QUMsult
GmbH & Co. KG

WebSARA
EHS-Software - Umwelt, Gesundheit, Sicherheit

Data security

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

Zertifiziertes Managementsystem
ISO 9001:2015
ISO 14001:2015

1 Data security

1.1 Technology and interfaces in use

Web SARA is developed according to the latest state of the art. All interfaces are kept up to date in order to minimize vulnerabilities.

1.2 Location of servers

The databases are stored on a MS SQL-Server. All data is located in ISO 27001 certified data centers in Nürnberg and Freiburg, Germany.

1.3 Encryption

Web SARA makes us of industry standard measures to backup data. This includes encryption, the use of firewalls and Secure Sockets Layer (SSL).
In order to encrypt, the SHA-256 algorithm with RSA is used.

1.4 Backups

Data is regularly backed up following a daily / weekly / montly rotation. Backups are stored separately.

1.5 Accounts and passwords

Every account has a 256-bit password and is only able to access its own database. Accidentaly accessing another database is thus not possible. In order to protect the account further from unauthorized access, Two-Factor-Authentication can be activated.

1.6 Access control

The Web application has a authorization concept. Users with different rights to read and write can be created and customized at any point in time.

1.7 Handling of data after cancellation

All data stored is kept for a period of one year after the cancellation before it is finally deleted. Upon request the deletion can be done at an earlier point.

Additionally all data can be provided free of charge as CSV file or SQL-compatible database file post cancellation.

2 (GDPRG) Technical and organizational measures

2.1 Confidentiality (Art. 32 Abs. 1 lit. b GDPRG)

Physical access control: No access to data processing systems: Keys / key allocation

System access control: No unauthorized system use: Password procedure (Special characters, minimum length, change of password in regular intervals) Setting up a master record for each user

Access control: No unauthorized reading, copying, changing or removing within the system: Differentiates authorization (profiles, roles, transactions and objects)

Separation control: Separate processing of data that was collected for different purposes. Individual databases for different data and customers.

2.2 Integrity (Art. 32 Abs. 1 lit. b GDPRG)

Disclosure control: No unauthorized reading, copying, changing or removing during electronic transmission or transport (HTTPS, SSL – SHA256), logging

Input control: Determining whether and by whom sensitive personal data has been entered, changed or removed in data processing systems: Logging, document management

2.3 Availability and Resilience (Art. 32 Abs. 1 lit. b GDPRG)

Availability Control: Protection against accidental or willful destructions and loss: backup strategy, uninterruptible power supply (UPS), virus protection, firewall reports and emergency plans

Rapid recoverability (Art. 32 Abs. 1 lit. c GDPRG)

The company’s servers and data centers are **located** in Germany.

2.4 Periodic review, assessment and evaluation procedures (Art. 32 Abs. 1 lit. d GDPRG; Art. 25 Abs. 1 GDPRG)

Privacy Management

Incident-Response-Management

Privacy-friendly presets (Art. 25 Abs. 2 GDPRG)

Order control: No order data processing according to Art. 28 GDPR without corresponding instructions from the client, e.g.: clear contract design, formalized management of orders, strict selection oft he service provider, obligation to convince in advance, follow-up checks.