Technisch-organisatorische Maßnahmen der Kickscale FlexCo

(nachfolgend die „**TOM**“)

Stand 05. Dezember 2025

1. Vertraulichkeit

Die Speicherung und Verarbeitung findet bei ausgewählten Providern in Rechenzentren statt, die hohe Sicherheits- und Verfügbarkeits- Standards garantieren. Kickscale stellt die Sicherheit der Daten durch eine sorgfältige Auswahl und regelmäßige Evaluierung dieser Subunternehmer sicher. Die eingesetzten Provider garantieren höchste Sicherheits- und Verfügbarkeitsstandards, die durch entsprechende Zertifizierungen (z. B. ISO 27001) sowie strikte DSGVO-Konformität und vertraglich zugesicherte Service Level Agreements (SLAs) belegt sind

Zutrittskontrolle: Der Auftragsverarbeiter verhindert den Zutritt nicht autorisierter Personen zu datenverarbeitenden Einrichtungen, mit/in denen personenbezogene Daten verarbeitet oder verwendet werden durch folgende Maßnahmen: Schlüssel, elektrische Türöffner

Datenspeicherung und physische Infrastruktur (Zutrittskontrolle) in den Rechenzentren:

Die Speicherung und Verarbeitung der Daten erfolgt in Rechenzentren spezialisierter Cloud-Provider (Subunternehmer). Da Kickscale keine eigenen Rechenzentren betreibt, wird die physische Zutrittskontrolle direkt durch die jeweiligen Betreiber ausgeübt.

Die durch die Subunternehmer implementierten Maßnahmen zur Zutrittskontrolle umfassen insbesondere:

- **Zutrittsschutz:** Verwehrung des Zutritts für nicht autorisierte Personen zu den datenverarbeitenden Einrichtungen durch bauliche und technische Barrieren (z. B. Sicherheitsschleusen, elektrische Türöffner, biometrische Zugangskontrollen oder Kartensysteme).
- **Zonierung:** Unterbringung der Serverräumlichkeiten in speziell gesicherten Sicherheitszonen innerhalb des Rechenzentrums.

- **Überwachung:** Lückenlose Videoüberwachung der Außenbereiche, Zugänge und Serverräume.
- **Protokollierung:** Ausschließlich namentlich autorisierte Personen erhalten Zutritt; jeder Zutritt wird elektronisch protokolliert und regelmäßig auditiert.

Zugangskontrolle: Der Auftragsverarbeiter verhindert die Nutzung von datenverarbeitenden Systemen durch nicht autorisierte Personen durch folgende Maßnahmen: sichere Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern, Remote-Zugriff über Virtual Private Network (VPN), SSH-Schlüssel

Zugriffskontrolle: Der Auftragsverarbeiter gewährleistet, dass Personen, die autorisiert sind, ein datenverarbeitendes System zu benutzen, nur auf diejenigen Daten Zugriff haben, zu denen sie zugelassen sind und dass weder bei der Verarbeitung noch nach der Speicherung personenbezogene Daten ohne entsprechende Autorisierung gelesen, kopiert, geändert oder entfernt werden können, durch folgende Maßnahmen: Berechtigungsprofile, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen soweit möglich und zulässig, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten.

In den Rechenzentren:

- **Berechtigungssystem** - es werden ausschließlich „named-User“ verwendet. Die Zugriffsberechtigungen werden jährlich auf deren Angemessenheit geprüft.
- Die Zugriffsberechtigungen ergeben sich aus den **Auftragsverarbeiterverträgen**.
- **Multi-Factor-Authentication** (MFA)
- **Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).**

Zwecktrennung: Der Auftragsverarbeiter gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten, insbesondere verschiedener Auftraggeber, getrennt verarbeitet werden können, durch folgende Maßnahmen: getrennte Speicherung und Verarbeitung von Daten nach Auftrag, Berechtigungskonzept, Minimalprinzip bei Berechtigungsvergabe.

2. Integrität

- Weitergabekontrolle: Der Auftragsverarbeiter gewährleistet, dass personenbezogene Daten ohne Genehmigung während der elektronischen Datenübertragung oder -speicherung nicht gelesen, kopiert, geändert oder entfernt werden können und dass es möglich ist, zu überprüfen und festzustellen, an welchen Stellen die Übertragung personenbezogener Daten mittels Datenübertragungseinrichtungen vorgesehen ist, durch folgende Maßnahmen: Verschlüsselung der Verbindung, VPN, elektronische Signatur
- Eingabekontrolle: Der Auftragsverarbeiter gewährleistet, dass es möglich ist, nachträglich zu prüfen und festzustellen, ob und durch wen personenbezogene Daten in Datenverarbeitungssysteme eingegeben, geändert oder entfernt worden sind, durch folgende Maßnahmen: Protokollierung, Dokumentenmanagement
- Durch das Führen eines „Secure-Logs“ oder durch die Protokollierung im Event-Log. Diese Log-Files dienen zur Erkennung einer rechtswidrigen Datenverwendung und zur Abwehr von Angriffen. Die Protokolle werden vom Chief Information Security Officer (CISO) entsprechend dem Auditplan geprüft.

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust von Daten durch:

- Backup-Systeme
- Virenschutz und Firewall
- Meldewege und Notfallpläne
- Security Checks auf Infrastruktur- und Applikationsebene
- Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern

Rasche Wiederherstellbarkeit: Maßnahmen zur schnellen Wiederherstellung nach Ausfällen

Löschungsfristen: Regelungen für Daten, Backups und Metadaten (z. B. Logfiles)

Verfügbarkeitskontrolle und Ausfallsicherheit (Availability Control)

Die Sicherstellung der ständigen Verfügbarkeit und Belastbarkeit der Systeme wird durch eine Kombination aus der hochverfügbaren Infrastruktur unserer zertifizierten Rechenzentrumspartner (Subunternehmer) und den internen Backup-Strategien von Kickscale gewährleistet.

Physische Infrastruktur (durch evaluierte Subunternehmer): Die eingesetzten Provider garantieren die Aufrechterhaltung des Betriebs durch folgende Maßnahmen, die regelmäßig nach **ISO 27001** auditiert werden:

- **Redundanz:** Vollredundante Auslegung des Rechenzentrumsbetriebs (N+1 oder höher), um Einzelausfälle (Single Points of Failure) auszuschließen.
- **Energieversorgung:** Unterbrechungsfreie Stromversorgung (**USV**) sowie Notstromaggregate für alle kritischen Serversysteme.
- **Klimatisierung:** Redundante Präzisionsklimatisierung zur Einhaltung optimaler Betriebstemperaturen und Vermeidung von Überhitzung.
- **Brandschutz:** Modernste Brand- und Früherkennungssysteme mit automatischer Alarmierung und direktem Einsatz von Löschsystemen.

Business Continuity: Vorhalten eines Notfallplans zur schnellen Systemwiederherstellung.

- Definierte Service-Level-Ziele: **RPO** (Recovery Point Objective) und ein **RTO** (Recovery Time Objective)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiterschulungen
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen
- Datenschutzfreundliche Softwareentwicklung (Privacy bei Design)
- Durchführung von Penetration Testing in regelmäßigen Intervallen
- Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters, Vorabüberzeugungspflicht, Nachkontrollen.

5. Supplementary Measures

Zusätzlich wurden die Standardvertragsklauseln durch weitere (begleitende) Zusicherungen und Klarstellungsmöglichkeiten seitens des US Sub Dienstleister ergänzt, um die die vom EuGH festgestellten Nachteile für das Datenschutzniveau auszugleichen.

- Pflicht zur Prüfung, ob staatliche Maßnahmen erforderlich sind.
- Verpflichtung, sich bis zur Ausschöpfung des Rechtsweges gegen den staatlichen Zugriff auf Daten von EU- Bürgern zu wehren.
- Verpflichtung zur Zahlung einer Vertragsstrafe bei schuldhafter Verletzung von Pflichten aus den Standardvertragsklauseln.