

IT-Sicherheit in SORQA

Welche Schutzmaßnahmen die Software für Sortieranaysen heute umsetzt und was als Nächstes geplant ist.

Kurz gesagt

- ✓ Persönliche Zugänge, Passwörter nur als sicherer Hash, Sperre nach wiederholten Fehlversuchen.
- ✓ Fein abgestufte Rechte, die der Server bei jeder einzelnen Aktion prüft, nicht nur die Oberfläche.
- ✓ Verschlüsselte Übertragung (HTTPS) und moderne Schutzregeln im Browser gegen eingeschleusten Code.
- ✓ Lückenloser Änderungsverlauf, tägliche Datensicherung und Schreibschutz für abgeschlossene Projekte.
- ✓ Betrieb auf Servern in Deutschland, ohne Inhalte oder Dienste fremder Anbieter.

1 Anmeldung und Zugänge

- **Persönliche Zugänge:** Jeder Zugang gehört genau einer Person. Gleichzeitig angemeldet sein dürfen höchstens ein Handy oder Tablet und ein PC; eine neue Anmeldung beendet die ältere auf einem Gerät derselben Art. So fallen geteilte Zugänge auf.
- **Passwörter:** mindestens 8 Zeichen, gespeichert nur als Hash nach dem aktuellen Verfahren der Programmiersprache PHP, das sich bei Bedarf automatisch erneuert. Auch der Betreiber kann Passwörter nicht lesen.
- **Schutz vor Raten:** Nach 5 Fehlversuchen ist der Zugang für 5 Minuten gesperrt. Anfragen zum Zurücksetzen werden je Absender und Zugang begrenzt.
- **Passwort vergessen:** Einmal-Links, nur an bestätigte E-Mail-Adressen, 30 Minuten gültig und nur als Hash gespeichert. Die Software verrät nie, ob es zu einer Angabe einen Zugang gibt.
- **Sitzungen:** Eine Anmeldung endet nach 12 Stunden ohne Aktivität (einstellbar). Ein neues Passwort meldet den Zugang auf allen anderen Geräten ab; die Leitung kann Geräte abmelden und Zugänge sofort deaktivieren.
- **Benachrichtigung:** Wird ein Passwort oder eine E-Mail-Adresse geändert, bekommt die Person eine E-Mail.
- **Keine Standard-Passwörter:** Bei der Einrichtung erzeugt die Software ein zufälliges Passwort. Der Notfallzugang für Administratoren funktioniert nur mit einem Schlüssel, der auf dem Server selbst hinterlegt ist.

2 Rechte und Rollen

Gruppen

Vier Gruppen sind vorbereitet: Admin, Sortierleiter, Sortierkraft und Visitor (nur ansehen, kein Export). Weitere Gruppen lassen sich aus 14 Einzelrechten zusammenstellen, zum Beispiel Export, Datensicherung oder Kostenübersicht.

Geprüft auf dem Server

Jede Aktion prüft der Server gegen die Rechte der Person. Projekte lassen sich auf bestimmte Personen beschränken. Abgeschlossene Projekte sind schreibgeschützt; sensible Angaben wie Stundensätze einzelner Personen brauchen eine eigene Freigabe.

3 Übertragung und Browser

- **HTTPS:** Die Software leitet unverschlüsselte Aufrufe automatisch auf HTTPS um und weist den Browser an, die Seite künftig nur noch verschlüsselt zu öffnen.
- **Schutzregeln im Browser:** Eine Content Security Policy erlaubt nur Skripte vom eigenen Server. Weitere Kopfzeilen verhindern, dass fremde Seiten SORQA einbetten oder Dateien falsch deuten.
- **Schutz vor untergeschobenen Aktionen:** Jede Änderung braucht ein geheimes Prüfzeichen der laufenden Sitzung (CSRF-Schutz).
- **Sitzungs-Cookie:** für Skripte unsichtbar, nur über HTTPS gesendet, nicht an fremde Seiten weitergegeben und auf die jeweilige Installation begrenzt.
- **Keine fremden Inhalte:** keine externen Schriften, Skripte, Zähler oder Werbenetzwerke.

4 Server und Daten

- Programmteile, Fotos und Sicherungen sind über das Internet nicht direkt abrufbar. Fotos liefert die Software nur nach Anmeldung und Rechteprüfung aus.
- **Hochgeladene Dateien:** Angenommen werden nur echte Bilder (JPEG, PNG, WebP) bis 50 Megapixel. Der Server rechnet jedes Bild neu und speichert nur diese Fassung; versteckter Inhalt in einer Datei gelangt so nicht auf den Server.
- **Datenbank:** Eingaben gelangen über vorbereitete Abfragen in die Datenbank (Schutz vor SQL-Einschleusung). Alle Ausgaben werden so aufbereitet, dass eingegebener Text nie als Programmcode ausgeführt wird.
- **Zugangsdaten des Servers** liegen in einer Konfigurationsdatei, die nie ausgeliefert wird und auf Wunsch außerhalb des Web-Ordners liegt.
- **Eigene Installation:** Jeder Kunde erhält eine eigene Installation: eigene Adresse, eigener Programmordner, eigene Datenbank und eigene Zugänge.

5 Nachvollziehbarkeit und Verfügbarkeit

Maßnahme	Was sie bewirkt
Änderungsverlauf	Wer hat wann was geändert, mit altem und neuem Wert. Grundlage für eine prüffähige Dokumentation.
Tägliche Datensicherung	Automatisch beim ersten Aufruf des Tages, die letzten 14 bleiben. Vor jedem Update entsteht eine zusätzliche Sicherung.
Updates ohne Datenverlust	Neue Versionen passen die Datenbank schrittweise an; eine Neuinstallation ist nie nötig.
Netzaussetzer in der Halle	Eingaben, die nicht ankommen, bleiben auf dem Gerät und werden nachgesendet.
Bearbeitungssperren	Zwei Personen können nicht gleichzeitig denselben Behälter bearbeiten und sich gegenseitig überschreiben.

6 Ehrlicher Stand: was es noch nicht gibt

- **geplant** **Zwei-Faktor-Anmeldung** (z. B. mit einer Authenticator-App).
- **geplant** **Automatische Sicherung außerhalb des Servers.** Heute liegen die täglichen Sicherungen geschützt auf demselben Server; berechtigte Personen können sie jederzeit herunterladen.
- **auf Anfrage** **Externer Sicherheitstest** (Penetrationstest). Ein solcher Test hat bisher nicht stattgefunden.
- **auf Anfrage** **Verschlüsselung gespeicherter Daten** über die Maßnahmen des Hosters hinaus.

Zertifizierung: SORQA selbst ist nicht zertifiziert. Die Software unterstützt eine prüffähige Dokumentation, zum Beispiel für Qualitäts- oder Umweltmanagementsysteme nach ISO-Normen.

Fragen zur Sicherheit? Eine Liste der technischen und organisatorischen Maßnahmen stellen wir Ihnen gern zur Verfügung.

SORQA · sorqa.app · info@sorqa.app

Stand: Oktober 2026, SORQA Version 1.40. SORQA ist ein Arbeitstitel. Hosting: STRATO GmbH, Rechenzentren in Deutschland.

Die beschriebenen Maßnahmen geben den Stand der Software wieder. Sie ersetzen keine eigene Prüfung der Anforderungen Ihres Unternehmens.