Stand: 22. September 2026

Anhang 1a: Technische und organisatorische Massnahmen (TOM)

Dieser Anhang beschreibt die Massnahmen, mit denen Trustlytics ein angemessenes Sicherheitsniveau gewährleistet. Berücksichtigt werden dabei Art und Umfang der Bearbeitung sowie die Risiken für die Rechte und Freiheiten der betroffenen Personen.

01 Vertraulichkeit, Integrität, Verfügbarkeit und Stabilität

- Der Datenschutz ist fester Bestandteil des Risikomanagements von Trustlytics.
- Die Mitarbeitenden sind qualifiziert und zur Geheimhaltung verpflichtet.
- Die Mitarbeitenden wissen, welche Folgen ein Verstoss gegen Sicherheitsvorschriften und Sicherheitsverfahren hat.
- Die Mitarbeitenden erhalten klare Anweisungen zu Zugangskontrolle, Kommunikationssicherheit und Betriebssicherheit.
- Fällt eine kritische Systemkomponente aus, wird der Betrieb innert kürzester Zeit wiederhergestellt, etwa durch Ersatzkomponenten, redundante Systeme oder Datenspiegelung.

02 Anonymisierung und Verschlüsselung

- Bei den Analysedaten werden die IP-Adressen gekürzt, damit sich einzelne Personen nicht identifizieren lassen.
- Wo möglich, werden Personendaten verschlüsselt. Algorithmus und Schlüssellänge richten sich danach, wie heikel die Daten sind.
- Die Schlüssel erhalten nur wenige Personen, und sie werden sicher aufbewahrt.

03 Wiederherstellung nach einem Zwischenfall

- Für die Sicherung besteht eine Strategie. Diese richtet sich nach der Art der Daten und danach, wie oft sie ändern.
- Für die Sicherungssysteme gelten dieselben Sicherheitsmassnahmen wie für die Produktivsysteme.
- Die Mitarbeitenden, die Daten wiederherstellen, sind dafür geschult.

04 Identifizierung und Berechtigungen

- Der Zugang zu den Systemen ist durch branchenübliche Identifikations- und Authentifizierungsverfahren geschützt.
- Benutzerkonten und Berechtigungen verwalten wenige dafür verantwortliche Mitarbeitende, nach einem restriktiven und bedarfsorientierten Konzept.
- Zugriff auf Personendaten haben nur Mitarbeitende, die ihn für ihre Funktion tatsächlich brauchen.
- Soweit möglich wird für den Zugang eine Mehrfaktor-Authentifizierung eingesetzt.

05 Schutz bei der Datenübertragung

- Der Fernzugriff läuft ausschliesslich über verschlüsselte Verbindungen.
- Alle Daten, auch Personendaten, werden mit branchenüblichen Verfahren verschlüsselt übertragen.

06 Schutz bei der Speicherung

- Personendaten dürfen nur jene Personen einsehen, eingeben, ändern und löschen, die diese Daten bearbeiten müssen.
- Die Daten im Rechenzentrum sind vor physischem Zugriff geschützt (siehe Abschnitt 07) und werden nach Möglichkeit verschlüsselt.

07 Physische Sicherheit und Protokollierung

Für Systeme, die bei externen Dienstleistern betrieben und gewartet werden, bestehen Vereinbarungen über entsprechende Massnahmen. Die Dienstleister setzen diese um und stehen dafür ein. Dazu gehören unter anderem:

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um das gesamte Rechenzentrumsgelände
- dokumentierte Schlüsselvergabe an Mitarbeitende
- Richtlinien für die Begleitung und Kennzeichnung von Gästen im Gebäude
- Besetzung der Rechenzentren rund um die Uhr
- Videoüberwachung an Ein- und Ausgängen, bei Sicherheitsschleusen und in Serverräumen
- Zutritt für betriebsfremde Personen, etwa Lieferanten, nur in Begleitung von Mitarbeitenden

08 Interne IT und Systeme mit Personendaten

- Alle Systeme und die gesamte Software werden regelmässig aktualisiert.
- Sicherheitsupdates werden rasch installiert.
- Sicherheitshinweise werden überwacht und bewertet, Sicherheitslücken werden behoben.
- Fernzugriff durch Dritte ist nicht gestattet.

09 Löschung von Personendaten

Die gespeicherten Personendaten werden regelmässig überprüft und gelöscht, sobald sie nicht mehr gebraucht werden. Vorbehalten bleiben gesetzliche und vertragliche Aufbewahrungspflichten. Aus Sicherungskopien verschwinden die Daten, sobald diese Sicherung im üblichen Zyklus überschrieben wird.

10 Datenübertragbarkeit

Anfragen zur Datenübertragbarkeit werden unverzüglich an die zuständige Stelle weitergeleitet und dort bearbeitet, damit die gesetzlichen Fristen eingehalten werden.

11 Unterauftragsbearbeiter

Alle von Trustlytics beauftragten Unterauftragsbearbeiter haben technische und organisatorische Massnahmen umgesetzt, die den hier beschriebenen entsprechen.