Informationssicherheitskonzept, Technische und organisatorische Massnahmen (TOM)

der Sobrado Software AG

Informationssicherheitskonzept, Technische und organisatorische Massnahmen (TOM) der Sobrado Software AG
nach [Art. 8 DSG](https://www.fedlex.admin.ch/eli/cc/2022/491/de#art_8)

# Allgemeine Bestimmungen

Dieses Dokument beschreibt das Informationssicherheitskonzept und die technischen und organisatorischen Massnahmen (TOM), welche Sobrado zum Schutz der Vertraulichkeit, Integrität und vertragsgemässen Verfügbarkeit von Personendaten trifft.

# Technische und organisatorische Sicherheitsmassnahmen

## Vertraulichkeit

### Zugangskontrolle

*Unbefugten ist der (räumliche) Zutritt zu Datenverarbeitungsanlagen, in denen Kundendaten (einschliesslich Personendaten) verarbeitet werden oder genutzt werden, zu verwehren.*

Umgesetzte Massnahmen:

Die Zutrittskontrolle zu den Gebäuden ist nicht relevant, da Sobrado ausschliesslich online arbeitet. Es gilt eine Clean-Desk Policy.

### Benutzerkontrolle

*Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*

Umgesetzte Massnahmen:

Die Zugangskontrolle zu allen Systemen geschieht vollständig mit einer Zwei-Faktor Authentisierung. Sämtliche Datenträger, Rechner und sämtliche Kommuniktationswege (ausser eMail) sind verschlüsselt, die Schlüssel dazu werden an einem sicheren Ort mit restriktiven und nachvollziehbaren Zugriffsrechten verwaltet. Alle Systeme sind durch einer Firewall geschützt, Betriebseinheiten sind zusätzlich durch eine virtualisierung von Maschinen und Infrastruktur komplett von der Aussenwelt abgeschirmt. (Kubernetes OpenShift-Cluster mit SELinux.)

Die Details dazu sind in der Architektur-Dokumentation [Kapitel 8: Übergreifende Konzepte](https://sobrado.atlassian.net/wiki/spaces/IT/pages/2890562076/8.%2BCross-cutting%2BConcepts) und dessen Unterkapiteln beschrieben.

### Zugriffskontrolle und Speicherkontrolle

*Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die zur Erfüllung ihrer Aufgaben notwendigen (Need-to-Know) und ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Kundendaten (einschliesslich Personendaten) bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.*

Umgesetzte Massnahmen:

Die Zugriffskontrollen sind in einem aufwändigen Rechtesystem implementiert. Die Details dazu sind in der Architektur-Dokumentation [Kapitel 8: Übergreifende Konzepte](https://sobrado.atlassian.net/wiki/spaces/IT/pages/2890562076/8.%2BCross-cutting%2BConcepts) und dessen Unterkapiteln beschrieben, insbesondere das Unterkapitel ACL.

# Integrität

## Weitergabekontrolle (Transportkontrolle, Datenträgerkontrolle und Bekanntgabekontrolle)

*Es ist zu gewährleisten, dass Personendaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung von Personendaten durch Einrichtungen zur Datenübertragung vorgesehen ist.*

Umgesetzte Massnahmen:

Verschiedene technische Massnahmen zur sicherere Weitergabe von Daten sind implementiert: dazu gehörten wie oben erwähnt: - die vollständige Verschlüsselung aller Verbindungen - aller Datenträger - Zwei-Faktor-Authentisierung auf allen Systemen - Zentralisierte Rechte-Verwaltung für Sobrado selber und für die Infrastruktur

Die Details dazu sind in der Architektur-Dokumentation [Kapitel 8: Übergreifende Konzepte](https://sobrado.atlassian.net/wiki/spaces/IT/pages/2890562076/8.%2BCross-cutting%2BConcepts) und dessen Unterkapiteln beschrieben.

## Eingabekontrolle und Protokollierung

*Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Personendaten in Datenverarbeitungs­systeme eingegeben, verändert oder entfernt worden sind.*

Umgesetzte Massnahmen:

Die Protokollierung bzw. das Auditing ist nur teilweise umgesetzt, da aber gemäss [Art 4 DSG](https://www.fedlex.admin.ch/eli/cc/2022/568/de#art_4) keine «besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet» werden, ist eine vollständige Protkolloierung nicht notwendig. Die Details zum Auditing «watchdog» sind in der Architektur-Dokumentation [Kapitel 8: Übergreifende Konzepte](https://sobrado.atlassian.net/wiki/spaces/IT/pages/2890562076/8.%2BCross-cutting%2BConcepts) bzw. dem Unterkapitel «Auditing» beschrieben.

# Verfügbarkeit und Belastbarkeit

## Verfügbarkeitskontrolle und Wiederherstellung

*Es ist zu gewährleisten, dass Kundendaten (einschliesslich Personendaten) gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt sind. Rasche Wiederherstellbarkeit ist sicherzustellen.*

Umgesetzte Massnahmen:

Sämtliche Kundendaten sind auf den Systemen unseres Infrastruktur-Providers gegen diese Fehlmanipulationen geschützt. Es werden in regelmässigen Abständen Sicherungskopien auf separaten Systemen erstellt.
Die Details dazu sind in der Architektur-Dokumentation [Kapitel 8: Übergreifende Konzepte](https://sobrado.atlassian.net/wiki/spaces/IT/pages/2890562076/8.%2BCross-cutting%2BConcepts) und dessen Unterkapiteln beschrieben, insbesondere das Unterkapitel Backup Strategies.

## Belastbarkeit und Zuverlässigkeit

*Es ist sicherzustellen, dass IT- Systeme möglichst auch bei Störungen und Fehlern funktionsfähig bleiben. Zudem ist sicherzustellen, dass Fehlfunktionen von IT Systemen intern gemeldet werden.*

Umgesetzte Massnahmen:

Die System von Sobrado werden von verschiedenen Monitor-System bei Sobrado und bei unserem Infrastruktur-Provider überwacht, welche je nach Schwere des Vorfalls Alarm schlagen, im schlimmsten Fall per Telefon. Dazu gehören: - Überwachung von Endpoints auf Verfügbarkeit - Überwachung von Applkations-Logs - Überwachung von kubernetes-Metriken auf dem Cluster - Überwachung der Cloud-Clusters im Rechenzentrum

Im Falle einer schweren Störung («mayor incident») steht ein Plan zur «Emergency - Disaster Recovery - Business Continuity» zur Verfügung, welches auch die Behandlung von Fehlfunktionen beschreibt, Details dazu sind im Dokument [«Emergency - Disaster Recovery - Business Continuity»](https://sobrado.atlassian.net/wiki/spaces/Business/pages/3590782977/Emergency%2B-%2BDisaster%2BRecovery%2B-%2BBusiness%2BContinuity) beschrieben.

Die Systeme der Sobrado werden regelmässig durch Statische Code-Analyse und durch simulierte Angriffe (Penetrations Tests nach OWASP Top 10 et al.) auf Schwachstellen geprüft.
Details zur Überwachung sind in der Architektur-Dokumentation [Kapitel 8: Übergreifende Konzepte](https://sobrado.atlassian.net/wiki/spaces/IT/pages/2890562076/8.%2BCross-cutting%2BConcepts) und dessen Unterkapiteln beschrieben.

# Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

## Datenschutz-Management

Umgesetzte Massnahmen:

Um die Gewährleistung der Datenschutzes zu gewährleisten, sind die Rechte zu den kritischen Systemen aufs Minimun eingeschränkt und werden bei jeder Veränderung überprüft, insbesonderen durch das Durchführen von Code-Reviews und Abnahmetests.
Die Details dazu sind in der Architektur-Dokumentation [Kapitel 8: Übergreifende Konzepte](https://sobrado.atlassian.net/wiki/spaces/IT/pages/2890562076/8.%2BCross-cutting%2BConcepts) und dessen Unterkapiteln beschrieben.

## Incident-Response-Management (Erkennung und Minderung oder Beseitigung von Verletzungen der Datensicherheit)

Umgesetzte Massnahmen:

Im Falle einer schweren Störung («mayor incident») steht ein Plan zur «Emergency - Disaster Recovery - Business Continuity» zur Verfügung, welches auch den Prozess zur Wiederherstellung, Information der Betroffenen Personen und Umsetzung von Verbesserung anschliessend an den Vorfall regelt.

Konkret gelten folgende Reaktionszeiten auf Störungen als Richtlinien:

| Prioritäts-Code | Behandlung Emergency | Reaktionszeit-Vorgabe | Lösungszeit-Vorgabe |
| --- | --- | --- | --- |
| 1 (Rot) | Major incident | 10 Minuten | 4 Stunden |
| 2 (Hellrot) | Major incident | 1 Stunde | 8 Stunden |
| 3 (Orange) | Little incident | 4 Stunden | 24 Stunden |
| 4 (Grün) | Little incident | 1 Tag | 1 Woche |

Wobei die Prioritäten wie folgt definiert sind:

* 1 beträchtliche oder existenzbedrohende Auswirkung, sehr hohe Dringlichkeit
* 2 begrenzte oder beträchtliche Auswirkungen, mittlere Dringlichkeit
* 3 begrenzete Auswirkungen, geringe Dringlichkeit
* 4 vernachlässigbare Auswirkungen, geringe Dringlichkeit

Details zum Incident-Response-Management sind im Dokument [«Emergency - Disaster Recovery - Business Continuity»](https://sobrado.atlassian.net/wiki/spaces/Business/pages/3590782977/Emergency%2B-%2BDisaster%2BRecovery%2B-%2BBusiness%2BContinuity) beschrieben.

## Datenschutzfreundliche Voreinstellungen

Umgesetzte Massnahmen:

Die Rechteverwaltung in Sobrado ist so implementiert, dass im Standardfall keine unnötigen Rechte vergeben werden.
Die Details dazu sind in der Architektur-Dokumentation [Kapitel 8: Übergreifende Konzepte](https://sobrado.atlassian.net/wiki/spaces/IT/pages/2890562076/8.%2BCross-cutting%2BConcepts) und dessen Unterkapiteln beschrieben.

## Auftragskontrolle

*Keine Auftragsdatenverarbeitung oder Unter-Auftragsbearbeitung ohne entsprechende Weisung des Kunden.*

Umgesetzte Massnahmen:

Die Sobrado regelt über SLA mit allen Kunden die Details der Datenverarbeitung.