

## 1 Datensicherheit

### 1.1 Eingesetzte Techniken und Schnittstellen

Web SARA wird unter Verwendung von ASP.NET Core und Angular.JS (PAUL) entwickelt. Alle Schnittstellen werden regelmäßig aktualisiert, um potenzielle Sicherheitslücken zu minimieren.

### 1.1 Server Standorte

#### Unsere Serverstandorte:

Sämtliche Server die von uns genutzt und für die Anwendungen zur Verfügung gestellt werden liegen ausschließlich in Deutschland bei unseren Dienstleistern (Freiburg, Nürnberg oder Falkenstein). Die Standorte sind jeweils gemäß ISO 27001 zertifiziert.

#### PAUL:

Die Datenbanken von PAUL werden auf einem PostgreSQL-Server betrieben (Nürnberg).

#### Web SARA

Datenbanken:

Die Datenbanken im Testbetrieb, werden auf einem MS-SQL-Server betrieben (Nürnberg). Die Datenbanken im Produktivbetrieb (bei Kauf), werden auf einem MS-SQL-Server betrieben (Freiburg).

Anwendung:

Die Anwendung von Web SARA wird je nach Bedarf in einem von unseren Dienstleistern betriebenen Rechenzentrum gehostet.

Dienstleister:

Alle externen Dienstleister, die Rechenzentren verwalten bzw. bereitstellen, sind ebenfalls nach ISO 27001 zertifiziert (Continum, Netcup und Hetzner).

### 1.2 Verschlüsselungen

Unsere Anwendungen nutzen die branchenüblichen Maßnahmen zur Sicherung der Daten, einschließlich Verschlüsselung, Firewalls und Secure Sockets Layer (SSL).

Als Verschlüsselung dient ein SHA-256 mit RSA-Verschlüsselungs-Algorithmus.



## 1.3 Backups

Es werden täglich, wöchentlich sowie monatlich Datenbackups erzeugt. Die Sicherungskopien werden separat aufbewahrt.

### **Backups – Zeitfenster und gesicherte Übertragung**

Die Backups werden ausschließlich in einem kurzen, festgelegten Zeitfenster in der Nacht erstellt. Nach Abschluss der Datensicherung werden die Backup-Server/Systeme automatisch vom Netzwerk getrennt und sind somit nicht mehr erreichbar. Die Übertragung der Daten erfolgt dabei über eine sichere, verschlüsselte Kommunikationsverbindung

### **Physische und logische Isolation:**

Die Sicherungskopien werden in separaten, isolierten Speichersystemen aufbewahrt, die nicht direkt mit dem primären Produktionssystem verbunden sind. Diese Trennung minimiert das Risiko, dass Angreifer, die in das Hauptsystem eindringen, auch auf die Backups zugreifen können.

## 1.4 Zugänge und Passwörter

Jeder Zugang ist durch ein 256-Bit-Passwort geschützt und ermöglicht ausschließlich den Zugriff auf die entsprechenden Datenbestände des jeweiligen Nutzers. Ein unbeabsichtigter Zugriff eines Kunden auf eine andere Datenbank ist somit ausgeschlossen. Optional kann eine Zwei-Faktor-Authentifizierung (2FA) aktiviert werden, um den Zugang zusätzlich vor unbefugtem Zugriff zu schützen.

## 1.5 Zugriffskontrolle

Die Webanwendung verfügt über ein umfassendes Berechtigungskonzept, das es ermöglicht, verschiedenen Benutzern unterschiedliche Lese- und Schreibrechte zuzuweisen. Diese Berechtigungen können jederzeit flexibel angepasst werden

## 1.6 Umgang mit Daten nach Kündigung

Nach der Kündigung werden alle bei uns gespeicherten Daten standardmäßig für ein Jahr aufbewahrt und anschließend gelöscht.

Auf Kundenwunsch kann die Löschung auch kundenspezifisch oder früher erfolgen. Zusätzlich bieten wir nach der Kündigung die Möglichkeit, die Daten in Form von CSV-Dateien oder SQL-kompatiblen Datenbank-Dateien kostenlos zur Verfügung zu stellen.

Die Daten werden als passwortgeschützte ZIP-Datei per Downloadlink zur Verfügung gestellt, der für einen Monat gültig ist. Alternativ können die Daten auch über ein vom Kunden bereitgestelltes System ausgetauscht werden.



## 2 (DSGVO) Technische-organisatorische Maßnahmen

### 2.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

**Zutrittskontrolle:** Kein unbefugter Zutritt zu Datenverarbeitungsanlagen: Schlüssel / Schlüsselvergabe

**Zugangskontrolle:** Keine unbefugte Systembenutzung: Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts) Einrichtung eines Benutzerstammsatzes pro User

**Zugriffskontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems: Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)

**Trennungskontrolle:** Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden. Sowie einzelne Datenbanken für unterschiedliche Daten und Kunden.

### 2.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

**Weitergabekontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport: Verschlüsselung (HTTPS, SSL – SHA256), Protokollierung

**Eingabekontrolle:** Erfassung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind: Protokollierung, Dokumentenmanagement

### 2.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

**Verfügbarkeitskontrolle:** Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust: Backup-Strategie, unterbrechungsfreie Stromversorgung (USV) Virenschutz, Firewall Meldewege und Notfallpläne

Rasche **Wiederherstellbarkeit** (Art. 32 Abs. 1 lit. c DSGVO)

**Standort** der unternehmenseigenen Server und des Rechenzentrums befinden sich in Deutschland

### 2.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Datenschutz-Management

Incident-Response-Management

**Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DSGVO)

**Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

