

Sicherheitsblatt

Wo Ihre Daten liegen, wie sie geschützt sind und was wir nachweisen können

Sinew GmbH · Trennio

Stand: 24. September 2026

Inhalt

Sicherheitsblatt.....	1
Wo die Daten liegen.....	2
Wer Zugang hat.....	2
Wie die Daten geschützt sind.....	3
Was nachvollziehbar bleibt.....	3
Sicherungen und Wiederherstellung.....	3
Überwachung.....	4
Wenn etwas passiert.....	4
Dienstleister.....	4
Ihre Daten gehören Ihnen.....	4
Was wir nicht haben.....	4
Fragen.....	5

Sicherheitsblatt

Dieses Blatt fasst zusammen, wie Trennio die Daten Ihrer Gemeinde schützt. Die verbindlichen Zusagen stehen im Auftragsbearbeitungsvertrag (AVV) und in seinem Anhang A; dieses Blatt erklärt sie und nennt, was dahintersteht.

Wo die Daten liegen

Was

Ort

Anwendung und Datenbank

Nürnberg, Deutschland

Sicherung, zweite Kopie

Nürnberg, Deutschland, getrennter Server

Sicherung, dritte Kopie

Schweiz

Auslieferung der App an die Bevölkerung

europäisches Netz, Inhalte aus Deutschland

Deutschland gilt aus Schweizer Sicht als Land mit angemessenem Datenschutz. Verlangt Ihre Gemeinde ausdrücklich Hosting in der Schweiz, sagen Sie es vor Vertragsabschluss: es ist möglich, aber es ist ein eigener Schritt und kein Standardfall.

Wer Zugang hat

Ihre Mitarbeitenden melden sich im Portal mit Benutzername, Passwort und einem zweiten Faktor an. Der zweite Faktor ist Pflicht, nicht optional. Rollen bestimmen, wer was sehen und ändern darf.

Die Bevölkerung braucht weder Konto noch Passwort. Es gibt keine Bürgerkonten, die gestohlen werden könnten.

Der Betreiber kommt nur über einen zusätzlich abgesicherten Zugang an die Verwaltung. Auf die Server führt kein offener Fernzugang; Wartung läuft ausschliesslich über ein geschlossenes Netz.

Wie die Daten geschützt sind

Unterwegs: Alle Verbindungen sind verschlüsselt, und die Verschlüsselung ist erzwungen.

Passwörter werden nicht gespeichert, sondern nur als nicht umkehrbarer Prüfwert nach einem aktuellen Verfahren abgelegt.

Geheimnisse wie Zugangsschlüssel liegen verschlüsselt, nicht im Klartext.

IP-Adressen werden in der Anwendung nie im Klartext gespeichert, sondern nur als nicht umkehrbarer Prüfwert.

Trennung der Gemeinden: Jede Gemeinde ist ein eigener Mandant. Eine Abfrage kann die Grenze nicht überschreiten; das ist an jeder Stelle geprüft und mit Tests abgesichert.

Scan-Bilder werden nicht gespeichert und nicht zum Training von Modellen verwendet.

Fotos aus dem Mängelmelder werden beim Hochladen von Standortangaben in der Bilddatei befreit und nach Abschluss der Meldung gelöscht.

Was nachvollziehbar bleibt

Änderungen im Portal werden protokolliert und mit einer fortlaufenden Prüfkette gegen nachträgliche Änderung gesichert. Ein einzelner Eintrag lässt sich nicht entfernen, ohne die Kette zu zerstören. Das ist beabsichtigt: es macht das Protokoll zum Nachweis. Ein tägliches Prüfprogramm kontrolliert, dass die Kette unversehrt ist.

Sicherungen und Wiederherstellung

Die Datenbank wird **stündlich** gesichert, zusätzlich täglich.

Die Sicherungen liegen **verschlüsselt an drei Orten** in zwei Ländern.

Der Schlüssel zur Entschlüsselung liegt getrennt von den Sicherungen.

Die **Wiederherstellung ist dokumentiert und geübt**, zuletzt am 15. September 2026. Geübt heisst: eine Sicherung wurde tatsächlich zurückgespielt, nicht nur die Anleitung gelesen.

Überwachung

Der Betrieb wird mehrstufig überwacht: Erreichbarkeit von aussen, Zustand der Dienste, Frische der Sicherungen und Unversehrtheit des Prüfprotokolls.

Meldungen gehen an den Betreiber, nicht an Ihre Gemeinde. Fällt die Überwachung selbst aus, meldet sich ein zweiter, davon unabhängiger Dienst.

Wenn etwas passiert

Kommen Personendaten abhanden oder in falsche Hände, melden wir es Ihnen **innert 48 Stunden** ab dem Zeitpunkt, an dem wir es entdecken, mit Angaben zu Art, betroffenen Daten, möglichen Folgen und bereits ergriffenen Massnahmen. Dahinter steht ein schriftlicher Ablauf, nicht nur die Zusage. Die Meldung an Ihre kantonale Datenschutzstelle liegt bei Ihnen; wir liefern Ihnen jede Angabe, die Sie dafür brauchen.

Dienstleister

Trennio setzt Dienstleister ein, unter anderem für Server, Auslieferung, Übersetzung, die Materialerkennung und den Versand von Mitteilungen. Die vollständige Liste mit Sitzland und Rechtsgrundlage steht im AVV, Ziffer 5, und ist Teil des Vertrags. Wechselt ein Dienstleister oder kommt einer hinzu, erfahren Sie es 30 Tage im Voraus und können begründet widersprechen.

Ihre Daten gehören Ihnen

Sie holen jederzeit selbst alles heraus, was Sie erfasst haben: Abfuhrtermine, Sammelstellen, Gebiete, Mitteilungen und Meldungen. Der Export liegt im Portal und verlangt Ihren zweiten Faktor. Was bei einer Kündigung geschieht, steht im Exit-Blatt.

Was wir nicht haben

Damit Sie es nicht suchen müssen:

Keine ISO-27001-Zertifizierung und kein externes Sicherheitsaudit. Die Massnahmen oben sind umgesetzt und intern geprüft, aber nicht von einer unabhängigen Stelle bestätigt.

Kein Rechenzentrum in der Schweiz im Standardfall, nur die dritte Sicherungskopie.

Keine Stellvertretung. Trennio wird von einer Person betrieben. Was bei einem Ausfall weiterläuft und was nicht, steht im Betriebsblatt.

Kein Bereitschaftsdienst rund um die Uhr. Erreichbarkeit und Reaktionszeiten stehen im Betriebsblatt.

Wenn Ihre Gemeinde für die Beschaffung einen Nachweis braucht, den wir hier nicht nennen, sagen Sie es vor dem Entscheid. Dann sagen wir Ihnen, ob und bis wann wir ihn beschaffen können, statt es offenzulassen.

Fragen

Sicherheit und Datenschutz: info@trennio.app