Checkliste zum Schutz von sensiblen Daten

Schützen Sie Ihre Passwörter!

Schicken Sie uns niemals Informationen zu Passwörtern wie Private Keys o.ä. Nutzen Sie stattdessen den TeamViewer oder teilen Sie in einem Call den Bildschirm mit uns, um ein Problem zu lösen.

Ist es nötig, die Daten zu senden?

Überlegen Sie, ob das Senden der Daten für die Lösung des Problems tatsächlich notwendig ist. Senden Sie personenbezogene Daten nur dann, wenn es unumgänglich ist.

Löschen Sie unnötige Daten!

Stellen Sie sicher, dass nur minimal notwendige Informationen in Dokumenten enthalten sind und gesendet werden. Entfernen Sie alle nicht relevanten personenbezogenen Daten aus den Dokumenten oder Screenshots.

ID-Nummern statt Namen verwenden!

Ersetzen Sie Namen von Personen mit der ID-Nummer aus der Applikation. Diese lässt ohne Datenbankzugriff keine Rückschlüsse auf die Person zu.

Bearbeiten Sie PDF-Dateien!

Nutzen Sie PDF-Editoren, um Inhalte zu entfernen. Fragen Sie Ihre:n IT-Verantwortliche:n, welche Apps Sie dafür verwenden können (z.B. Acrobat Pro). Löschen Sie sensible Daten. Speichern Sie das Dokument.

Bearbeiten Sie Word-Dateien!

Löschen oder ersetzen Sie Namen, Geburtsdatum, AHV-Nummern und andere personenbezogene Informationen durch sonderzeichen. Oder ersetzen Sie Text durch Platzhalter (wie «GELÖSCHT»).

Bearbeiten Sie Bildschirmaufnahmen!

Mit Bearbeitungssoftware können Sie personenbezogene Daten in Screenshots entfernen oder verdecken (z.B. Paint, GIMP, Photoshop). Schneiden Sie personenbezogene Daten aus oder schwärzen Sie diese.

Durch die Umsetzung dieser Massnahmen tragen Sie aktiv dazu bei, die Sicherheit und den Schutz personenbezogener Daten zu gewährleisten. Vielen Dank für Ihre Mithilfe! 😄🔒🖥️