Was wird in goTRESOR geschützt?

Auf goTRESOR werden geschützt:

- **Austauschdaten:** Daten, die unter den Usern ausgetauscht werden (Nachrichten, Notizen, Bemerkungen, Termine, Internet-Links usw.).
- **Dateien:** Von den Usern hochgeladenen Dateien (Dateien mit beliebigem Dateiformat).
- **Personenbezogene Daten:**
  User-Daten: *Kontodaten des Users, die er bei seiner Registrierung erfassen kann (Namen, Anschrift, Geburtsdatum, E-Mail-Adresse, Telefonnummern, usw. sowie sein User-Name und Passwort).*
  Daten der Kontakte: *Daten, die ein User von den Kontakten anlegen und pflegen kann (Name, Anschrift, Geburtsdatum, E-Mail-Adresse, Telefonnummern usw.).*

Wo und wie wird in goTRESOR geschützt?

In goTRESOR gilt grundsätzlich, dass Daten und Dateien zu **keinem** Zeitpunkt

1) unverschlüsselt übertragen werden,
2) auf dem Server unverschlüsselt abgelegt werden und
3) von Personen eingesehen werden können, für die sie nicht bestimmt sind.

Das logische Prinzip von goTRESOR fußt auf zwei Objekttypen: "Tresorraum" und "Schließfach". Ähnlich den Tresorräumen einer Bank gibt es "Tresorräume", in denen beliebig viele "Schließfächer" angelegt werden können. Die "Tresorräume" sind voneinander getrennt. Die "Schließfächer" in einem "Tresorraum" sind ebenfalls voneinander getrennt.

Schutz durch logische Trennung der Ablageorte

Im Tresorraum werden **die personenbezogenen Daten** geschützt.

Im Schließfach werden **die Austauschdaten** und **die hochgeladenen Dateien** geschützt.

Schutz durch eindeutige Zugangsrechte

- Mit der Anlage eines Schließfachs wird der User zum Eigentümer desselben und nur er entscheidet, wem er den Zugang in sein Schließfach gewährt.
- In einem "Tresorraum" sind für den User nur die Schließfächer sichtbar, für die er zugangsberechtigt ist.
- Ein User hat nur dann Einsicht in die Schließfächer, wenn er eine Zugangsberechtigung vom Schließfach-Eigentümer erhalten hat und diese bestätigt hat.

Die 4-Keys-Technology

Schutz durch Verschlüsselung

- Die Daten (personenbezogene Daten sowie Austauschdaten) und die Dateien werden erst verschlüsselt und dann gespeichert.
- Bei Dateien werden auch die Dateinamen verschlüsselt und unter dem verschlüsselten Namen gespeichert.
- Die Verschlüsselung erfolgt immer mittels des AES-Verfahrens (256-Bit) und eines eindeutigen Schlüssels.
- Die Schlüssel werden auch mit dem AES-Verfahrens (256-Bit) verschlüsselt und verschlüsselt gespeichert. Kein Schlüssel liegt im goTRESOR-System auf einem Datenspeichermedium in lesbarer Form vor, damit sind die Schlüssel für niemanden einsehbar.

Die Schlüsseltypen

Für die 4-Keys-Technology werden in goTRESOR vier Schlüsseltypen verwendet:

Tresor-Schlüssel Dient der Verschlüsselung personenbezogener Daten.

Schließfach-Schlüssel Dient der Verschlüsselung aller Inhalte im Schließfach.

Private-User-Key (PUK) Dient der Verschlüsselung der User-eigenen Zugriffsdaten.

Mobile PIN Dient der Verschlüsselung von Zugangsdaten für die User.

Der PUK und die MobilePIN werden in goTRESOR **nicht** gespeichert! Diese kennt nur der User.
Damit ist sichergestellt, dass nur derjenige Zugang zu den Daten und Dateien hat, für den diese Daten und Dateien bestimmt sind (auch die Systemadministratoren haben keinen Zugang zu diesen Daten und Dateien).