Allgemeine technische und organisatorische Maßnahmen

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

GRUNDSÄTZE

Die Anwendungen der samedi GmbH werden im Rechenzentrum der filoo GmbH in Frankfurt / Main gehostet. Mit dem Zusatz [RZ] gekennzeichnete Maßnahmen gelten nur für das Rechenzentrum der filoo GmbH, nicht für die Büroräume der samedi GmbH. Maßnahmen, die nur für die Büroräume der samedi GmbH gelten, sind mit dem Zusatz [SA] gekennzeichnet.

1 Vertraulichkeit

Zutrittskontrolle

- [SA] samedi® nutzt das vorhandene Sicherheits-Schließsystem des Vermieters.
- [SA] Zugang zum Gebäude und den Büroräumen jeweils nur mit Schlüsselkarte möglich.
- [SA] Besucher befinden sich stets in Begleitung eines samedi®-Mitarbeiters und haben zu keinem Zeitpunkt Zugang zu datenverarbeitenden Prozessen.

- [RZ] Separate Räumlichkeiten nur Befugten und anderen Personen in Begleitung zugänglich.
- [RZ] Abschließbare Räumlichkeit, ein Schlüssel nur bei filoo-Techniker und für Notfälle ein weiterer beim Rechenzentrumsbetreiber, verschlossen außerhalb von Geschäftstätigkeiten.
- [RZ] Schlüssel müssen an der Pforte bzw. am Leitstand beantragt werden.
- [RZ] Zugang zu den Häusern ist durch eine Pforte und eine Durchgangsschleuse gesichert.
- [RZ] Zugang zu Gebäuden, Zugang zu den jeweiligen Etagen und Zugang zu Käfigen jeweils nur mit Schlüsselkarte vom Rechenzentrum möglich.
- [RZ] Jeder Besucher bekommt seine eigene Schlüsselkarte für Tracking.
- [RZ] Der Leitstand des Rechenzentrums ist 24 Stunden am Tag, 7 Tage die Woche durchgehend besetzt. Auf dem Gelände werden regelmäßige Kontrollgänge durchgeführt. Des Weiteren ist das gesamte Gelände mit Kameras überwacht. Alle Türen sind mit Kartenlesern ausgestattet welche den Zugang zu den entsprechenden Bereichen ermöglichen.
- [RZ] Von den Kartenlesern werden entsprechende Zugangsnachweise angefertigt. Eine EMA ist an sämtlichen Zugängen vorhanden und auf den zentralen Werkschutz geschaltet.
- [RZ] Jeder Zutritt in die Serverräumlichkeiten wird protokolliert und kann durch Schlüsselkarte nachverfolgt werden.

Technische und Organisatorische Maßnahmen (Stand 06/2018)
samedi GmbH, Rigaer Strasse 44, 10247 Berlin

Zugangskontrolle

- [SA] Der Zugang zu Datenverarbeitungssystemen ist nur autorisierten Mitarbeitern möglich.
- [SA] Es besteht ein verbindliches Verfahren zur Vergabe von Berechtigungen.
- [SA] Es besteht eine eindeutige Zuordnung von Benutzerkonten zu Benutzern.
- [SA] Jeder Mitarbeiter der samedi GmbH muss sich mit persönlicher Benutzerkennung und Passwort authentifizieren.
- [SA] Es bestehen verbindliche Vorgaben für die Passwortqualität (Mindestlänge 8 Zeichen, muss Sonderzeichen, Zahlen und Groß-/Kleinschreibung enthalten).
- [SA] Sperrung des Benutzerkontos nach drei fehlgeschlagenen Anmeldeversuchen.
- [SA] Automatisches Logout nach inaktiver Zeit.
- [SA] Manuelles Auslösen einer Passwort-Änderung durch Administrator.
- [SA] Kontrolle des Zugriffs einzelner Benutzer durch Einschränkung von IP-Adressen.
- [SA] Automatische, passwortgeschützte Bildschirm- und Rechnersperre.
- [SA] Verbindliches Verfahren zur Rücksetzung „vergessener“ Passwörter.
- [SA] Richtlinie zum sicheren, ordnungsgemäßen Umgang und Änderung von Passwörtern.
- [SA] Daten der samedi®-Plattform sind mehrfach gesichert:
    - Authentifizierung am System durch sichere Passwörter
    - Datenübertragung über eine TLS-gesicherte Verbindung
    - Festplattenverschlüsselung
    - Daten, die der Schweigepflicht unterliegen, werden auf Basis asymmetrischer (2048 Bit RSA) und symmetrischer (256 Bit AES-CBC) Algorithmen verschlüsselt. Die Schweigepflicht wird somit nicht durchbrochen.
- [SA] Es wird gewährleistet, dass niemand, der physischen Zugriff auf die Serversysteme hat, die Kennwörter und Zugangsdaten zu den Systemen erhält.
- [SA] Rechner und Serversysteme sind nur mit Passwort und über passwortgeschützte, verschlüsselte Verbindung durch Benutzer mit Administratorrechten nutzbar.
- [SA] Die Systeme sind durch Firewalls und entsprechend gehärtete Konfigurationen aller Systemkomponenten gegen unbefugten Zugriff von außen abgesichert. Regelmäßige Updates der Software-Komponenten werden durch die Administratoren durchgeführt, überwacht und automatisiert auf die Server verteilt.
- [SA] Zum Schutz vor unbefugtem Datenzugriff sind auch die Festplatten der Datenbankserver AES-verschlüsselt, mit einer Schlüssellänge von 256 Bit. Dadurch können die DB-Server ohne Kenntnis des Festplattenkennworts nicht hochgefahren werden. Das Kennwort selbst ist nur den Administratoren der Server bekannt.

Technische und Organisatorische Maßnahmen (Stand 06/2018)
samedi GmbH, Rigaer Strasse 44, 10247 Berlin

Zugriffskontrolle

- [SA] Die Zugriffskontrolle wird administrativ durch ein verbindliches Berechtigungskonzept für alle Bereiche (z.B. Produktions-Server, Domäne, abhängige Berechtigungen, Firewall, VPN- und Internetzugänge) gewährleistet.
- [SA] Die Rechtevergabe erfolgt nur in dem Rahmen, der in Abhängigkeit von der Tätigkeit erforderlich ist.
- [SA] Zugriff auf die Anwendungs- und Datenbankserver haben nur einzelne, durch die samedi® GmbH bestimmte und entsprechend qualifizierte Mitarbeiter.
- [SA] Zugriffe auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten, werden protokolliert.
- [SA] Bei Austritt eines Mitarbeiters werden unverzüglich dessen Zugangsberechtigungen gesperrt bzw. gelöscht.
- [SA] Passwörter werden nach Benutzergruppen getrennt in geschützten Passwortcontainern gespeichert.
- [SA] Es besteht eine Richtlinie zur sicheren, ordnungsgemäßen Erstellung, dem Umgang mit und der Änderung von Passwörtern.
- [SA] Elektronische Datenträger werden ihrer Art nach so gelöscht oder vernichtet, dass keine Daten rekonstruiert werden können.
- [SA] Einsatz von Aktenvernichtern mit Partikelschnitt.

Trennung

- [SA] Es besteht ein verbindliches Verfahren zur Vergabe von Berechtigungen.
- [SA] Die in verwendeten Systemen verfügbaren Berechtigungsmechanismen ermöglichen die exakte Umsetzung der Vorgaben des Berechtigungskonzeptes.
- [SA] Es besteht eine eindeutige Zuordnung von Benutzerkonten zu Benutzern.
- [SA] Trennung von Produktiv- und Testsystemen.
- [SA] Separate Tables innerhalb von Datenbanken in Abhängigkeit von der Art der Daten.
- [SA] Getrennte Datenbanken in Abhängigkeit vom Anwendungszweck.
- [SA] Logische Mandatentrennung (softwareseitig).

Pseudonymisierung & Verschlüsselung

- [SA] Die elektronische Übermittlung von Daten wird durch gängige Verschlüsselungstechnologien, VPN und Firewall geschützt.
- [SA] Daten der samedi®-Plattform sind mehrfach gesichert:
    - Datenübertragung über eine TLS-gesicherte Verbindung
    - Daten, die der Schweigepflicht unterliegen werden zusätzlich vor der Übertragung auf Basis asymmetrischer (2048 Bit RSA) und symmetrischer (256 Bit AES-CBC) Algorithmen verschlüsselt.

2 Integrität

Eingabekontrolle

- [SA] Es besteht eine eindeutige Zuordnung von Benutzerkonten zu Benutzern.
- [SA] Jeder Mitarbeiter muss sich mit persönlicher Benutzerkennung und Passwort authentifizieren.
- [SA] Bei Dateneingabe erfolgt in vielen Fällen eine Plausibilitätsprüfung der zu speichernden Daten.

Weitergabekontrolle

- [SA] Eine Weitergabe der verarbeiteten Daten findet nur im vereinbarten Maße an namentlich bekannte und dafür berechtigte Personen statt.
- [SA] Systemzugriffe werden automatisiert geloggt.
- [SA] Die elektronische Übermittlung von Daten wird durch gängige Verschlüsselungs-technologien, VPN und Firewall geschützt.
- [SA] Daten der samedi®-Plattform sind mehrfach gesichert:
    - Datenübertragung über eine TLS-gesicherte Verbindung
    - Daten, die der Schweigepflicht unterliegen werden auf Basis asymmetrischer (2048 Bit RSA) und symmetrischer (256 Bit AES-CBC) Algorithmen verschlüsselt.

3 Verfügbarkeit und Belastbarkeit

- [SA] Alle essentiellen Komponenten der Server, also sowohl Hard- als auch Software, sind redundant ausgelegt, um einen Single Point Of Failure zu vermeiden. Dazu gehören:
    - Netzteile
    - Festplatten (RAID-1 bei den Anwendungsservern, RAID-5 bei den Datenbankservern)
    - Load-Balancer
    - Server-Typen (mind. Ja 2 Anwendungs- und Datenbankserver)

- [SA] Vollständiges Backup- und Recovery-Konzept mit täglicher automatisierter Sicherung der Datenträger.
- [SA] Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramm, SPAM-Filter) und schriftliche Konzeption ihres Einsatzes.
- [SA] Automatisierte Standartroutinen für regelmäßige Aktualisierung von Schutzsoftware (z.B. Virenscanner).
- [SA] Es existiert ein mehrstufiges Backup-Konzept (on-site/off-site)

- [RZ] Die Telehouse-Gebäude sind mit modernster Brandmeldetechnik, Brandfrüherkennungssystemen, automatisierter Löschtechnik, Überspannungsschutz, Klimaanlage ausgestattet.
- [RZ] Zur Vermeidung von Fehlauslösungen, bzw. Ansprüchen auf Kostenerstattung unterliegen

alle Benutzer (Kunden, Fremdfirmen, Betreiber usw.) bestimmten Verhaltensregeln.

- [RZ] Die filoo GmbH stellt eine unterbrechungsfreie Stromversorgung (USV) und Notstrom-aggregate zur Verfügung.

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- [SA] Es gibt eine klare Vertretungsregelung der Geschäftsleitung.
- [SA] Es erfolgen regelmäßige Schulungen der Mitarbeiter zum Datenschutz (Einzel-/Gruppenschulung bei Arbeitsantritt; ansonsten jährlich); Schulungsnachweise liegen vor.
- [SA] Nachweise über die Verpflichtung auf das Datengeheimnis sind vorhanden.
- [SA] Nachweise über die Verpflichtung zur Wahrung von Geschäfts- und Betriebsgeheimnissen (§17 UWG) sind vorhanden.
- [SA] Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit Dr. med. Tobias Wauschkuhn (Email: datenschutz@samedi.de; Tel.: 030-212307072) benannt.
- [SA] Nachweise über die Fachkunde des Datenschutzbeauftragten liegen vor.
- [SA] Es bestehen unternehmensweite Richtlinien für die Mitarbeiter zum Umgang mit personenbezogenen Daten.
- [SA] Ein Prozess zur Gewährleistung der Meldepflichten bei Datenschutzverletzungen wurde im Unternehmen implementiert.
- [SA] Ein Prozess zur Durchführung von Datenschutz-Folgenabschätzungen wurde etabliert.
- [SA] Ein Verzeichnis von Verarbeitungstätigkeiten ist vorhanden, vollständig und aktuell.
- [SA] Ein Datenschutzmanagementsystem (DSMS) wurde implementiert.
- [SA] Regelmäßige Überprüfung der Einhaltung der Datenschutzbestimmungen durch eine externe, unabhängige Firma (derzeit: TÜV Saarland; Zertifikat „Geprüfter Datenschutz“ vom 21.12.2017).

- [RZ] Zertifizierung des Rechenzentrums nach ISO:27001 (vom 30.08.2016).