Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

Die Locaboo/Ayunis betreibt Ihre Server (vgl. AVV Anlage 1) in zertifizierten Rechenzentren. Zertifikate und Beschreibungen der Sicherheitskonzepte können auf Anfrage gesondert bereitgestellt werden.

Es sind technisch-organisatorische Maßnahmen ergriffen worden, die ein angemessenes Datenschutzniveau und dessen Aufrechterhaltung gewährleisten:

a. Der Auftragsverarbeiter hat ein angemessenes Datenschutzmanagementsystem, bzw. ein Datenschutzkonzept implementiert und gewährleistet dessen Umsetzung.
b. Eine geeignete Organisationsstruktur für die Datensicherheit und Datenschutz ist vorhanden und die Informationssicherheit ist integriert in unternehmensweite Prozesse und Verfahren integriert
c. Es sind interne Sicherheitsricht- bzw. -leitlinien definiert, die unternehmensintern gegenüber Mitarbeitern als verbindliche Regeln kommuniziert werden.
d. Der Auftragsverarbeiter führt bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durch. Das Verfahren ist entsprechend dem PDCA-Zyklus aufgebaut und besteht aus einer kontinuierlichen Beobachtung der technischen und organisatorischen Maßnahme sowie Festlegung des Istzustandes, als auch des zu erreichenden Soll-Zustandes mit folgender Umsetzungs- und sich daran anschließenden Überprüfungsphase sowie Evaluierung der Umsetzung und Ableitung der gewonnenen Erfahrungen für künftige Optimierungen und Vorgehen im Hinblick auf die Sicherheitsstandards.
e. Es werden regelmäßig und auch anlasslos System- und Sicherheitstests, wie z. B. Code-Scan und Penetrationstests, durchgeführt.
f. Die technischen und organisatorischen Maßnahmen nach werden regelmäßig, mindestens jährlich, nach dem PDCA-Zyklus (Plan-Do-Check-Act) überprüft und angepasst.
g. Die Entwicklung des Standes der Technik und sowie der Entwicklungen, Bedrohungen und Sicherheitsmaßnahmen werden fortlaufend beobachtet und in geeigneter Art und Weise auf das eigene Sicherheitskonzept abgeleitet.
h. Es besteht ein Konzept, das die Wahrung der Betroffenenrechte durch den Auftraggeber gewährleistet (insbesondere im Hinblick auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche). Zu dem Konzept gehört die Unterrichtung der Mitarbeiter über die Informationspflichten gegenüber dem Auftraggeber, Einrichtung von Umsetzungsverfahren und die Benennung zuständiger Personen sowie regelmäßige Kontrolle und Evaluierung der ergriffenen Maßnahmen.
i. Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Gefährdungen und Verletzungen des Schutzes personenbezogener Daten gewährleistet. Zu dem Konzept gehört die Unterrichtung der Mitarbeiter über die Informationspflichten gegenüber dem Auftraggeber, Einrichtung von

Umsetzungsverfahren und die Benennung zuständiger Personen sowie regelmäßige Kontrolle und Evaluierung der ergriffenen Maßnahmen.

j. Sicherheitsvorkommnisse werden konsequent dokumentiert, auch wenn sie nicht zu einer externen Meldung (z. B. an die Aufsichtsbehörde, betroffene Personen) führen (sogenanntes "Security Reporting").
k. Konsultation und Einbindung des Datenschutzbeauftragten bei Sicherheitsfragen und in Sicherheitsverfahren, die den Schutz personenbetroffener Daten betreffen.
l. Ausreichende fachliche Qualifikation des Datenschutzbeauftragten für sicherheits-relevante Fragestellungen und Möglichkeiten zur Fortbildung in diesem Fachbereich.
m. Ausreichende fachliche Qualifikation des IT-Sicherheitsbeauftragten für sicherheits-relevante Fragestellungen und Möglichkeiten zur Fortbildung in diesem Fachbereich.
n. Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden (Wartungs-, Wach-, Transport- und Reinigungsdienste, freie Mitarbeiter, etc.), werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten. Sofern die Dienstleister im Rahmen ihrer Tätigkeit Zugang zu personenbezogenen Daten des Auftraggebers erhalten oder sonst das Risiko eines Zugriffs auf die personenbezogenen Daten besteht, werden sie speziell auf Verschwiegenheit und Vertraulichkeit verpflichtet.
o. Eingesetzte Software und Hardware wird stets auf dem aktuell verfügbaren Stand gehalten und Softwareaktualisierungen werden ohne Verzug innerhalb einer angesichts des Risikograd es und eines eventuellen Prüfnotwendigkeit angemessenen Frist ausgeführt. Es wird keine Software und Hardware eingesetzt, die von den Anbietern im Hinblick auf Belange des Datenschutzes- und Datensicherheit nicht mehr aktualisiert wird (z. B. abgelaufene Betriebssysteme).
p. Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen.
q. Eine Geräteverwaltung erlaubt die Bestimmung, welche Beschäftigten oder Beauftragten welche Geräte in welchen Bereichen einsetzen.
r. Es wird ein „papierloses Büro“ geführt, d. h. Unterlagen werden grundsätzlich nur digital gespeichert und nur in Ausnahmefällen in Papierform aufbewahrt.
s. Unterlagen im Papierformat werden nur dann aufbewahrt, wenn keine im Hinblick auf die Auftragsverarbeitung, ihrem Zweck und den Interessen der von den Inhalten der Unterlagen betroffenen Personen adäquate digitale Kopie vorliegt oder eine Aufbewahrung mit dem Auftraggeber vereinbart wurde oder gesetzlich erforderlich ist.
t. Es liegt ein den Datenschutzanforderungen der Auftragsverarbeitung und dem Stand der Technik entsprechendes Lösch- und Entsorgungskonzept vor. Die physische Vernichtung von Dokumenten und Datenträgern erfolgt datenschutzgerecht und entsprechend den gesetzlichen Vorgaben, Branchenstandards und dem Stand der Technik entsprechenden Industrienormen. Mitarbeiter wurden über gesetzliche Voraussetzungen, Löschfristen und soweit zuständig, über Vorgaben für die Datenvernichtung oder Gerätevernichtung durch Dienstleister unterrichtet.

u. Die Verarbeitung der Daten des Auftraggebers, die nicht entsprechend den Vereinbarungen dieses Auftragsverarbeitungsvertrages gelöscht wurden (z.B. in Folge der gesetzlichen Archivierungspflichten), wird im erforderlichen Umfang durch Sperrvermerke und/oder Aussonderung eingeschränkt.

Datenschutz auf Mitarbeiterebene:

Es sind Maßnahmen ergriffen worden, die gewährleisten, dass die mit personenbezogenen Daten beschäftigten Mitarbeiter über die datenschutzrechtlich nötige Sachkenntnis und Zuverlässigkeit verfügen.

1. Mitarbeiter werden auf Vertraulichkeit und Verschwiegenheit (Datengeheimnis) verpflichtet.
2. Mitarbeiter werden im Hinblick auf den Datenschutz entsprechend den Anforderungen ihrer Funktion sensibilisiert und unterrichtet. Die Schulung und Sensibilisierung werden, wenn es die Umstände erfordern, wiederholt.
3. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden (Home- und Mobile Office), werden Mitarbeiter über die speziellen Sicherheitsanforderungen sowie Schutzpflichten in diesen Konstellationen unterrichtet, sowie auf deren Einhaltung unter Vorbehalt von Kontroll- und Zugriffsrechten verpflichtet.
4. Die an Mitarbeiter ausgegebenen Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus den Diensten des Auftragsverarbeiters, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.
5. Mitarbeiter werden verpflichtet, ihre Arbeitsumgebung aufgeräumt zu hinterlassen und so insbesondere den Zugang zu Unterlagen oder Datenträgern mit personenbezogenen Daten zu verhindern (Clean Desk Policy).

Die nachfolgende Matrix beschreibt den Betrieb der SaaS-Plattformen, die sowohl die Anforderungen aus Art. 32 DSGVO als auch die Vorgaben des Cyber Resilience Act (CRA) berücksichtigen.

Kategorie	Maßnahmen (DSGVO + CRA)
1. Zutrittskontrolle	- Gesicherte Rechenzentren (ISO 27001) - Zugang nur für autorisierte Personen - Besucherprotokollierung
2. Zugangskontrolle	- MFA für alle Benutzer - Rollenbasierte Rechte - Passwort-Policy (kein Default) - CRA: Secure by Default
3. Zugriffskontrolle	- Least-Privilege-Prinzip

	- Logging aller Zugriffe - CRA: Zero-Trust-Architektur
4. Weitergabekontrolle	- TLS 1.3 für alle Datenübertragungen - VPN für interne Admin-Zugriffe - CRA: Verschlüsselung „in transit“
5. Eingabekontrolle	- Audit-Logs für Änderungen - Vier-Augen-Prinzip bei kritischen Prozessen
6. Auftragskontrolle	- AVV mit Subunternehmern - Prüfung auf DSGVO- und CRA-Konformität
7. Verfügbarkeitskontrolle	- Georedundante Backups - Disaster-Recovery-Tests - CRA: Nachweis Resilienz gegen Cyberangriffe
8. Trennungskontrolle	- Mandantenfähigkeit - Logische Datenisolierung - CRA: SBOM für eingesetzte Komponenten
9. Schwachstellenmanagement	- Regelmäßige Penetrationstests - Patch-Management - CRA: Koordinierte Schwachstellenmeldung (CVD)
10. Monitoring & Logging	- SIEM-System für Echtzeitüberwachung - CRA: Meldung von Sicherheitsvorfällen an zentrale Plattform
11. Datenschutzmaßnahmen	- Pseudonymisierung & Verschlüsselung personenbezogener Daten - Privacy by Design
12. Organisatorische Maßnahmen	- Schulungen zu DSGVO & Informationssicherheit - Sicherheitsbeauftragter im DevOps-Prozess - CRA: CE-Konformitätsdokumentation