnis der Zwei-Faktor-Anmeldung, Sitzungs- und Anmeldeprotokolle; bei Anmeldung über den eigenen Anmeldedienst eines Betriebs zusätzlich Aussteller und Client-Kennung dieses Dienstes, die dort vergebene Kennung des Kontos, die bei der Verknüpfung übermittelte E-Mail-Adresse und der Anzeigename, bei Microsoft Entra die Objekt- und Verzeichniskennung des Kontos und bei Google die Domänenangabe
Ausbildung	Ausbildungsberuf, Ausbildungszeitraum, Standort, Abteilung, Ausbildungsplan, Aufgaben, Kurse, Prüfungen
Berichtsheft und Nachweise	Einträge, Tätigkeitsbeschreibungen, Zeiten, Anhänge, die Anwesenheitsangabe des Tages einschließlich „krank“, Status, Freigaben und Ablehnungen mit Person und Zeitpunkt
Bewertungen und Gespräche	Beurteilungen, Noten, Vermerke, Entwicklungsgespräche, Zeugnisse
Arbeitszeit	bei eingeschaltetem Modul: Zeitpunkte des Kommens und Gehens mit Art des Eintrags und Kommentar, Korrekturen und Stornierungen mit Person, Zeitpunkt und Grund samt Änderungsverlauf, Anträge auf Korrektur, Abschlüsse eines Zeitraums, vereinbarte Arbeitszeiten und die Regeln zur Prüfung der Arbeitszeit

Gruppe	Angaben
Einsatz- und Schichtplanung	bei eingeschaltetem Modul: Pläne, Schichten mit Beginn, Ende und Beschreibung, die zugeordnete Person sowie Anfragen zum Tausch einer Schicht mit Begründung, Stand, Antwort und Entscheidung einschließlich der entscheidenden Person
Nachrichten im Mandanten	Nachrichten zwischen zwei Benutzern und in Gruppen mit Inhalt, Absender, Empfänger oder Gruppe, Zeitpunkt, Stand und der Angabe, wer eine Gruppennachricht gelesen hat
Abwesenheiten	Art der Abwesenheit einschließlich der Angabe „krank“, Zeitraum, Status, Entscheidung und Vermerk, dazu die je Person geführten Kontingente für Krankheitstage und die daraus abgeleiteten Zahlen. Bei einer Krankmeldung nimmt der geteilte Betrieb keinen Freitext an — weder Grund noch Prüfvermerk noch Stornogrund — und liefert vorhandene Werte auf keinem Leseweg aus. Ein Feld oder ein Uploadweg für Arbeitsunfähigkeitsbescheinigungen besteht nicht
Jugendarbeitsschutz	bei eingeschaltetem Modul das Datum der Erst- und Nachuntersuchung nach dem Jugendarbeitsschutzgesetz, die Angabe, ob die Bescheinigung vorliegt, und der Tag, bis zu dem die Person minderjährig ist. Keine Befunde, keine Diagnosen, keine Bescheinigungsdateien. Die Einträge werden mit dem 18. Geburtstag oder mit dem Ende des Ausbildungsverhältnisses entfernt
Bewerbungen	bei eingeschaltetem Modul: Vorname, Name, E-Mail-Adresse und Telefonnummer der bewerbenden Person, die Stelle, die Nachricht der Bewerbung, hochgeladene Bewerbungsunterlagen, Stand des Verfahrens, interne Vermerke und eine interne Bewertung, der Nachrichtenverkehr, Termine für Gespräche sowie Zeitpunkt und Fassung der Datenschutzangabe, die bei der Bewerbung gegolten hat
Übernahme eines Berichtshefts aus einem anderen System	der von der auszubildenden Person selbst ausgeführte Export als Datei, bei einem Export aus dem Digitalen Berichtsheft der Kammern das PDF und das Anhänge-Archiv, dazu Zeitraum, Herkunftsvermerk und ein Vermerk der ablegenden Person. Der Inhalt der Dateien wird nicht ausgelesen; Angaben, die ein solcher Export auf seinem Deckblatt trägt, etwa Geburtsdatum und Anschrift, liegen allein in der Datei und in keinem Feld der Anwendung
Onboarding	bei eingeschaltetem Modul: je auszubildender Person eine Checkliste mit Bezeichnung, Beginn, Fälligkeitstag und Stand; je Aufgabe Titel und Beschreibung, der Tag der Fälligkeit, die zuständige Person und die Rolle, aus der sie bestimmt wurde, die erledigende Person mit Zeitpunkt sowie die Zuordnung zu einem hinterlegten Dokument; Vorlagen mit der Person, die sie angelegt hat
Exporte	je Ausfuhr die auszubildende Person, die sie ausführende Person, Art und Zeitraum der Ausfuhr, Stand und Fehlermeldung sowie die erzeugte Datei mit Größe und Prüfwert; wird ein Prüfungspaket für eine Kammer erzeugt, zusätzlich die dabei verwendete Fassung des Prüfstellenprofils
Schnittstellen und Übermittlung	bei eingeschaltetem Modul: Schnittstellenzugänge mit Bezeichnung, Berechtigungen, Geltungsdauer, letzter Nutzung und der Person, die sie angelegt hat; Kalenderabonnements je Konto mit letzter Nutzung; Ziele für Webhooks mit Adresse, Auswahl der Ereignisse, Beschreibung und der Person, die sie zuletzt gespeichert hat; je Übermittlung das übermittelte Ereignis mit seinem Inhalt, die Zustellversuche, der Antwortstatus und eine Fehlermeldung
Automatisierte Abläufe	bei eingeschaltetem Modul: Regeln mit Bezeichnung, Beschreibung, Auslöser, Bedingungen und Schritten samt der Person, die sie angelegt hat; je Lauf die Person, um die es geht, die auslösende Person, die übergebenen Werte, Stand, Versuche und eine Fehlermeldung je Schritt; Regeln für die automatische Zuordnung neuer Konten mit dem verglichenen Merkmal und seinem Wert, dem Ausbildungsprogramm und der zugeordneten betreuenden Person. Auswertungen rechnen aus dem vorhandenen Bestand und legen keine eigenen Angaben ab
Dokumente und Dateien	hochgeladene Dateien und Anhänge mit den dazugehörigen Angaben; wird ein Dokument über einen Link geteilt, zusätzlich die Person, die den Link erstellt hat, seine Geltungsdauer, ein Widerruf sowie Zahl und Zeitpunkt der Abrufe

Gruppe	Angaben
Protokolle	Auditeinträge zu administrativen und fachlichen Vorgängen mit Person, Zeitpunkt, Netzadresse und Browserangabe, fortlaufend über eine Hashkette gesichert; Benachrichtigungen; die zum Betrieb des Mandanten erforderlichen technischen Protokolle

Kategorien betroffener Personen. Auszubildende, darunter Minderjährige; Ausbilderinnen und Ausbilder; weitere Beschäftigte des Verantwortlichen mit einem Konto im Mandanten; weitere Personen, denen der Verantwortliche ein Konto in seinem Mandanten gibt, etwa prüfende oder beauftragte Personen mit Lesezugang; bei eingeschaltetem Modul für Bewerbungen auch Bewerberinnen und Bewerber.

Besondere Kategorien. Gesundheitsdaten werden in begrenztem Umfang verarbeitet: die Abwesenheitsart „krank“ mit ihrem Zeitraum, die daraus gebildeten Krankheitskontingente und die daraus abgeleiteten Zahlen in Übersichten und Auswertungen, die Anwesenheitsangabe „krank“ in den Einträgen des Berichtshefts und, bei eingeschaltetem Modul, die Daten der Untersuchungen nach dem Jugendarbeitsschutzgesetz mit der Angabe, ob die Bescheinigung vorliegt. Schon diese Angaben sind Gesundheitsdaten; eine Diagnose ist dafür nicht erforderlich. Weitergehende Angaben sind nicht Zweck der Verarbeitung, und der geteilte Betrieb enthält dafür kein vorgesehenes Feld: Der Freitextgrund einer Abwesenheit ist dort abgeschaltet, einen Uploadweg für Arbeitsunfähigkeitsbescheinigungen gibt es nicht, und das Modul zum Jugendarbeitsschutz führt keine Befunde und keine Bescheinigungsdateien. Hochgeladene Bewerbungsunterlagen und Freitextfelder, etwa in den Berichtsheft-Einträgen, können solche Angaben dennoch enthalten; technisch ausschließen lässt sich das nicht. Der Verantwortliche prüft die Rechtsgrundlage einschließlich Art. 9 DSGVO und § 26 Abs. 3 BDSG, weist seine Benutzer darauf hin und begrenzt diese Angaben auf das Erforderliche.

Protokolle und eigene Sicherheitsdaten. Protokolle über fachliche und administrative Vorgänge eines Mandanten sowie die zur Bereitstellung der Benutzerkonten und zum Versand der fachlichen Benachrichtigungen erforderlichen Verarbeitungen erfolgen im Auftrag des Verantwortlichen. Davon getrennt verarbeitet der Auftragsverarbeiter die in der Datenschutzerklärung der Anwendung bezeichneten, auf das Erforderliche begrenzten Sicherheitsdaten zum Schutz der gesamten Installation in eigener Verantwortung; Inhalte aus Berichtsheften, Bewertungen, Nachrichten und Bewerbungsunterlagen werden dafür nicht übernommen. Dasselbe Ereignis kann in beiden Verarbeitungen vorkommen; Umfang, Zugriff und Löschfrist sind dann je Zweck festgelegt.

Rückgabe und Archiv. Das Archiv nach § 12 Abs. 1 enthält je Tabelle eine strukturierte Datei im JSON-Format, die hochgeladenen Dateien unverändert und ein Verzeichnis mit der Tabellenliste, den Prüfwerten je Datei und den ausgelassenen Feldern. Nicht enthalten sind die Zugangsgeheimnisse der Konten (Prüfwerte von Passwörtern, Geheimnisse der Zwei-Faktor-Anmeldung, Prüfwerte von Token, Client-Geheimnisse und verschlüsselt gespeicherte Geheimnisse), die Netzadresse einer Abzeichnung per Link sowie installationsweite Register, die keinem Mandanten zugeordnet sind. Diese Auslassungen sind abschließend; weitere Fachdaten werden nicht ausgelassen.

Dauer. Für die Laufzeit des Nutzungsverhältnisses; danach nach § 12.

Verarbeitungsort. Deutschland.

Öffentliche Karriereseite. Die Karriereseite eines Mandanten ist zunächst abgeschaltet. Sie wird erst erreichbar, wenn der Verantwortliche sie einschaltet und Impressum, Datenschutzerklärung und Nutzungsbedingungen seines Mandanten vollständig hinterlegt sind; fehlt eine dieser Angaben oder steht dort noch ein Platzhalter, bleibt die Seite aus. Jeder Mandant erhält eine eigene Karriereseite unter einer eigenen Adresse. Eine gemeinsame Seite, die mehrere Betriebe zusammen auflistet, gibt es in diesem Betriebsmodell nicht; sie würde offenlegen, welche Betriebe den Dienst nutzen. Für die Inhalte dieser Seiten und für die Information der Bewerberinnen und Bewerber ist der Verantwortliche zuständig.

Anmeldung über den eigenen Anmeldedienst eines Betriebs. Richtet der Verantwortliche für seinen Mandanten die Anmeldung über seinen eigenen Anmeldedienst ein, ist dieser Dienst kein Unterauftragsverarbeiter des Auftragsverarbeiters: Beauftragt wird er vom Verantwortlichen, und die Angaben kommen von dort zum Auftragsverarbeiter. Er steht deshalb nicht in Anlage 3. Übernommen

werden nur die in der Gruppe „Benutzer und Konten“ genannten Angaben; ein Verzeichnisabgleich findet nicht statt, und Zugriffs- oder Erneuerungstoken des Dienstes werden nicht gespeichert. Die Verknüpfung eines Kontos mit seiner Kennung bei diesem Dienst wird mit dem Konto gelöscht.

Nicht enthalten. Im geteilten Betrieb stehen instanzweites LDAP, SAML und die instanzweite Anbindung eines OIDC-Anbieters nicht zur Verfügung.

Anlage 2: Technische und organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen für den geteilten SaaS-Betrieb sind diesem Vertrag als Anlage 2 beigefügt und sind Bestandteil des Vertrags. Sie gelten in der Fassung dieses Vertrags; sie bleibt unter ihrer Bezeichnung und ihrem Prüfwert abrufbar. Änderungen richten sich nach § 5 Abs. 2.

Geltungsbereich

Diese Übersicht beschreibt die Maßnahmen nach Art. 32 DSGVO für den Betrieb von Skillent als geteilte Installation, in der mehrere Betriebe in getrennten Mandanten arbeiten. Sie ist Anlage 2 des Auftragsverarbeitungsvertrags für diesen Betrieb und gilt für alle Mandanten einheitlich.

Für Self-Hosted-Installationen und für Managed Hosting gelten die dortigen Maßnahmen; sie sind nicht Gegenstand dieses Dokuments.

Betriebsrahmen

- Die Anwendung läuft in einer von SoftwareGenie24 betriebenen Umgebung in Deutschland. Alle Daten und alle Sicherungen bleiben in Deutschland.
- Die Anwendung ist eine Eigenentwicklung von SoftwareGenie24. In sie ist kein Dienst eines Drittanbieters für Analyse, Fehlerverfolgung, Nutzungsmessung oder Produktunterstützung eingebunden. Für Rechenzentrum, Netz, Speicher und E-Mail-Versand sind die in der Liste der Unterauftragsverarbeiter genannten Unternehmen eingesetzt.
- Die ausgelieferten Seiten laden keine Skripte, Schriften oder Bilder von Adressen Dritter. Es gibt keine Reichweitenmessung und keine Werbenetzwerke.
- Eine Zertifizierung des Dienstes liegt nicht vor.

Trennung der Mandanten

Die Trennung fremder Betriebe in einer Installation ist die zentrale Maßnahme dieses Betriebsmodells. Sie beruht auf mehreren voneinander unabhängigen Schichten:

Schicht	Ausgestaltung
Datenbank	Die Tabellen mit Mandantenbezug stehen unter einer erzwungenen zeilenbasierten Zugriffsregel, geprüft gegen die je Transaktion gesetzte Mandantenkennung. Ausgenommen sind benannte Gruppen, in denen der Mandant beim Zugriff noch nicht feststeht oder die Verarbeitung bewusst instanzweit läuft: Anmeldung, Token und Rollen, die öffentlichen Wege für Bewerbungen und Freigabelinks, die fortlaufende Auditkette und die Vorgänge, die der Betreiber für einen Mandanten ausführt. Dort trägt die Trennung die Anwendung. Jede Ausnahme ist mit Grund verzeichnet, und ein Prüflauf in der Entwicklung leitet die Liste der Tabellen aus dem Datenbankschema ab und schlägt bei jeder nicht eingeordneten Tabelle fehl. Wo der Mandant erst mit der Anmeldung feststeht — bei der Zuordnung einer E-Mail-Domäne zu einem Mandanten und bei einem laufenden Anmeldevorgang über den eigenen Anmeldedienst eines Betriebs —, wird die Regel nicht aufgehoben, sondern auf die gesuchte Zeile verengt: lesbar ist allein die Zeile zu der abgefragten Domäne beziehungsweise zu dem Prüfwert des laufenden Vorgangs, und daraus gelesen wird nur der Mandant.
Datenbankrolle	Die Anwendung verbindet sich mit einer Rolle ohne Recht zur Umgehung der Zugriffsregel.
Anwendung	Eine Prüfschicht bricht jede Anfrage ab, bei der keine Mandantenkennung gesetzt ist. Zugriffe über Kennungen eines fremden Mandanten werden abgelehnt.

Schicht	Ausgestaltung
Identitäten	Konten werden über Mandantengrenzen hinweg nicht verknüpft: keine Verknüpfung über Verzeichniseinträge, Anmeldekennungen eines externen Anbieters oder E-Mail-Adressen, keine Suche über fremde Mandanten bei der Anmeldung.
Auskunft	Die Anwendung gibt keine Angaben über andere Mandanten heraus, auch nicht mittelbar durch Namensprüfungen oder Fehlermeldungen.
Betreiber	Konten des Betreibers liegen in einem eigenen Mandanten. Sie werden nicht in Kundenmandanten kopiert und haben dort keine Rechte.
Tests	Eine Testmatrix prüft die Schnittstellen der Anwendung mit Kennungen aus einem fremden Mandanten. Neue Wege werden in beiden Betriebsarten getestet.

Instanzweite Anmeldeverfahren sind in diesem Betrieb abgeschaltet: LDAP, SAML und die instanzweite Anbindung eines OIDC-Anbieters stehen nicht zur Verfügung. Eine solche Konfiguration verhindert den Start des geteilten Betriebs.

Art.-32-Übersicht

Kontrollbereich	Ausgestaltung
Zutrittskontrolle	Betrieb in einem Rechenzentrum des benannten Infrastrukturdienstleisters in Deutschland mit physischer Zutrittskontrolle. SoftwareGenie24 unterhält dort keine eigenen Räume.
Zugangskontrolle	Personalisierte administrative Zugänge, Need-to-know-Prinzip und starke Authentisierung für administrative Zugänge. Benutzerpasswörter werden mit Argon2 abgeleitet. Als zweiter Faktor stehen TOTP und Passkeys nach WebAuthn zur Verfügung; der Organisationsadministrator kann den zweiten Faktor für ausgewählte Rollen seines Mandanten verpflichtend setzen. Wer sich über den eigenen Anmeldedienst seines Betriebs anmeldet, bringt die Faktoren dieses Dienstes mit; die Vorgabe des Organisationsadministrators wirkt für diesen Weg nicht. Beim erstmaligen Verknüpfen eines bestehenden Kontos mit dem Anmeldedienst verlangt die Anwendung Passwort und, soweit eingerichtet, zweiten Faktor dieses Kontos.
Zugriffskontrolle	Rollen- und bereichsbezogene Rechtevergabe innerhalb des Mandanten, vom Organisationsadministrator verwaltet. Festgelegte Vorgänge können an die Zustimmung einer zweiten berechtigten Person gebunden werden; die antragstellende Person ist dabei ausgeschlossen. Eine Prüfrolle liest das Auditprotokoll, ohne etwas ändern zu können.
Weitergabekontrolle	Übertragung ausschließlich über HTTPS mit TLS 1.2 oder 1.3; ältere Protokollversionen sind abgeschaltet. Der Reverse Proxy setzt HTTP Strict Transport Security. Fachliche ausgehende Verbindungen aus einem Mandanten — Webhooks und Schnittstellenaufrufe — bestehen nur zu den Zielen, die der Mandant selbst hinterlegt; eine Adresse, die er dort einträgt, wird nicht von der Anwendung abgerufen, um Inhalte zu laden, sondern vor dem Aufruf gegen Namens- und Netzadresse geprüft, mit der geprüften Auflösung verbunden und ohne Weiterleitungen angesprochen, und ein Kalenderabonnement ist ein von der Anwendung erzeugter Feed ohne Import einer fremden Adresse. Davon getrennt bestehen die zum Betrieb erforderlichen Verbindungen zu E-Mail-Versand, Verwaltungsplattform und Sicherungsspeicher; die dafür eingesetzten Unternehmen stehen in der Liste der Unterauftragsverarbeiter.
Eingabekontrolle	Auditprotokoll je Mandant für administrative und fachliche Vorgänge mit Person und Zeitpunkt, fortlaufend über eine Hashkette gesichert. Anträge, Zustimmungen, Ablehnungen und Rückzüge einer Freigabe durch eine zweite Person sind darin enthalten.
Auftragskontrolle	Verarbeitung auf Grundlage des Auftragsverarbeitungsvertrags für den geteilten Betrieb; Weisungswege und Supportfreigabe sind dort geregelt.
Verfügbarkeitskontrolle	Mehrere Anwendungsprozesse hinter einem vorgelagerten Dienst, Überwachung des Betriebszustands, technische Health-Checks, dokumentierte Störungs- und Wiederanlaufwege. Updates werden prozessweise ausgebracht.

Kontrollbereich	Ausgestaltung
Trennungskontrolle	Siehe Abschnitt „Trennung der Mandanten“. Produktiv-, Test- und Administrationsumgebungen sind getrennt.
Pseudonymisierung und Verschlüsselung	Transportverschlüsselung wie oben. Die Anwendung verschlüsselt die Geheimnisse der Zwei-Faktor-Anmeldung, die Signierschlüssel für ausgehende Benachrichtigungen, eingereihte Passwort-Zurücksetzungen und das Client-Geheimnis eines eigenen Anmeldedienstes mit einem eigenen Feldschlüssel, der im laufenden Betrieb gewechselt werden kann. Das kurzlebige Geheimnis eines laufenden Anmeldevorgangs über diesen Dienst liegt ebenfalls verschlüsselt und nur bis zum Abschluss des Vorgangs. Die Fachdaten selbst liegen in der Datenbank unverschlüsselt; ihr Schutz beruht auf der Trennung der Mandanten, den Zugriffsrechten, dem Schutz des Servers und der Begrenzung der administrativen Zugänge. Das gilt auch für die Angaben zum Gesundheitszustand, die der Dienst führt; eine Verschlüsselung auf Anwendungsebene würde hier die Trennung, die Zugriffsrechte und die Auswertbarkeit nicht ersetzen, sondern den Schlüssel in dieselbe Umgebung legen. Wer administrativen Zugang zur Datenbank hat, kann die Inhalte technisch lesen; begrenzt wird das organisatorisch und über die Rechte der Anwendung, nicht technisch ausgeschlossen. Sicherungen werden verschlüsselt abgelegt. Geheimnisse werden getrennt von Daten und Quelltexten verwaltet.
Wiederherstellbarkeit	Tägliche verschlüsselte Sicherung der Datenbank und der Dateien, Aufbewahrung 30 Tage, Speicherort Deutschland. Ein einzelner Mandant lässt sich wiederherstellen, ohne die übrigen anzufassen; dabei ruht sein Zugang, und seine Sitzungen werden beendet. Angaben, die nach der Sicherung auf ein Löschverlangen einer betroffenen Person hin entfernt wurden, kehren dabei nicht zurück: Die Wiederherstellung eines einzelnen Mandanten wird abgelehnt, wenn für ihn nach dem Stand der Sicherung eine solche Löschung ausgeführt wurde, und bei der Wiederherstellung der gesamten Installation werden diese Löschungen erneut angewandt. Wird die gesamte Installation aus einer Sicherung wiederhergestellt, die vor der Löschung eines Mandanten entstanden ist, kann dieser Mandant dagegen zurückkehren; er wird dann erneut gelöscht. Ebenso kehren Datensätze zurück, die zwischen dem Stand der Sicherung und der Wiederherstellung durch einen regelmäßigen Löschlauf entfernt wurden — etwa nach Ablauf einer Aufbewahrungsfrist; der nächste Tageslauf entfernt sie erneut. Sicherheitsrelevante Einstellungen des Mandanten, die Anmeldefelder der Konten und privilegierte Rollen folgen nicht der Sicherung, sondern behalten den Stand im Zeitpunkt der Wiederherstellung. Eine Wiederherstellung hinterlässt keinen Mandanten ohne einen Organisationsadministrator, der sich danach anmelden kann; ist das nicht erreichbar, wird nichts verändert und der Mandant bleibt ausgesetzt. Eine Löschung, die mit dem Ende einer Zusatzbuchung fällig war, wird nach einer Wiederherstellung nachgeholt, solange die Zusatzbuchung beendet bleibt; letzter Abruftag und Tag der Löschung werden dafür neu genannt. Wiederherstellungen werden dokumentiert; die Abweichungen von der Sicherung stehen im Bericht zur Wiederherstellung und im Auditprotokoll des Mandanten. Zusätzlich wird eine verschlüsselte Kopie auf einem Speicher bei einem zweiten Anbieter in Deutschland gehalten; sie ist über einen eigenen Zugang getrennt, der keinen Zugriff auf die Instanz hat, und läuft spätestens mit ihr aus.
Regelmäßige Überprüfung	Dokumentierte Betriebsabläufe, Release- und Wiederherstellungsprüfungen, Überwachung, Störungsbearbeitung und Prüfung der Berechtigungen. Für die Rechtevergabe unterstützt die Anwendung Zugriffsprüfungen mit hinterlegbarem Prüftakt, weist den nächsten fälligen Termin aus und meldet Rückstand.
Sichere Verarbeitung von Dateien	Typ- und Größenprüfung der Uploads sowie Schadsoftwareprüfung. Die Prüfung wird fail-closed betrieben: Ist sie nicht durchführbar, wird der Upload abgewiesen.
Begrenzung des Datenbestands	Jeder Mandant hat ein Speicherkontingent in Byte. Ein Zähler je Mandant wird mit dem gespeicherten Objekt in derselben Transaktion fortgeschrieben; ein Abgleichlauf rechnet ihn aus den gespeicherten Größen nach. Ab wann das Kontingent weitere Uploads abweist, richtet sich nach dem Tarif: im kostenlosen Tarif unmittelbar, bei einem bezahlten Tarif oder einer bezahlten Zusatzbuchung erst nach Hinweis und Frist.

Kontrollbereich	Ausgestaltung
Sichere Entwicklung und Lieferkette	Linting, Typ- und Funktionstests, Secret- und Codeprüfung, Abhängigkeits- und Dateisystemanalyse sowie Prüfung der Image-Definitionen vor jeder Auslieferung. Die Prüfungen sind blockierend.

Datenminimierung im geteilten Betrieb

Der geteilte Betrieb führt weniger Datenarten als eine eigene Installation. Die folgenden Felder und Wege sind dort nicht verfügbar:

- kein Freitext bei einer Krankmeldung. Grund, Prüfvermerk und Stornogrund nimmt die Schnittstelle dort nicht an, und vorhandene Werte werden auf keinem Leseweg ausgeliefert, auch nicht im Auskunftsexport, im Protokoll und im Posteingang. Die Abwesenheit trägt damit nur Art, Zeitraum, Status und die Entscheidung; die Art „krank“ bleibt als Kategorie erhalten, weil sie für die Ausbildungszeit gebraucht wird.
- kein Feld und kein Uploadweg für Arbeitsunfähigkeitsbescheinigungen oder andere ärztliche Unterlagen. Auch die Einarbeitungsvorlage zur ärztlichen Erstuntersuchung entfällt im geteilten Betrieb.
- im Modul zum Jugendarbeitsschutz nur das Datum der Erst- und Nachuntersuchung, die Angabe, ob die Bescheinigung vorliegt, und der Tag, bis zu dem die Person minderjährig ist. Keine Befunde, keine Diagnosen, keine Dateien. Die Einträge werden mit dem 18. Geburtstag oder mit dem Ende des Ausbildungsverhältnisses entfernt.
- keine instanzweiten Anmeldeverfahren. Ein Betrieb kann für seinen Mandanten die Anmeldung über seinen eigenen Anmeldedienst einrichten; von dort kommen dann die Kennung des Kontos bei diesem Dienst, Name und E-Mail-Adresse zu uns. Ein Verzeichnisabgleich findet nicht statt: Gruppen, Abteilungen und weitere Verzeichnisangaben werden nicht übernommen, und Zugriffs- oder Erneuerungstoken des Dienstes werden nicht gespeichert.
- keine Reichweitenmessung, keine Nutzungsanalyse, keine Funktion künstlicher Intelligenz.

Die geteilte Instanz wird neu aufgesetzt. Eine bestehende Einzelinstallation wird nicht in den geteilten Betrieb umgestellt; damit gibt es dort keine Bestände aus einer Zeit, in der diese Felder noch befüllt werden konnten.

Freitextfelder in den fachlichen Einträgen bleiben bestehen. Was dort eingetragen wird, entscheidet der jeweilige Benutzer; die Anwendung weist an diesen Stellen darauf hin, nur die für die Ausbildung erforderlichen Angaben einzutragen.

Registrierung und Missbrauchsschutz

- Die Registrierung verlangt die Bestätigung der angegebenen E-Mail-Adresse. Ein Mandant entsteht erst nach der Bestätigung; unbestätigte Registrierungen werden nach Ablauf der Bestätigungsfrist gelöscht.
- Vor dem Absenden ist eine Rechenaufgabe im Browser zu lösen. Sie läuft ohne Dienst eines Drittanbieters und ohne Cookie.
- Die Zahl der Registrierungen wird nach Netzadresse und E-Mail-Domäne begrenzt.
- Fehlgeschlagene Anmeldeversuche werden begrenzt und protokolliert.

Zugriff durch den Betreiber

- Ein Zugriff auf die Inhalte eines Mandanten zur Unterstützung findet nur nach Freigabe durch den Organisationsadministrator dieses Mandanten statt. Die Freigabe ist befristet und widerruflich. Erteilung, Nutzung, Ablauf und Widerruf stehen mit Person und Zeitpunkt im Auditprotokoll.

- Der Umfang einer Freigabe ist weit, und das steht hier, damit niemand ihn für eng hält: Wer sie erteilt, öffnet den Mandanten für die lesende Einsicht in nahezu alle Bereiche, so wie sie ein Administrator des Mandanten sieht — einschließlich der Inhalte des Berichtshefts, der Bewertungen und der Dateien. Die Freigabe gilt nach Wahl des Administrators für 24 Stunden, drei oder sieben Tage und lässt sich jederzeit vorher beenden.
- Verändern kann der Betreiber in einem freigegebenen Mandanten nichts: Die Anwendung lässt dort nur lesende Zugriffe zu und weist jeden anderen ab. Ausgenommen sind auch lesend die Freigabe selbst, Export und Beendigung des Mandanten, die Auskunfts- und Löschvorgänge und die Verwaltung der Schnittstellenschlüssel. Geprüft wird das bei jeder einzelnen Anfrage; nach Ablauf oder Widerruf der Freigabe wird jeder Zugriff abgewiesen. Es ist eine Prüfung der Anwendung und kein gesondertes, nur lesendes Datenbankkonto. Was während einer Freigabe eingesehen oder heruntergeladen wurde, lässt der Widerruf nicht zurückholen.
- Ohne Freigabe sehen Betreiberkonten je Mandant nur Status, Tarif und Verbrauch, die bestätigte Kontaktadresse der registrierenden Person und die Angabe, ob ein Sperrvermerk die Beendigung des Mandanten verhindert. Zu dem Vermerk selbst — Gegenstand, Grund, Zeitraum und betroffene Datensätze — gehört diese Angabe nicht; sie steht im Mandanten.
- Betriebsmaßnahmen an Datenbank, Speicher und Sicherungen können technisch eine Einsicht ermöglichen. Eine gezielte Einsichtnahme in Inhalte unterbleibt ohne Freigabe.
- Systemzustand, Metriken, Instanzkonfiguration und Installationslizenz sind im geteilten Betrieb nur für Betreiberkonten erreichbar. Administratoren eines Mandanten sehen Tarif und Verbrauch ihres Mandanten.

Löschung

- Der Mandant löscht Daten innerhalb seines Bestandes selbst. Gelöschte Daten sind sofort nicht mehr zugänglich; ein täglicher Vorgang entfernt sie unverzüglich, spätestens nach sieben Kalendertagen, endgültig aus der Datenbank und hält Art und Anzahl der entfernten Datensätze im Auditprotokoll des Mandanten fest. Ein geltender Sperrvermerk hindert diese Entfernung.
- Nach dem Ende des Nutzungsverhältnisses läuft zuerst die Exportfrist des Auftragsverarbeitungsvertrags; solange sie läuft, bleibt der Mandant bestehen und ist nur noch zur Ansicht und zum Export erreichbar. Erst danach wird er beendet, und damit endet der Zugang.
- Ein beendeter Mandant wird nach Ablauf der im Auftragsverarbeitungsvertrag genannten Frist physisch gelöscht: Dateien, Daten in Abhängigkeitsreihenfolge und Protokolle dieses Mandanten. Eine Kennung verhindert, dass er durch eine Wiederherstellung zurückkehrt. Ein gesetzter Sperrvermerk hindert Beendigung, Löschung und Wiederherstellung, solange er gilt.
- Sicherungen, die gelöschte Daten oder einen gelöschten Mandanten noch enthalten, laufen nach dem Sicherungszyklus aus und werden nicht einzeln bearbeitet.

Organisatorische Maßnahmen

- Zugriffsberechtigte Personen sind auf Vertraulichkeit verpflichtet und für Datenschutz und Informationssicherheit unterrichtet.
- Administrative Rechte werden auf konkrete Aufgaben begrenzt und bei Wegfall des Bedarfs entzogen.
- Weisungen, Supportfreigaben, Sicherheitsmeldungen und Löschaufträge werden über nachvollziehbare Kommunikationswege bearbeitet.
- Sicherheitsrelevante Änderungen und Vorfälle werden dokumentiert und nach Risiko behandelt.
- Unterauftragsverarbeiter werden nach dem Auftragsverarbeitungsvertrag ausgewählt, gebunden und vor einer Änderung angekündigt.

- Störungen und Sicherheitsvorfälle werden nach einem dokumentierten Verfahren bearbeitet; betroffene Mandanten werden unterrichtet.

Grenzen

- Der geteilte Betrieb ist für die beschriebenen Ausbildungsdaten ausgelegt. Besondere Kategorien personenbezogener Daten sind nicht sein Zweck.
- Kundeneigene Vorgaben zu Kryptografie, Netztrennung, Aufbewahrung oder Verfügbarkeit lassen sich in einer geteilten Installation nicht umsetzen. Dafür stehen Self-Hosted und Managed Hosting zur Verfügung.
- Eine Verfügbarkeitszusage ist für den geteilten Betrieb nicht vereinbart.
- Diese Maßnahmen ersetzen nicht die Schutzbedarfsanalyse des Verantwortlichen.

Änderung der Maßnahmen

SoftwareGenie24 darf die Maßnahmen fortentwickeln, solange das Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen mit Auswirkung auf die Auftragsverarbeitung werden in Textform mitgeteilt.

Anlage 3: Unterauftragsverarbeiter

Die Liste der Unterauftragsverarbeiter für den geteilten SaaS-Betrieb ist diesem Vertrag als Anlage 3 beigefügt und ist Bestandteil des Vertrags. Sie gilt in der Fassung dieses Vertrags; sie bleibt unter ihrer Bezeichnung und ihrem Prüfwert abrufbar. Weitere Unterauftragsverarbeiter kommen nur über das Verfahren nach § 7 hinzu.

Diese Liste ist Anlage 3 des Auftragsverarbeitungsvertrags für den geteilten SaaS-Betrieb von Skillent. Sie gilt nur für dieses Betriebsmodell. Für Self-Hosted-Installationen und Managed Hosting gilt die Unterauftragsverarbeiterliste des Vendor-Pakets.

Verarbeitungskette

Ebene	Unternehmen	Anschrift	Leistung	Verarbeitungsort
unmittelbarer Unterauftragsverarbeiter	Host-Unlimited.de; Betreiberin: Bieber IT GmbH; AG Hildesheim, HRB 207358; USt-IdNr. DE340893627; Geschäftsführung: Tim-Gerrit Bieber	Braunschweiger Straße 22, 38518 Gifhorn, Deutschland	Rechenzentrums-, Server-, Datenbank- und Speicherinfrastruktur für die geteilte Instanz einschließlich der Sicherungen	Deutschland
unmittelbarer Unterauftragsverarbeiter	Host-Unlimited.de; Betreiberin: Bieber IT GmbH; AG Hildesheim, HRB 207358	Braunschweiger Straße 22, 38518 Gifhorn, Deutschland	Serverinfrastruktur für die Verwaltungs-, Lizenz- und Supportplattform von SoftwareGenie24, in der je Mandant Status, Tarif und Verbrauch verarbeitet werden, bei Mandanten eines Betriebs zusätzlich die bestätigte Kontaktadresse der registrierenden Person	Deutschland

Ebene	Unternehmen	Anschrift	Leistung	Verarbeitungsort
unmittelbarer Unterauftragsverarbeiter	Hetzner Online GmbH; AG Ansbach, HRB 6089	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Speicher für die verschlüsselte Sicherungskopie der geteilten Instanz, in einem eigenen Unterzugang ohne Zugriff auf die Instanz	Deutschland
unmittelbarer Unterauftragsverarbeiter	GieMedia UG (haftungsbeschränkt); AG Braunschweig, HRB 211082	Dorfstraße 24, 38319 Remlingen-Semmenstedt, Deutschland	Serverinfrastruktur für den E-Mail-Versand der Anwendung und für die Support- und Vertragskorrespondenz	Deutschland
weiterer Unterauftragsverarbeiter, zweite Stufe über GieMedia	Keyweb AG; AG Jena, HRB 112403	Neuwerkstraße 45/46, 99084 Erfurt, Deutschland	Rechenzentrumsleistung für die Serverinfrastruktur der GieMedia UG	Deutschland

Mit allen genannten Unternehmen besteht ein Vertrag nach Art. 28 DSGVO. Über die genannten Unternehmen hinaus ist für diesen Dienst kein Unterauftragsverarbeiter eingesetzt. Die Keyweb AG ist als zweite Stufe über die GieMedia UG eingebunden; sie erbringt die Rechenzentrumsleistung und hat keinen fachlichen Zugriff auf Inhalte.

Verarbeitungsort

Alle Daten der geteilten Instanz, alle Dateien und alle Sicherungen liegen in Deutschland. Eine Verarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums findet nicht statt und ist für diesen Dienst nicht freigegeben. Produktregionen der eingesetzten Anbieter außerhalb der EU oder des EWR werden nicht genutzt.

Was nicht eingesetzt wird

Diese Liste ist auch deshalb kurz, weil der Dienst ohne die üblichen Zulieferer arbeitet:

- kein Dienst eines Drittanbieters für Reichweitenmessung, Nutzungsanalyse oder Werbung
- kein Auslieferungsnetz für Skripte, Schriften oder Bilder; alle Dateien kommen vom eigenen Server
- kein Captcha-Dienst eines Drittanbieters; die Rechenaufgabe vor der Registrierung läuft im Browser des Nutzers gegen den eigenen Server
- kein Dienst eines Drittanbieters für Fehlerverfolgung oder Betriebsüberwachung
- kein Helpdesk-, Ticket- oder CRM-Dienst eines Drittanbieters; die Supportplattform ist eine Eigenentwicklung von SoftwareGenie24
- keine Push-Benachrichtigungen über die Zustelldienste der Browser- und Betriebssystemhersteller
- kein Dienst eines Drittanbieters für Zahlungen innerhalb der Anwendung; ein bezahlter Tarif wird über den Bestellweg von SoftwareGenie24 bestellt, für den die dortige Datenschutzerklärung gilt. Die Anwendung übermittelt für eine Bestellung keine Daten; der bestellte Tarif erreicht den Mandanten als Lizenz

Vom Nutzer selbst gewählte Ziele

Der Mandant kann Adressen hinterlegen, an die die Anwendung Daten sendet, etwa ein Ziel für ausgehende Benachrichtigungen. Solche Empfänger wählt der Mandant selbst; sie sind seine Dienstleister und werden nicht zu Unterauftragsverarbeitern von SoftwareGenie24. Die bloße technische Anschlussmöglichkeit genügt dafür nicht.

Ein eigener Mailserver steht in der geteilten Installation nicht zur Verfügung. Die Anmeldung über den eigenen Anmeldedienst eines Betriebs ist zum Start nicht freigeschaltet; wird sie freigeschaltet, kann ein Betrieb sie für seinen Mandanten einrichten. Dieser Dienst ist kein Unterauftragsverarbeiter von SoftwareGenie24, weil ihn der Betrieb selbst beauftragt und die Angaben von dort zu SoftwareGenie24 kommen. Er steht deshalb nicht in der Tabelle. Die Einbindung eines Anmeldedienstes für die gesamte Installation gibt es nicht.

Auswahl und vertragliche Bindung

Vor der Beauftragung werden Leistungszweck, Verarbeitungsort, Zugriffsmöglichkeit, Schutzmaßnahmen und die erforderlichen Vertragsregelungen bewertet. Die einschlägigen Datenschutzpflichten werden auf jeder Stufe der Verarbeitungskette weitergegeben; dazu gehören Vertraulichkeit, Sicherheit, Weisungsbindung, Unterstützung, Löschung und Kontrollmöglichkeiten. SoftwareGenie24 bleibt gegenüber dem Kunden für die Erfüllung dieser Pflichten verantwortlich.

Änderungen

1. SoftwareGenie24 unterrichtet vor dem Einsatz eines neuen oder ausgetauschten Unterauftragsverarbeiters mindestens vier Wochen vorher in Textform.
2. Die Unterrichtung nennt Unternehmen, Leistung und Verarbeitungsort.
3. Der Verantwortliche kann innerhalb von zwei Wochen aus wichtigem datenschutzrechtlichem Grund widersprechen. Die Folgen regelt § 7 des Auftragsverarbeitungsvertrags.
4. Diese Liste ist als Anlage 3 Bestandteil des Auftragsverarbeitungsvertrags und gilt in dessen Fassung. Sie wird bei jeder Änderung fortgeschrieben; für einen bestehenden Vertrag wirkt eine Änderung nur über das Verfahren nach den Absätzen 1 bis 3. Die bei der Annahme geltende Fassung bleibt unter ihrer Bezeichnung und ihrem Prüfwert abrufbar.

Fassung 2026-10-27 · Prüfwert e29a4559137bafc2403fa10bf5b4ef78be3b515f0f49004fefce5209852aa090 · SoftwareGenie24 UG (haftungsbeschränkt), Mauernstraße 33, 38100 Braunschweig