QUMsult
GmbH & Co. KG

WebSARA

EHS-Software - Umwelt, Gesundheit, Sicherheit

Datenschutz / -sicherheit

QUMsult GmbH & Co. KG
Eisenbahnstraße 41
D-79098 Freiburg

Tel 07 61 / 2 92 86-10
E-Mail info@qumsult.de
Internet www.qumsult.de

1 Datensicherheit

1.1 Eingesetzte Techniken und Schnittstellen

Web SARA wird nach aktuellem Stand der Technik in ASP.Net Core programmiert. Alle Schnittstellen werden auf aktuellem Stand gehalten, um Sicherheitslücken zu minimieren.

1.2 Server Standorte

Die Datenbanken werden in einem MS SQL-Server gespeichert. Die Daten sind physikalisch in einem nach ISO 27001-zertifizierten Rechenzentrum in Nürnberg abgelegt.

1.3 Verschlüsselungen

Web SARA nutzt 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.

1.4 Backups

Es werden regelmäßig (täglich/wöchentlich/monatlich) Daten-Backups erzeugt und auf getrennte Aufbewahrung dieser Backup-Daten geachtet.

1.5 Zugänge und Passwörter

Die einzelnen Zugänge haben ein 256Bit – Passwort und können nur auf die jeweils eigenen Datenbestände zugreifen. Ein versehentlicher Zugriff von einem Kunden auf eine andere Datenbank ist somit ausgeschlossen. Optional kann eine Zwei-Faktor-Authentisierung(2FA) aktiviert werden und den Zugang zusätzlich vor unbefugtem Zugriff schützen.

1.6 Zugriffskontrolle

Die Webanwendung verfügt über ein Berechtigungskonzept. Es können Benutzer mit verschiedenen Lese- und Schreibrechten vergeben und jederzeit angepasst werden.

1.7 Umgang mit Daten nach Kündigung

Alle bei uns gespeicherten Daten werden mit einer Frist von 1 Jahr nach Kündigung noch ein Jahr aufbewahrt und anschließend gelöscht.
Auf Nachfrage kann die Löschung auch kundenspezifisch bzw. früher erfolgen.

Des Weiteren können auf Wunsch nach Kündigung die Daten als CSV-Dateien oder SQL-kompatible Datenbank-Dateien ohne Zusatzkosten zur Verfügung gestellt 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: Feststellung, 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.