RECHTLICHES

Auftragsverarbeitungsvertrag

Vereinbarung nach Art. 28 Abs. 3 DSGVO zwischen deinem Betrieb als Verantwortlichem und SADU Development e.U. als Auftragsverarbeiter. Fassung vom 22. September 2026.

---

§ 1 Vertragsparteien

Verantwortlicher (im Folgenden „der Betrieb"):

Firma _____
Anschrift _____
Vertreten durch _____
E-Mail _____

Auftragsverarbeiter (im Folgenden „SADU"):

SADU Development e.U.
Inhaber: Sandin Đulić
Gußriegelstraße 40/2/45, 1100 Wien, Österreich
FN 617186b, Handelsgericht Wien · UID ATU80014226
hallo@sadu.at

Ein Datenschutzbeauftragter ist bei SADU nicht bestellt. Ansprechpartner für alle Fragen aus diesem Vertrag ist die oben genannte Adresse.

---

§ 2 Gegenstand, Umfang und Dauer

SADU stellt dem Betrieb die Anwendung **Schichtanker** zur Arbeitszeiterfassung, Dienstplanung und Abwesenheitsverwaltung bereit und verarbeitet dabei personenbezogene Daten ausschließlich im Auftrag des Betriebs. Gegenstand, Art und Zweck der Verarbeitung, die Arten der Daten und die Kategorien betroffener Personen sind in Anlage 1 beschrieben.

Der Betrieb ist Verantwortlicher im Sinne von Art. 4 Z 7 DSGVO. Er entscheidet allein über Zwecke und Mittel der Verarbeitung der Daten seiner Beschäftigten und über deren Rechtsgrundlage und Aufbewahrung. SADU handelt ausschließlich auf seine Weisung.

Dieser Vertrag gilt für die Laufzeit des Nutzungsvertrags über Schichtanker und endet mit ihm. Eine gesonderte Kündigung ist nicht möglich, solange der Nutzungsvertrag besteht.

Die Daten werden in Rechenzentren innerhalb der Europäischen Union gespeichert. Soweit ein Unterauftragsverarbeiter seinen Sitz außerhalb der Union hat und ein Zugriff von dort nicht ausgeschlossen werden kann (Anlage 3), stützt sich dieser auf die Garantien des Kapitels V DSGVO, insbesondere auf Standardvertragsklauseln. Eine darüber hinausgehende Übermittlung in ein Drittland erfolgt nicht.

---

§ 3 Weisungen

SADU verarbeitet die Daten nur auf dokumentierte Weisung des Betriebs, einschließlich der Übermittlung in Drittländer, es sei denn, eine Rechtsvorschrift der Union oder eines Mitgliedstaats verpflichtet SADU zur Verarbeitung. In diesem Fall teilt SADU dem Betrieb diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Die Bedienung der Anwendung durch den Betrieb und die von ihm berechtigten Personen gilt als Weisung. Darüber hinausgehende Einzelweisungen erfolgen in Textform an hallo@sadu.at und werden von SADU dokumentiert.

Ist SADU der Ansicht, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen verstößt, teilt SADU dies dem Betrieb unverzüglich mit. SADU ist berechtigt, die Ausführung der Weisung bis zu deren Bestätigung oder Änderung auszusetzen.

---

§ 4 Pflichten von SADU

- **Vertraulichkeit.** SADU verpflichtet alle Personen, die zur Verarbeitung der Daten befugt sind, zur Vertraulichkeit, soweit sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung gilt über das Ende der Tätigkeit hinaus.

- **Sicherheit der Verarbeitung.** SADU ergreift die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und hält sie während der Vertragslaufzeit auf dem Stand der Technik. Maßnahmen dürfen angepasst werden, solange das Schutzniveau nicht unterschritten wird.
- **Unterstützung.** SADU unterstützt den Betrieb unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei der Einhaltung der Art. 32 bis 36 DSGVO, insbesondere bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen und bei einer Datenschutz-Folgenabschätzung.
- **Zweckbindung.** SADU verwendet die Daten des Betriebs nicht für eigene Zwecke, gibt sie nicht an Dritte weiter, außer an die in Anlage 3 genannten Unterauftragsverarbeiter, und wertet sie nicht zu Werbe- oder Profilbildungszwecken aus.
- **Berichtigung, Einschränkung, Löschung.** SADU berichtigt, löscht oder schränkt die Verarbeitung der Daten nur auf Weisung des Betriebs ein, soweit nicht dieser Vertrag oder eine gesetzliche Pflicht etwas anderes vorsieht.

---

§ 5 Pflichten des Betriebs

- Der Betrieb ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Rechtsgrundlage der Verarbeitung von Beschäftigtendaten, für die Information seiner Beschäftigten nach Art. 13 und 14 DSGVO und für die Einbindung einer allfälligen betrieblichen Interessenvertretung.
- Der Betrieb verwaltet die Zugänge in der Anwendung: Er legt Personen an, vergibt Rollen, entzieht Zugänge bei Austritt und ist dafür verantwortlich, dass nur berechtigte Personen Einsicht in Personaldaten erhalten.
- Der Betrieb entscheidet über Aufbewahrung und Löschung. Er berücksichtigt dabei gesetzliche Aufbewahrungspflichten, insbesondere für Arbeitszeitaufzeichnungen.
- Der Betrieb meldet SADU unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 6 Unterauftragsverarbeiter

Der Betrieb erteilt SADU die allgemeine Genehmigung, weitere Auftragsverarbeiter heranzuziehen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt und gelten mit Unterzeichnung als genehmigt.

SADU informiert den Betrieb über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters mindestens vier Wochen im Voraus in Textform. Der Betrieb kann der Änderung innerhalb von zwei Wochen ab Zugang aus einem wichtigen datenschutzrechtlichen Grund widersprechen. Widerspricht er, kann jede Partei den Nutzungsvertrag zum Zeitpunkt der beabsichtigten Änderung kündigen.

SADU legt jedem Unterauftragsverarbeiter dieselben Datenschutzpflichten auf, die in diesem Vertrag vereinbart sind, und haftet gegenüber dem Betrieb für deren Einhaltung.

§ 7 Rechte der betroffenen Personen

Wendet sich eine betroffene Person unmittelbar an SADU, leitet SADU das Anliegen unverzüglich an den Betrieb weiter und beantwortet es nicht selbst.

SADU unterstützt den Betrieb mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Betroffenenrechte nach Kapitel III DSGVO. Die Anwendung stellt dafür bereit:

- **Auskunft (Art. 15).** Für jede Person kann in der Personalakte ein vollständiges Datenpaket als Datei heruntergeladen werden; Beschäftigte können es über ihren eigenen Zugang selbst abrufen.
- **Berichtigung (Art. 16).** Stammdaten, Zeiten und Abwesenheiten sind im Betrieb änderbar; Änderungen an der Personalakte werden protokolliert.
- **Löschung (Art. 17).** Ein Löschantrag kann in der Anwendung aufgenommen werden. Kontakt- und Zugangsdaten werden in einem Schritt entfernt, Name und Zeitaufzeichnungen erst nach Ablauf der gesetzlichen Aufbewahrung durch Anonymisierung. Die Ausführung obliegt dem Betrieb.
- **Datenübertragbarkeit (Art. 20).** Zeitdaten stehen als Export zur Verfügung, das Auskunftspaket in maschinenlesbarer Form.

§ 8 Verletzungen des Schutzes personenbezogener Daten

SADU meldet dem Betrieb jede Verletzung des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden, spätestens innerhalb von 48 Stunden, in Textform an die vom Betrieb genannte Adresse. Die Meldung enthält, soweit bekannt, die Art der Verletzung, die betroffenen Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Maßnahmen.

Die Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO und die Benachrichtigung der betroffenen Personen nach Art. 34 DSGVO obliegen dem Betrieb. SADU unterstützt ihn dabei.

§ 9 Löschung und Rückgabe nach Vertragsende

Nach Beendigung des Nutzungsvertrags löscht SADU alle personenbezogenen Daten des Betriebs oder gibt sie nach dessen Wahl zurück. Der Betrieb teilt seine Wahl bis zum Ende des Vertrags mit; trifft er keine Wahl, werden die Daten gelöscht.

Der Betrieb kann seine Daten bis zum Ende des Vertrags jederzeit selbst exportieren. SADU räumt ihm dafür nach Vertragsende eine Frist von **30 Tagen** ein, in der die Daten vorgehalten und auf Anforderung herausgegeben werden. Nach Ablauf dieser Frist werden sie innerhalb von weiteren 30 Tagen gelöscht, einschließlich vorhandener Sicherungskopien.

Ausgenommen sind Daten, deren Aufbewahrung SADU nach dem Recht der Union oder eines Mitgliedstaats verpflichtet ist, sowie das Protokoll der Betreiberzugriffe nach Anlage 2, das den beschriebenen Vorgang überdauern muss. Dieses Protokoll enthält keine Namen und keine Inhalte aus dem Betrieb.

§ 10 Nachweise und Überprüfungen

SADU stellt dem Betrieb alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind, und ermöglicht Überprüfungen einschließlich Inspektionen.

Der Nachweis erfolgt vorrangig durch Auskunft in Textform. Eine Überprüfung vor Ort wird mit angemessenem Vorlauf von mindestens zwei Wochen angekündigt, findet während der üblichen Geschäftszeiten statt und darf den Betriebsablauf nicht unangemessen stören. Sie erfolgt höchstens einmal jährlich, es sei denn, ein konkreter Anlass rechtfertigt eine weitere Überprüfung.

---

§ 11 Haftung und Schlussbestimmungen

Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Nutzungsvertrags.

Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Das gilt auch für die Aufhebung dieses Formerfordernisses. Bei Widersprüchen zwischen diesem Vertrag und dem Nutzungsvertrag gehen die Regelungen dieses Vertrags vor, soweit sie den Datenschutz betreffen.

Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen. Zwingende Verbraucher- und Datenschutzbestimmungen des Sitzstaates des Betriebs bleiben unberührt.

Anlage 1 — Gegenstand der Verarbeitung

Zweck

Erfassung und Nachweis von Arbeitszeiten, Planung von Diensten und Wochen, Verwaltung von Urlaub und Abwesenheiten, Führung der Personalakte, Zugang der Beschäftigten zur Anwendung.

Art der Verarbeitung

Erheben, Erfassen, Speichern, Ordnen, Auslesen, Abfragen, Verwenden, Berichtigen, Einschränken, Löschen und Bereitstellen durch eine Webanwendung, ein Wandtablet und eine mobile App.

Kategorien betroffener Personen

Beschäftigte des Betriebs einschließlich Aushilfen und Lehrlingen, Führungskräfte und Inhaber als Nutzer der Anwendung sowie die von Beschäftigten angegebenen Notfallkontakte.

Stammdaten

Vor- und Nachname, Geburtsdatum, Anschrift, E-Mail-Adresse, Telefonnummer, Foto (sofern hinterlegt), Notfallkontakt.

Vertrags- und Einsatzdaten

Beschäftigungsart, Eintritts- und Austrittsdatum, Vertragsbeginn und -ende, vereinbarte und maximale Wochenstunden, Stundenlohn (sofern hinterlegt), Team, Rolle und Berechtigungsstufe, Verfügbarkeiten und Wünsche.

Zeit- und Planungsdaten

Stempelungen (Kommen, Pausenbeginn, Pausenende, Gehen) mit Zeitpunkt, Gerät und Herkunft, Korrekturen mit der handelnden Person, geplante Dienste, Wochenpläne und Notizen dazu.

Abwesenheiten

Urlaub, unbezahlte Abwesenheit und **Krankenstand** mit Zeitraum, Status und Notiz. Die Angabe eines Krankenstands ist ein Gesundheitsdatum im Sinne von Art. 9 Abs. 1 DSGVO. Die Anwendung speichert keine Diagnosen und keine ärztlichen Bescheinigungen.

Zugangsdaten

Passwort als argon2id-Hash, PIN ausschließlich als HMAC mit serverseitigem Geheimnis, Kennung des NFC-Chips, Gerätekennungen registrierter Tablets und Telefone, Sitzungsmerkmale als Hash.

Protokolle

Änderungsprotokoll der Personalakte mit altem und neuem Wert, Protokoll der Betreiberzugriffe, Versandprotokoll ausgehender E-Mails, Server- und Zugriffsprotokolle.

Dauer

Für die Laufzeit des Nutzungsvertrags, im Übrigen nach den Weisungen und Aufbewahrungsentscheidungen des Betriebs und nach § 9 dieses Vertrags.

Anlage 2 — Technische und organisatorische Maßnahmen

Maßnahmen nach Art. 32 DSGVO, Stand der oben genannten Fassung:

- **Vertraulichkeit — Zugangskontrolle.** Alle Zugriffe laufen über verschlüsselte Verbindungen (TLS) mit automatisch erneuerten Zertifikaten. Passwörter werden ausschließlich als argon2id-Hash gespeichert, PINs als HMAC mit einem serverseitigen Geheimnis, das getrennt von der Datenbank verwahrt wird. Eine gestohlene Datenbank gibt weder Passwörter noch PINs preis. Anmeldeversuche und Wiederherstellungsanfragen sind je Absender mengenmäßig begrenzt.

- **Vertraulichkeit — Mandantentrennung.** Die Daten jedes Betriebs sind in der Datenbank technisch getrennt. Die Trennung wird nicht von der Anwendung, sondern von der Datenbank selbst durchgesetzt (Row Level Security je Betrieb); eine Abfrage ohne gültigen Betriebskontext liefert keine Zeilen. Tabellen mit plattformseitigen Geheimnissen sind dem Anwendungskonto der Datenbank vollständig entzogen.
- **Vertraulichkeit — Zugriffskontrolle im Betrieb.** Rollen trennen Beschäftigte, Schichtleitung und Geschäftsführung. Personalakte, Lohnangaben und Datenschutzfunktionen sind der Geschäftsführung vorbehalten; eine Schichtleitung sieht sie nicht.
- **Transparenz — Protokollierung.** Änderungen an der Personalakte werden mit altem Wert, neuem Wert, handelnder Person und Zeitpunkt protokolliert. Jeder schreibende Zugriff des Betreibers in einen fremden Betrieb wird in einem eigenen, unveränderlichen Protokoll festgehalten, das aus dem Betrieb heraus nicht lesbar ist und keine Namen enthält.
- **Integrität — Eingabekontrolle.** Stempelungen werden nicht überschrieben; eine Korrektur entsteht als eigener Eintrag mit Herkunft und handelnder Person. Datenbankseitige Fremdschlüssel verhindern, dass Zeitaufzeichnungen ohne die zugehörige Person existieren oder mit ihr gelöscht werden.
- **Verfügbarkeit.** Die Datenbank liegt auf einem dauerhaften Speicher, der Neuveröffentlichungen der Anwendung übersteht. Eine Bereitschaftsprüfung, die bis zur Datenbank durchgreift, meldet einen nicht betriebsbereiten Zustand. Sicherungen werden derzeit manuell erstellt; eine geplante Sicherung mit Ziel außerhalb des Anwendungsservers und geprüfter Wiederherstellung ist in Umsetzung. Der Betrieb kann seine Zeitdaten jederzeit selbst exportieren.
- **Datenminimierung.** Fehlerberichte an den Dienstleister für Fehler-Tracking werden vor dem Versand um Namen, Mailadressen, Telefonnummern, Chip-Kennungen, Zugangsdaten und Abfragewerte bereinigt. Statistik und Sitzungsaufzeichnung sind einwilligungsgebunden und in Personal-, Abrechnungs- und Verwaltungsbereichen abgeschaltet.
- **Belastbarkeit und Überprüfung.** Die Anwendung wird durch eine automatisierte Testsuite abgesichert, die vor jeder Veröffentlichung läuft und unter anderem die Mandantentrennung, die Zugriffsrechte der Rollen und die Bereinigung der Fehlerberichte prüft. Datenbankänderungen werden vor der Veröffentlichung gegen Bestandsdaten erprobt.

Anlage 3 — Unterauftragsverarbeiter

Hetzner Online GmbH
Industriestraße 25, 91710 Gunzenhausen, Deutschland. Betrieb der Server und der Datenbank in einem Rechenzentrum in der Europäischen Union.

Brevo

Versand der E-Mails an Beschäftigte und Betriebsleitung (Einladung, Passwort setzen, Wiederherstellung). Empfänger- und Absenderadresse, Betreff und Inhalt der jeweiligen Nachricht.

Functional Software, Inc. (Sentry), EU-Region

Fehler-Tracking für den Betrieb der Anwendung. Es werden bereinigte technische Fehlerberichte übermittelt; Namen, Kontaktdaten, Chip-Kennungen und Zugangsdaten werden vor dem Versand entfernt.

PostHog, Inc., EU-Region

Nutzungsstatistik und Sitzungsaufzeichnung, ausschließlich nach ausdrücklicher Einwilligung der jeweiligen nutzenden Person und nur auf ausgewählten Seiten. Personal-, Abrechnungs- und Verwaltungsbereiche sind ausgenommen. Ohne Einwilligung findet keine Übermittlung statt.

Kein Unterauftragsverarbeiter im Sinne dieses Vertrags ist der Zahlungsdienstleister Stripe: Er verarbeitet die Abrechnungsdaten des Betriebs als Kunde von SADU. Dafür ist SADU selbst Verantwortlicher; Beschäftigtendaten werden ihm nicht übermittelt.

Unterschriften

Ort, Datum	Ort, Datum
Für den Betrieb (Verantwortlicher)	**Für SADU Development e.U.** (Auftragsverarbeiter)