Technische und Organisatorische Maßnahmen (Art. 32 DSGVO)

1. Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a)

- Data Masking der Authentifizierungsdaten (Passwort-Hashing)
- Data At Rest Encryption
    - Verschlüsselung der Datenbank durch AWS (Amazon Web Services) data encryption nach Industriestandard AES-256 (Advanced Encryption Standard)
- Data In Transit Encryption
    - Datentransfers ausschließlich über Verschlüsselung durch TLS (Transport Layer Security) nach dem Stand der Technik
- Key-Management durch AWS KMS key management für Amazon RDS (Relational Database Service)
- Personenbezogene Identifikationsmerkmale werden endgültig gelöscht

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b)

- Double-Opt-In im Registrierungsverfahren in der Plattform (begrenzt gültiger Aktivierungslink)
- Die Login-Seiten sind gegen Brute-Force-Attacken geschützt
- Zutrittskontrolle
    - Bürogebäude
        - Alle Türen sind abschließbar und können von nur von Mitarbeitern
        - mithilfe einer Chipkarte betreten werden
        - Es existiert eine Schlüsselregelung
        - Alle Daten werden ausschließlich auf digitalen Datenträgern (Laptops)
        - verarbeitet und gespeichert, es besteht somit für Besucher und Gäste
        - kein physischer Zugang zu auf Papier gespeicherten personenbezogene Daten
        - elektronische Geräte wie Laptops besitzen einen Auto-Logout
    - Rechenzentrum
        - Endkundendaten werden in Rechenzentren von AWS verarbeitet und gespeichert
        - die von AWS Frankfurt getroffenen technischen und organisatorischen Maßnahmen finden Sie in unserer Subunternehmerliste – im Folgenden zu finden unter der URL https://sevdesk.de/datenschutz
- Datenträgerkontrolle
    - Aktenvernichtung (mindestens Stufe 3)
    - Vermeiden von nicht geschützten Datenträgern (Papier, …)
    - Verschlüsselung von digitalen Datenträgern
    - digitale Datenträger wie Laptops sind durch ein starkes Passwort geschützt

- Speicherkontrolle
    - Clean Desk Policy
    - Trennung des WLAN in intern und öffentlich
    - Es wird ein Passwort zur WLAN-Authentifizierung genutzt
    - Passwort-Mindestlänge von 12 Zeichen
    - Richtlinie für den Umgang mit Passwörtern
    - Es existieren technische Maßnahmen zur Umsetzung der Passwortrichtlinie
- Zugriffskontrolle
    - Ein Berechtigungskonzept ist vorhanden, um Benutzerrechte zu verwalten
    - Unterschiedliche Zugriffsberechtigungen bzgl. Lesen, Schreiben und Löschen von Daten
    - Betriebliche Anweisung zum Umgang mit mobilen Datenträgern
    - Anzahl der Administratoren auf das “Notwendigste“ reduziert
    - Externe Wartung und Fernwartung - Regelungen und Kontrollen
    - Schutz gegen unberechtigte interne und externe Zugriffe durch eine Firewall besteht
    - Zugriff auf interne Dienste aus einem externen Netz sind nur durch ein VPN möglich
- Benutzerkontrolle
    - Mitarbeiter-Schulungen zum Thema Datenschutz
    - Verpflichtung der Mitarbeiter auf die Vertraulichkeit
- Trennbarkeit
    - Trennung in Test-, Produktions-und Entwicklungsebene
    - getrennte Verarbeitung zweckgebundener Daten
    - Mandantenfähigkeit

3. Integrität (Art. 32 Abs. 1 lit. b)

- Datenintegrität
    - Regelmäßige Software-Updates
    - Virenschutz des Netzwerkes und der IT-Systeme
- Weitergabekontrolle
    - Soweit Daten über das Internet übertragen werden, sind diese Datenübertragungskanäle immer TLS verschlüsselt
    - Wo dies technisch möglich ist, kommen VPN-Verbindungen zum Einsatz
    - Personaldokumente oder sonstige Informationen werden verschlüsselt versendet
- Wiederherstellbarkeit
    - Wiederherstellbarkeit wird durch den Clouddienstleister AWS gewährleistet, vgl. Technische und organisatorische Maßnahmen von AWS Frankfurt in unser Subunternehmerliste
- Auftragskontrolle
- Auswahl der Auftragnehmer unter Sorgfalt-Gesichtspunkten (Zertifizierung, Referenzen, usw.)

- Eindeutige Vertragsgestaltung
- Klare Anweisungen an den Auftragnehmer hinsichtlich des Umfangs der Verarbeitung personenbezogener Daten.
- Soweit eine Datenverarbeitung im Auftrag durchgeführt wird, wird der Auftragnehmer vor Aufnahme der Datenverarbeitung nach den Vorschriften der DSGVO auf die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen überprüft. Über jeden Auftrag wird ein Vertrag nach den Vorschriften der Datenschutz-Grundverordnung abgeschlossen. Dies gilt auch für Verträge über Wartungsarbeiten an den Datenverarbeitungssystemen und Softwarepflege je nach Bedarf und sonstige IT Service-Unterstützung, wenn dabei ein Zugriff auf personenbezogenen Daten nicht ausgeschlossen werden kann. Bei der Überprüfung der Auftragnehmer und der Vergabe von Aufträgen im Rahmen einer Datenverarbeitung im Auftrag wird unser Datenschutzbeauftragter hinzugezogen.

4. Verfügbarkeit (Art. 32 Abs. 1 lit. b)

- Im Rahmen der SAAS Dienstleistung ist das Rechenzentrum nach ISO/IEC 27001:2013 zertifiziert
- die von AWS Frankfurt getroffenen technischen und organisatorischen Maßnahmen finden Sie unter dem folgenden Link: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf