Technische und organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DSGVO, 2020 Audyem GmbH

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Kontrolle der Weitergabe
5. Kontrolle des Auftragsverarbeiters
6. Verfügbarkeitskontrolle
7. Trennungsgebot
8. Organisationskontrolle

1 — Zutrittskontrolle

Entfällt, da der Zugang zu unseren Systemen nicht ortsabhängig erfolgt. Alle Mitarbeiter können sich auch remote anmelden (siehe Sicherheitsvorkehrungen in Abschnitt 2).

2 — Zugangskontrolle

Wir betreiben unsere Systeme mit Amazon Web Services (AWS). Dabei existieren innerhalb unserer AWS Organisation hermetisch gegeneinander abgetrennte Nutzerkonten für a) den produktiven Betrieb unserer Software, b) die Staging-Umgebung und c) pro Mitarbeiter/Entwickler. Die produktive Umgebung unserer Clouddienste ist allein durch den Geschäftsführer und den CTO zugänglich und mit einem Multifaktor-Anmeldeverfahren gesichert. Nur in dieser produktiven Umgebung lagern personenbezogene Daten (personally identifiable information, PII).

3 — Zugriffskontrolle

Unsere kundenseitige Admin-Oberfläche (Self-Service Portal, SSP) erzwingt die Authentifizierung mit einem Hardware-Device oder Google Authenticator (Multifaktor-Authentifizierung, MFA). Einen Zugang zu den erhobenen PII über diese Weboberfläche gibt es derzeit jedoch nicht, die Daten werden an einen TLS-gesicherten Endpunkt des Kunden via Webhook übertragen.

4 — Kontrolle der Weitergabe

Wir stellen MFA-gesicherte Zugangsdaten für die Nutzerinnen unserer Produkte auf Mandantenebene zur Verfügung. Außerdem erinnern wir turnusmäßig daran, bestehende Passwörter zu erneuern. Dieser Vorgang erfolgt in der Regel alle 4 Wochen. Es kann ein verschlüsselter Dump der PII durch Mandanten angefordert werden. Wir übermitteln diesen wiederum ausschließlich signiert.

5 — Kontrolle des Auftragsverarbeiters

Wir beschäftigen in Deutschland ansässige Software-Entwickler auf Vertragsbasis. Abgesehen von unserem Leiter der Technik haben diese Entwickler keinen Zugriff auf die erhobenen PII. Wir beschäftigen keine Subunternehmen, abgesehen von Amazon/AWS gibt es keine dritten technischen Dienstleister, durch deren Systeme von uns erhobene PII fließen. Wir nutzen ausschließlich Server mit Standort innerhalb der EU (AWS Europe/Ireland).

6 — Verfügbarkeitskontrolle

Unsere Eventdaten werden sämlich auf einen nicht-öffentlichen Langzeit-Speicher abgelegt (S3 bzw. AWS Glacier) und können dort granular eingesehen oder gelöscht werden. AWS gewährleistet für diese Speicherklassen umfangreiche Sicherheitsstandards und Compliance-Zertifizierungen, darunter SEC Rule 17a-4, PCI-DSS, HIPAA/HITECH, FedRAMP, EU-DSGVO und FISMA.

7 — Trennungsgebot

Die Verarbeitung von PII erfolgt getrennt von Entwicklungssystemen, unsere Kundendaten werden separat von PII verarbeitet und in separaten Tables vorgehalten.

8 — Organisationskontrolle

Audits unserer Logs- und Zugriffe finden wöchentlich statt. Zudem setzen wir alle unsere Entwicklerkonten und -umgebungen alle zwei Wochen zurück bzw. überschreiben diese mit der neuesten Umgebungskonfiguration (infrastructure-as-a-service). So minimieren wir das Risiko offener Endpunkte oder Schnittstellen — auch wenn über diese keinesfalls PII zugreifbar sind (siehe oben). Bevor Updates in die produktive Umgebung ausgerollt werden, wird der betreffende Quellcode nach dem 4-Augen-Prinzip+ getestet und beurteilt.