Löschmatrix AnyGuard

Datenhaltung, Aufbewahrung und Löschung

Dokumentversion: 2.0
Stand: November 2026
Dokumentverantwortung: Datenschutz & Compliance, Solutioneers AG
Kontakt: privacy@s-ag.ch

---

1. Zweck und Geltungsbereich

Diese Löschmatrix dokumentiert die Speicherorte, Aufbewahrungsfristen, Löschereignisse und technischen Löschmechanismen für Daten, die im Rahmen der Nutzung von AnyGuard verarbeitet werden.

Sie gilt produktübergreifend für:

- AnyGuard AI
- AnyGuard Dental/Health
- AnyGuard Legal
- AnyGuard Public

Abweichungen aufgrund einer individuellen Kundenkonfiguration, eines besonderen Hosting-Modells oder einer vertraglich vereinbarten Aufbewahrungsfrist werden in der jeweiligen Instanzdokumentation, im Angebot oder im Auftragsverarbeitungsvertrag ausgewiesen.

Die Löschmatrix dient insbesondere als Grundlage für:

- die datenschutzrechtliche Erstbewertung,
- das Verzeichnis von Verarbeitungstätigkeiten,
- eine Datenschutz-Folgenabschätzung,
- interne Lösch- und Aufbewahrungskonzepte,
- Audits und Informationssicherheitsprüfungen.

2. Grundsätze der Datenlöschung

AnyGuard folgt bei Speicherung und Löschung den Grundsätzen der Datenminimierung und Speicherbegrenzung.

Dabei gelten insbesondere folgende Prinzipien:

Zweckgebundene Speicherung

Daten werden nur so lange gespeichert, wie dies für die Bereitstellung der jeweiligen Funktion, die Erfüllung vertraglicher Pflichten oder die Gewährleistung von Sicherheit und Stabilität erforderlich ist.

Kundenseitige Steuerung

Der Kunde kann Aufbewahrungsfristen selbst konfigurieren oder Daten unmittelbar löschen.

Trennung von Produktivsystem und Backup

Eine Löschung im Produktivsystem entfernt den betreffenden Datensatz aus der laufenden Nutzung. War der Datensatz bereits Bestandteil einer Sicherung, erfolgt seine vollständige Entfernung mit dem turnusmäßigen Ablauf der dokumentierten Backup-Retention.

Keine unnötige Inhaltsprotokollierung

Klartextinhalte von Chats, Dokumenten oder Pseudonymzuordnungen werden nicht zusätzlich in technischen Systemlogs gespeichert.

Kaskadierende Löschung

Abgeleitete Datenobjekte wie Dokumenten-Chunks oder Embeddings werden zusammen mit dem zugrunde liegenden Quelldokument gelöscht.

3. Löschmatrix

Datenobjekt	Speicherort	Aufbewahrung	Löschereignis	Technischer Löschmechanismus	Kundenseitig konfigurierbar
Chatinhalte	Workspace-Datenbank	Nach kundenseitiger Konfiguration; speicherlose Nutzung kann instanzabhängig verfügbar sein	Manuelle Löschung, Ablauf der Retention Policy oder Vertragsende	Entfernung aus dem Produktivsystem; anschließendes Auslaufen aus Backups	Ja
KI-Antworten	Workspace-Datenbank	Wie zugehöriger Chat	Löschung des Chats, Ablauf der Retention Policy oder Vertragsende	Kaskadierende Entfernung mit dem Chat	Ja
Pseudonymzuordnung zwischen Klartext und Platzhalter	Temporärer Verarbeitungsspeicher der Kundeninstanz	Ausschließlich für die Dauer der aktiven Anfrage	Abschluss oder Abbruch der Anfrage	Automatisierte Entfernung aus dem temporären Verarbeitungsspeicher	Nein
Temporäre Prompt- und Antwortdaten während der Rekontextualisierung	Temporärer Verarbeitungsspeicher	Ausschließlich für die Dauer der aktiven Verarbeitung	Abschluss oder Abbruch der Anfrage	Automatisierte Entfernung nach Verarbeitung	Nein

Datenobjekt	Speicherort	Aufbewahrung	Löschereignis	Technischer Löschmechanismus	Kundenseitig konfigurierbar
Live-Audiostream	Temporärer Verarbeitungsspeicher der selbst betriebenen Speech-to-Text-Komponente	Nur während der laufenden Transkription	Abschluss oder Abbruch der Transkription	Automatisierte Entfernung aus dem Verarbeitungsspeicher	Nein
Transkript aus Live-Audio	Workspace-Datenbank	Wie Chat oder Dokument	Manuelle Löschung, Ablauf der Retention Policy oder Vertragsende	Entfernung aus dem Produktivsystem; anschließendes Auslaufen aus Backups	Ja
Hochgeladene Audiodatei	Object-Storage des Workspaces	Wie Chat oder Dokument	Manuelle Löschung, Ablauf der Retention Policy oder Vertragsende	Entfernung aus dem Object-Storage; anschließendes Auslaufen aus Backups	Ja
In der mobilen App aufgenommene Audiodatei im Workspace	Object-Storage des Workspaces	Wie Chat oder Dokument	Manuelle Löschung, Ablauf der Retention Policy oder Vertragsende	Entfernung aus dem Object-Storage; anschließendes Auslaufen aus Backups	Ja

Datenobjekt	Speicherort	Aufbewahrung	Löschereignis	Technischer Löschmechanismus	Kundenseitig konfigurierbar
Lokal in der App gespeicherte Audiodatei	App-Sandbox des Endgeräts	Maximal 7 Tage, sofern nicht vorher gelöscht	Manuelle Löschung, Logout, Deinstallation oder Ablauf von 7 Tagen	Entfernung aus der lokalen App-Datenbank und dem App-Sandbox-Speicher	Teilweise
Temporäre Audio-Konvertierungsdateien	Temporärer Verarbeitungsspeicher	Nur während des Preprocessings	Abschluss oder Abbruch der Verarbeitung	Automatisierte Entfernung	Nein
Text-to-Speech-Audiodaten	Temporärer Verarbeitungsspeicher	Nur während der Ausgabeerzeugung	Abschluss der Audioausgabe	Keine dauerhafte serverseitige Speicherung; automatisierte Entfernung	Nein
Hochgeladene Dokumente	Workspace bzw. Wissensdatenbank	Bis zur Löschung durch den Nutzer, Ablauf einer konfigurierten Frist oder Vertragsende	Manuelle Löschung, Retention Policy oder Vertragsende	Entfernung aus Datenbank und Object-Storage	Ja
Extrahierte Dokumententexte	Wissensdatenbank	An das Quelldokument gekoppelt	Löschung des Quelldokuments	Kaskadierende Löschung	Indirekt

Datenobjekt	Speicherort	Aufbewahrung	Löschereignis	Technischer Löschmechanismus	Kundenseitig konfigurierbar
Dokumenten-Chunks	Vektordatenbank	An das Quelldokument gekoppelt	Löschung des Quelldokuments	Kaskadierende Löschung	Indirekt
Embeddings	Vektordatenbank	An das Quelldokument gekoppelt	Löschung des Quelldokuments	Kaskadierende Löschung	Indirekt
Inhalte aus angebundenen Cloudquellen	Workspace bzw. Wissensdatenbank	Nach Synchronisations- und Löschregeln der Kundeninstanz	Entfernung aus der Quelle, manuelle Löschung, Beendigung der Synchronisation oder Vertragsende	Entfernung aus Wissensdatenbank, Chunks und Vektordatenbank	Teilweise
Generierte Bilder	Object-Storage des Workspaces	Wie Chatinhalt	Löschung des Chats, Ablauf der Retention Policy oder Vertragsende	Entfernung aus dem Object-Storage; anschließendes Auslaufen aus Backups	Ja
Nutzerkonto	Benutzer- und Berechtigungsdatenbank	Für die Dauer des Vertrags- bzw. Nutzungsverhältnisses	Löschung durch Administrator, Vertragsende oder berechtigte Betroffenenanfrage	Deaktivierung bzw. Entfernung des Kontos und der zugehörigen Zugriffsberechtigungen	Ja, durch Administrator

Datenobjekt	Speicherort	Aufbewahrung	Löschereignis	Technischer Löschmechanismus	Kundenseitig konfigurierbar
Organisations- und Workspace-Konfiguration	Konfigurationsdatenbank	Für die Dauer des Vertragsverhältnisses	Vertragsende oder Löschung der Organisation	Entfernung aus dem Produktivsystem; anschließendes Auslaufen aus Backups	Teilweise
Authentifizierungs- und Zugriffsereignisse	Logsystem	Maximal 30 Tage	Ablauf der festen Aufbewahrungsfrist	Automatisierte zeitbasierte Löschung bzw. Überschreibung	Nein
Technische Systemlogs	Logsystem	Maximal 30 Tage	Ablauf der festen Aufbewahrungsfrist	Automatisierte zeitbasierte Löschung bzw. Überschreibung	Nein
Fehler- und Debug-Daten	Logsystem	14 Tage	Ablauf der festen Aufbewahrungsfrist	Automatisierte zeitbasierte Löschung bzw. Überschreibung	Nein
Administrative Änderungen	Audit- bzw. Logsystem	Gemäß dokumentierter Systemkonfiguration, maximal entsprechend der für Auditlogs ausgewiesenen Frist	Ablauf der Aufbewahrungsfrist	Automatisierte zeitbasierte Löschung	Nein

Datenobjekt	Speicherort	Aufbewahrung	Löschereignis	Technischer Löschmechanismus	Kundenseitig konfigurierbar
Supporttickets	Selbst betriebenes Ticketsystem	Nach internem Support- und Aufbewahrungskonzept	Abschluss des Vorgangs und Ablauf der vorgesehenen Aufbewahrungsfrist	Löschung oder Anonymisierung im Ticketsystem	Nein
Support-Screensharing	Keine systemseitige dauerhafte Speicherung durch AnyGuard	Nur während der Sitzung	Ende der Sitzung	Beendigung der Echtzeitübertragung	Nein
Freigegebene Administrations- und Notfallzugriffe	Audit- und Sicherheitslog	Nach dokumentierter Sicherheitsaufbewahrung	Ablauf der festgelegten Logfrist	Automatisierte Löschung bzw. Überschreibung	Nein
Backups der Kundeninstanz	Verschlüsselte Sicherungsinfrastruktur	7 Tage rollierend	Ablauf der jeweiligen Sicherung	Automatisches Überschreiben bzw. Entfernen aus der Backup-Rotation	Nein
Vertrags-, Abrechnungs- und Ansprechpartnerdaten	Systeme eigener Geschäftsprozesse der Solutioneers AG	Nach gesetzlichen und vertraglichen Aufbewahrungspflichten	Ende der gesetzlichen oder vertraglichen Aufbewahrungsfrist	Löschung oder Einschränkung der Verarbeitung	Nein

Datenobjekt	Speicherort	Aufbewahrung	Löschereignis	Technischer Löschmechanismus	Kundenseitig konfigurierbar
Allgemeine E-Mail-Kommunikation	Microsoft 365 Schweiz	Nach internem Kommunikations- und Aufbewahrungskonzept	Zweckfortfall und Ablauf einschlägiger Aufbewahrungspflichten	Löschung aus dem Postfach; anschließendes Auslaufen aus Sicherungs- und Retentionssystemen	Teilweise

4. Löschung von Chat- und Workspace-Inhalten

Manuelle Löschung

Berechtigte Nutzer können eigene Inhalte im Rahmen der verfügbaren Produktfunktionen löschen. Administratoren können zusätzlich Nutzerkonten, Berechtigungen und organisationsweite Inhalte verwalten.

Automatische Retention Policy

Soweit für die jeweilige Instanz aktiviert, können Chat-Inhalte nach einer festgelegten Dauer automatisiert gelöscht werden. Die verfügbaren Fristen und der Geltungsbereich der Richtlinie werden instanzbezogen konfiguriert.

Eine Retention Policy kann je nach Produktkonfiguration gelten für:

- einzelne Nutzer,
- Benutzergruppen,
- einzelne Workspaces,
- die gesamte Kundenorganisation.

Speicherlose Nutzung

Soweit für die konkrete Instanz technisch verfügbar und aktiviert, können Chats ohne dauerhafte Speicherung im Workspace verarbeitet werden. Temporäre Verarbeitungsvorgänge und die gegebenenfalls geltenden Retention-Zeiten externer KI-Provider bleiben hiervon unberührt.

5. Löschung von Dokumenten und Wissensdatenbanken

Bei der Löschung eines Quelldokuments werden automatisch auch die daraus erzeugten Datenobjekte entfernt.

Dies umfasst insbesondere:

- extrahierte Textinhalte,
- Dokumenten-Chunks,
- Metadaten,
- Vektor-Embeddings,
- Such- und Referenzzuordnungen.

Die Löschung erfolgt kaskadierend, damit keine losgelösten abgeleiteten Inhalte in der Wissensdatenbank verbleiben.

Bei synchronisierten externen Quellen kann die Löschung zusätzlich davon abhängen, ob:

- die Datei aus der angebundenen Quelle entfernt wurde,

- die Synchronisation weiterhin aktiv ist,
- eine erneute Übernahme beim nächsten Synchronisationslauf erfolgt.

Der Kunde muss daher sicherstellen, dass eine dauerhaft zu löschende Datei gegebenenfalls auch in der angebundenen Primärquelle entfernt oder von der Synchronisation ausgeschlossen wird.

6. Sprach- und Audiodaten

Live-Transkription

Bei der Live-Transkription wird der Audiostream nicht als dauerhafte Audiodatei gespeichert. Der Stream wird während der laufenden Sitzung verarbeitet und nach Abschluss oder Abbruch automatisiert aus dem Verarbeitungsspeicher entfernt.

Das erzeugte Transkript wird wie ein normaler Chat- oder Dokumenteninhalt behandelt.

Hochgeladene Audiodateien

Hochgeladene Audiodateien werden im Workspace gespeichert und bleiben dort verfügbar, bis sie:

- manuell gelöscht werden,
- durch eine konfigurierte Retention Policy entfernt werden,
- oder das Vertragsverhältnis endet.

Mobile App

In der mobilen App aufgenommene Audiodateien können zusätzlich lokal im geschützten App-Sandbox-Verzeichnis des Endgeräts gespeichert werden.

Für diese lokalen Dateien gelten folgende Löschereignisse:

- manuelle Löschung durch den Nutzer,
- Logout,
- Deinstallation der App,
- Ablauf der automatischen lokalen Aufbewahrungsfrist von 7 Tagen,
- gegebenenfalls Remote-Wipe über ein kundenseitiges MDM.

Die Dateien sind von automatischen Geräte- und Cloudbackups der App ausgenommen, soweit dies durch die jeweilige Betriebssystem- und App-Konfiguration technisch umgesetzt wird.

7. Pseudonymisierungsdaten

Die Zuordnung zwischen Klartextinformationen und generischen Platzhaltern wird ausschließlich innerhalb der jeweiligen AnyGuard-Kundeninstanz und nur während der aktiven Anfrage vorgehalten.

Diese Zuordnung:

- wird nicht dauerhaft gespeichert,
- wird nicht in Systemlogs übernommen,
- ist für externe KI-Provider nicht zugänglich,
- wird nach Abschluss oder Abbruch der Verarbeitung automatisiert entfernt.

Die temporäre Zuordnung ist daher nicht Bestandteil der regulären Workspace-Datenhaltung und unterliegt keiner längerfristigen Retention Policy.

8. Technische Logs und Fehlerdaten

Technische Logs dienen ausschließlich:

- der Systemsicherheit,
- der Fehleranalyse,
- der Stabilität,
- der Missbrauchsprävention,
- der Nachvollziehbarkeit administrativer Vorgänge.

Klartextinhalte von Chats und die Zuordnung zwischen Pseudonym und Klartext werden bewusst nicht in technischen Logs gespeichert.

Für technische Logs gelten folgende maximale Fristen:

- allgemeine technische Systemlogs: 30 Tage,
- Authentifizierungs- und Zugriffsereignisse: 30 Tage,
- Fehler- und Debug-Daten: 14 Tage.

Nach Ablauf erfolgt eine automatisierte Löschung oder Überschreibung.

9. Backups

Backups dienen ausschließlich der Wiederherstellung der Kundeninstanz nach einem technischen Ausfall, einer Beschädigung oder einem Sicherheitsvorfall.

Umfang

Backups können insbesondere enthalten:

- Datenbankstände,
- Chat- und Dokumenteninhalte,
- Embeddings,
- Konfigurationsdaten,
- Benutzer- und Berechtigungsinformationen.

Verschlüsselung

Backups werden verschlüsselt gespeichert.

Retention

Die Backup-Retention beträgt 7 Tage und wird rollierend umgesetzt.

Löschung bereits gesicherter Daten

Wird ein Datenobjekt im Produktivsystem gelöscht, kann es bis zum Ablauf der jeweiligen Backup-Retention noch Bestandteil einer bestehenden Sicherung sein.

Eine selektive Veränderung einzelner Datenobjekte innerhalb unveränderlicher Sicherungsstände erfolgt grundsätzlich nicht, da dies die Integrität und Wiederherstellbarkeit des Backups beeinträchtigen könnte.

Die vollständige Entfernung erfolgt automatisch durch:

- Ablauf der jeweiligen Sicherung,
- Überschreiben im Rahmen der Backup-Rotation,
- Entfernung aus dem aktiven Sicherungsbestand.

Eine Wiederherstellung aus einem Backup erfolgt ausschließlich zu Zwecken der Systemwiederherstellung. Dabei wiederhergestellte Daten unterliegen erneut den im Produktivsystem geltenden Löschregeln.

10. Externe KI-Provider

Externe KI-Provider erhalten ausschließlich die für die jeweilige Funktion erforderlichen und zuvor pseudonymisierten Inhalte.

Die providerseitige Speicherung liegt außerhalb der technischen Löschsteuerung der Kundeninstanz und richtet sich nach den vertraglichen Bedingungen und technischen Konfigurationen des jeweiligen Providers.

OpenAI (OpenAI Ireland Ltd, EU-Region)

Für Text- und Chat-Anfragen ist Zero Data Retention aktiviert. Kundeninhalte werden von OpenAI weder für die Missbrauchsüberwachung protokolliert noch gespeichert. Es werden ausschließlich ZDR-fähige, zustandslose API-Endpunkte eingesetzt. Technisch bedingt können beim Prompt Caching verschlüsselte Zwischenwerte für bis zu 24 Stunden lokal auf den Verarbeitungsmaschinen vorgehalten werden.
KI-Bildstudio: Das KI-Bildstudio ist derzeit nicht Teil des ZDR- und EU-Rollouts. Dort gelten die Standardbedingungen von OpenAI mit einer Aufbewahrung von bis zu 30 Tagen zur Missbrauchsüberwachung. Eine Nutzung der übermittelten Inhalte zum Training der Modelle ist nach den für die API geltenden Bedingungen ausgeschlossen.

Google Gemini API

Für das von AnyGuard eingesetzte Projekt ist zum Zeitpunkt dieser Dokumentversion die kürzeste durch die verwendete Logging-Konfiguration unterstützte Aufbewahrungsdauer von 7 Tagen aktiviert.

Eine freiwillige Freigabe für Modelltraining oder dauerhafte Speicherung zur Modellverbesserung erfolgt nicht.

Lokale Modelle

Bei Verwendung selbst gehosteter Modelle erfolgt keine Übermittlung an einen externen KI-Provider. Es gelten ausschließlich die Speicher- und Löschregeln der jeweiligen AnyGuard-Kundeninstanz.

Änderungen an Providern oder wesentlichen Retention-Zeiträumen werden im Trust Center und in der Subunternehmerdokumentation aktualisiert.

11. Vertragsende und Löschung der Kundeninstanz

Nach Beendigung des Vertragsverhältnisses wird die Kundeninstanz nach Maßgabe der vertraglichen Vereinbarungen deaktiviert und gelöscht.

Dabei werden insbesondere entfernt:

- Workspace-Inhalte,
- Chats,
- Dokumente,
- Audiodateien,
- Bilder,
- Wissensdatenbanken,
- Chunks und Embeddings,
- Benutzerkonten,
- Rollen und Berechtigungen,

- organisationsspezifische Konfigurationen.

Die produktive Löschung erfolgt gemäß dem vereinbarten Offboarding-Prozess.

Soweit die gelöschten Inhalte Bestandteil einer bestehenden Sicherung waren, erfolgt ihre vollständige Entfernung nach Ablauf der Backup-Retention von maximal 7 Tagen.

Daten, die Solutioneers für eigene gesetzliche Nachweis-, Vertrags- oder Abrechnungszwecke aufbewahren muss, sind hiervon ausgenommen. Diese Daten werden für die Dauer der jeweiligen Aufbewahrungspflicht in ihrer Verarbeitung eingeschränkt und anschließend gelöscht.

12. Betroffenenanfragen

Der Kunde bleibt als Verantwortlicher primärer Ansprechpartner für Anfragen betroffener Personen.

Solutioneers unterstützt den Kunden im Rahmen des Auftragsverarbeitungsvertrags insbesondere bei:

- Auskunft,
- Berichtigung,
- Einschränkung,
- Löschung,
- Datenexport,
- Nachweis der angewandten Speicher- und Löschregeln.

Eine Löschung kann eingeschränkt sein, soweit:

- gesetzliche Aufbewahrungspflichten entgegenstehen,
- die Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden,
- die Daten noch Bestandteil einer Sicherung innerhalb der dokumentierten Backup-Retention sind.

13. Löschkontrolle und Nachweis

Die Einhaltung der Löschfristen wird durch eine Kombination aus technischen und organisatorischen Maßnahmen abgesichert.

Dazu gehören insbesondere:

- automatisierte zeitbasierte Löschprozesse,
- kaskadierende Löschung abgeleiteter Daten,
- fest konfigurierte Log-Retention,
- rollierende Backup-Retention,
- Rollen- und Berechtigungsprüfungen,

- dokumentierte Offboarding-Prozesse,
- technische Überwachung fehlgeschlagener Löschprozesse,
- regelmäßige Überprüfung der dokumentierten Fristen.

Sofern eine individuelle Löschbestätigung erforderlich ist, kann diese im Rahmen der vertraglichen und technischen Möglichkeiten auf Anfrage bereitgestellt werden.

14. Verantwortlichkeiten

Kunde als Verantwortlicher

Der Kunde ist insbesondere verantwortlich für:

- Festlegung der zulässigen Speicherdauer,
- Konfiguration der verfügbaren Retention Policy,
- rechtzeitige Löschung nicht mehr erforderlicher Inhalte,
- Beachtung eigener gesetzlicher Aufbewahrungspflichten,
- Steuerung von Benutzerkonten und Berechtigungen,
- Löschung von Daten in angebundenen Primärsystemen,
- Verwaltung lokaler Daten auf Endgeräten,
- Prüfung der Löschanforderungen im Rahmen der eigenen DSFA.

Solutioneers AG als Auftragsverarbeiter

Solutioneers ist insbesondere verantwortlich für:

- technische Umsetzung der dokumentierten Löschmechanismen,
- Betrieb der automatisierten Lösch- und Retentionsprozesse,
- Einhaltung der festen technischen Log- und Backup-Fristen,
- kaskadierende Löschung abgeleiteter Datenobjekte,
- Unterstützung bei Betroffenenanfragen,
- transparente Dokumentation von Änderungen.

15. Abweichende Vereinbarungen

Individuelle Vertrags-, Instanz- oder Branchenanforderungen können abweichende Löschfristen oder besondere Löschmechanismen erfordern.

Solche Abweichungen müssen:

- ausdrücklich vereinbart,
- technisch umsetzbar,
- in der Instanzdokumentation festgehalten,
- und in der DSFA bzw. im Verzeichnis der Verarbeitungstätigkeiten des Kunden berücksichtigt werden.

Im Konfliktfall gehen individuelle schriftliche Vereinbarungen den allgemeinen Angaben dieser Löschmatrix vor.

16. Änderungsverlauf

Version	Datum	Änderung
1.0	Juli 2026	Erstveröffentlichung der produktübergreifenden Löschmatrix für AnyGuard AI, Dental/Health, Legal und Public
2.0	November 2026	Aktualisierung der Angaben zu externen KI-Providern (Abschnitt 10): Für OpenAI (OpenAI Ireland Ltd, EU-Region) ist Zero Data Retention für Text- und Chat-Anfragen aktiviert; die providerseitige Aufbewahrung von bis zu 30 Tagen entfällt dort und gilt nur noch für das KI-Bildstudio. Die Aufbewahrungsfristen der Kundeninstanz (u. a. Systemlogs 30 Tage, Debug-Daten 14 Tage, Backups 7 Tage) sind unverändert.

17. Kontakt

Fragen zur Löschmatrix oder zu instanzbezogenen Aufbewahrungsfristen können an folgende Stelle gerichtet werden:

Team Datenschutz & Compliance
Solutioneers AG
E-Mail: privacy@s-ag.ch