

Technische und organisatorische Maßnahmen für MYSKILLFLOW (Anlage 1 zum AVV)

MYSKILLFLOW | Version 1.1 | Stand 18.10.2026

1. Gegenstand

Diese Anlage 1 zum AVV Version 1.2 beschreibt die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO für MYSKILLFLOW. Betreiberin ist Katharina Epp, MYSKILLBRIDGE, Ringstraße 27/1, 78244 Gottmadingen, hallo@myskillbridge.de. Die Maßnahmen berücksichtigen, dass auch Daten minderjähriger Auszubildender verarbeitet werden.

MYSKILLFLOW ist eine Next.js-Anwendung, die in Docker-Containern hinter dem Reverse Proxy Traefik auf einem virtuellen Server der netcup GmbH im Rechenzentrum Nürnberg betrieben wird. Datenbank, Authentifizierung und Dateispeicher werden von Supabase in der Region Central EU (Frankfurt) bereitgestellt. Zur Fehlerdiagnose wird Sentry mit EU-Datenregion eingesetzt. E-Mails werden über einen Mailserver von netcup versendet.

Für die physische Sicherheit der Rechenzentren, die Verschlüsselung der dort gespeicherten Daten und die Infrastruktursicherheit gelten ergänzend die technischen und organisatorischen Maßnahmen von netcup (ISO 27001), Supabase (SOC 2) und Sentry (ISO 27001, SOC 2) aus den mit ihnen geschlossenen Vereinbarungen.

2. Zutrittskontrolle

Die Server und Datenbanken befinden sich ausschließlich in den Rechenzentren der Unterauftragsverarbeiter, die Zutritt nach ihren zertifizierten Verfahren kontrollieren. MYSKILLBRIDGE betreibt keine eigenen Server.

Die lokale Sicherungsfestplatte wird in den Räumen der Inhaberin aufbewahrt und ist vollständig mit VeraCrypt verschlüsselt.

3. Zugangskontrolle

Benutzer melden sich mit E-Mail-Adresse und Passwort an. Passwörter werden von Supabase ausschließlich als Hashwerte gespeichert. Sitzungen werden über Cookies verwaltet und bei jeder Anfrage serverseitig geprüft; deaktivierte Benutzer und inaktive Unternehmen werden abgewiesen.

Benutzerkonten entstehen nur über Einladungen. Eine Einladung ist an eine E-Mail-Adresse, ein Unternehmen und eine Rolle gebunden und verfällt nach sieben Tagen. Die öffentliche Registrierung legt ausschließlich ein neues Unternehmen mit einer Ausbildungsleitung an; Rolle und Unternehmen werden serverseitig festgelegt und nicht aus der Anfrage übernommen.

Die Registrierung ist durch ein verstecktes Prüffeld, eine Mindestausfüllzeit und eine datenbankgestützte Begrenzung der Versuche je IP-Adresse und E-Mail-Adresse gegen automatisierten Missbrauch geschützt. Die Prüfwerte werden als SHA-256-Hashwerte gespeichert und nach einem Tag gelöscht.

Die Verwaltungszugänge zu netcup, Supabase, Sentry und zum Quellcode-Repository sind ausschließlich der Inhaberin zugänglich und durch starke, individuelle Passwörter und Zwei-Faktor-Authentifizierung geschützt. Der administrative Zugriff auf den Server erfolgt ausschließlich über SSH.

4. Zugriffskontrolle und Mandantentrennung

MYSKILLFLOW verwendet ein rollenbasiertes Berechtigungskonzept:

- Auszubildende sehen ihre eigenen Ausbildungsdaten.
- Ausbilderinnen und Ausbilder sehen die Daten der ihnen zugeordneten Abteilungen.
- Ausbildungsleitungen verwalten die Benutzer, Einladungen und Einstellungen des eigenen Unternehmens; Ausbildungsfortschritte sehen sie für die ihnen zur Betreuung zugeordneten Auszubildenden.
- Die Vertragsverwaltung erfordert eine gesonderte Freischaltung.
- Plattformadministration hat unternehmensübergreifende Rechte und ist ausschließlich der Inhaberin vorbehalten.

Die Trennung der Daten verschiedener Unternehmen wird in der Datenbank durch Row Level Security (PostgreSQL) und zusätzlich durch serverseitige Berechtigungsprüfungen in der Anwendung durchgesetzt. Fehlt eine Zuordnung, wird der Zugriff verweigert. Privilegierte Datenbankzugriffe sind auf serverseitige Funktionen beschränkt und prüfen Rolle und Zielunternehmen selbst.

Hochgeladene Dateien liegen in einem nicht öffentlichen Speicherbereich in unternehmensbezogenen Pfaden und sind nur über zeitlich begrenzte, signierte Links abrufbar (eine Stunde gültig). Dateityp und Dateigröße (höchstens 10 MiB) werden beim Hochladen geprüft. Kundenexporte liegen in einem gesonderten, nur für die Administration zugänglichen Speicherbereich.

5. Weitergabekontrolle

Sämtliche Verbindungen zwischen Browser, Anwendung, Supabase und Sentry sind per TLS (HTTPS) verschlüsselt; die Zertifikate werden automatisch erneuert. Der E-Mail-Versand an den netcup-Mailserver erfolgt verschlüsselt.

An Sentry wird im Benutzerfeld ausschließlich eine interne Kennung übermittelt. Vor der Übermittlung werden Cookies, Request-Header, Query-Strings, URL-Fragmente und Eingabewerte in Breadcrumbs entfernt; Sitzungsaufzeichnungen sind deaktiviert. Fehlermeldungen und technische Ereignisdaten können im Einzelfall dennoch personenbezogene Angaben enthalten; Sentry ist deshalb als Unterauftragsverarbeiter vertraglich eingebunden. Performancedaten werden stichprobenartig (10 %) erfasst.

Kundenexporte werden ausschließlich über einen zeitlich begrenzten, signierten Downloadlink an eine berechtigte Person übergeben.

6. Eingabekontrolle

Fachliche Änderungen innerhalb eines Kundenkontos, etwa das Anlegen von Benutzern, Rollenänderungen, Einladungen und Datei-Uploads, werden mit handelnder Person, Zeitpunkt und Zielobjekt protokolliert. Diese Protokolle sind für die Plattformadministration einsehbar. Bei Löschung des Kundenkontos werden Namen, E-Mail-Adressen, Dateinamen und weitere bekannte personenbezogene Felder entfernt; die verbleibenden pseudonymen Einträge werden drei Jahre nach Abschluss der Löschung gelöscht.

7. Verfügbarkeit und Wiederherstellbarkeit

Die Anwendung läuft in Docker-Containern und kann aus dem versionierten Quellcode jederzeit neu aufgebaut werden. Fehler werden über Sentry erfasst und gemeldet.

Im genutzten Supabase-Tarif werden keine Projektsicherungen durch Supabase bereitgestellt. MYSKILLBRIDGE sichert deshalb selbst, sobald Kundendaten gespeichert sind, mindestens einmal im Monat die Datenbank (Schema, Rollen und Daten) und die hochgeladenen Dateien auf die VeraCrypt-verschlüsselte lokale Festplatte. Zu jeder Sicherung werden Prüfsummen erstellt; sie dienen

der Kontrolle, dass die Sicherungsdateien unverändert und unbeschädigt sind. Es werden jeweils die beiden letzten Sicherungen aufbewahrt; ältere werden gelöscht. Nach einer Wiederherstellung werden alle seit der Sicherung durchgeführten Löschungen erneut angewendet.

Eine bestimmte Verfügbarkeit oder Wiederherstellungszeit wird nicht zugesichert.

8. Trennungskontrolle

Daten verschiedener Kunden werden logisch getrennt (siehe Abschnitt 4). Entwicklungs- und Testumgebungen verwenden keine Kundendaten. Eigene Vertrags- und Nachweisdaten von MYSKILLBRIDGE werden in gesonderten Tabellen geführt, auf die Kunden keinen Zugriff haben.

9. Löschung und Datenminimierung

Die Löschung erfolgt nach dem Lösch- und Aufbewahrungskonzept (Anlage 2). Ein täglicher automatischer Wartungslauf beendet abgelaufene Testzugänge und Verträge, plant die Löschung 30 Tage nach Test- oder Vertragsende, löscht nie aktivierte Registrierungen, nicht angenommene Einladungen und abgelaufene Nachweisdaten und erinnert die Betreiberin an fällige Kundenlöschungen.

Die Löschung eines Kundenkontos entfernt Dateien, Datensätze, Benutzer- und Authentifizierungskonten und Exportdateien schrittweise; fehlgeschlagene Schritte werden wiederholt, bis die Löschung vollständig ist. In Protokollen werden die bekannten personenbezogenen Felder entfernt; pseudonyme Restangaben werden nach Anlage 2 gelöscht.

Server- und Containerprotokolle werden nach 14 Tagen automatisch gelöscht. Fehlerdaten bei Sentry werden nach höchstens 90 Tagen automatisch gelöscht.

10. Organisatorische Maßnahmen

Die Inhaberin ist die einzige Person mit administrativem Zugriff auf Kundendaten. Sollten weitere Personen Zugriff erhalten, werden sie vorher schriftlich auf die Vertraulichkeit verpflichtet und erhalten nur die erforderlichen Rechte, die bei Wegfall des Zwecks entzogen werden.

Betriebssystem, Container und Abhängigkeiten werden regelmäßig aktualisiert. Änderungen an der Anwendung werden versioniert, vor der Auslieferung getestet und können auf den vorherigen Stand zurückgesetzt werden.

Bei einer Datenschutzverletzung wird der Vorfall eingedämmt, dokumentiert und der Kunde nach Abschnitt 8 des AVV unverzüglich informiert.

Diese Maßnahmen werden mindestens einmal jährlich sowie bei wesentlichen Änderungen der Anwendung oder der eingesetzten Dienstleister überprüft und angepasst.