



Datenschutzerklärung

Update: [03/03/2026]

1. Datenschutzerklärung ELVIDA App	3
1. Allgemeines	3
2. Datenverantwortlicher	3
3. Erhebung und Verarbeitung von Personendaten	3
3.1 Registrierung und Kontodaten	3
3.2 Dokumentenuploads und -speicherung	4
3.3 Versicherungssituation (App-Verhalten)	5
3.4 Zahlungsdaten	5
3.5 Kommunikation	5
4. KI-Verarbeitung (OpenAI)	5
5. Internationale Datenübermittlung	6
6. Auftragsverarbeiter	7
7. Datensicherheit	8
8. Speicherdauer und Löschung	8
9. Ihre Rechte	9
10. Datenlecks und Sicherheitsvorfälle	10
11. Automatisierte Entscheidungsfindung	10
12. Änderungen dieser Datenschutzerklärung	10
13. Anwendbares Recht und Gerichtsstand	10
2. Déclaration de protection des données de l'application ELVIDA	11
1. Généralités	11
2. Responsable du traitement des données	11
3. Collecte et traitement des données personnelles	11
3.1 Inscription et données de compte	11
3.2 Téléchargement et stockage de documents	12
3.3 Situation d'assurance (comportement dans l'app)	13
3.4 Données de paiement	13
3.5 Communication	13
4. Traitement IA (OpenAI)	13
5. Transferts internationaux de données	14
6. Sous-traitants	15
7. Sécurité des données	15
8. Durée de conservation et suppression	16
9. Vos droits Vous disposez des droits suivants :	17
10. Fuites de données et incidents de sécurité	17
11. Prise de décision automatisée	18
12. Modifications de cette déclaration de protection des données	18
13. Droit applicable et lieu de juridiction	18
3. Informativa sulla protezione dei dati dell'app ELVIDA	19
1. Generalità	19
2. Titolare del trattamento dei dati	19
3. Raccolta e trattamento dei dati personali	19
3.1 Registrazione e dati dell'account	19

3.2 Caricamento e archiviazione dei documenti	20
3.3 Situazione assicurativa (comportamento nell'app)	21
3.4 Dati di pagamento	21
3.5 Comunicazione	21
4. Trattamento IA (OpenAI)	21
5. Trasferimenti internazionali di dati	22
6. Responsabili del trattamento	23
7. Sicurezza dei dati	23
8. Durata di conservazione e cancellazione	24
9. I vostri diritti	24
10. Violazioni dei dati e incidenti di sicurezza	25
11. Processo decisionale automatizzato	26
12. Modifiche alla presente informativa sulla protezione dei dati	26
13. Diritto applicabile e foro competente	26
4. ELVIDA App Privacy Policy	27
1. General	27
2. Data Controller	27
3. Collection and Processing of Personal Data	27
3.1 Registration and Account Data	27
3.2 Document Uploads and Storage	28
3.3 Insurance situation (app behavior)	28
3.4 Payment Data	29
3.5 Communication	29
4. AI Processing (OpenAI)	29
5. International Data Transfers	30
6. Processors	31
7. Data Security	31
8. Retention Periods and Deletion	32
9. Your Rights	32
10. Data Breaches and Security Incidents	33
11. Automated Decision-Making	33
12. Changes to This Privacy Policy	33
13. Applicable Law and Jurisdiction	33

1. Datenschutzerklärung ELVIDA App

Letzte Überarbeitung: Februar 2026

Dokumentenstatus: Diese Datenschutzerklärung ist als PDF in der ELVIDA-App unter "Einstellungen > Daten & Konto" verfügbar.

Geltungsbereich: Diese Datenschutzerklärung gilt für die ELVIDA-App und die damit verbundenen Dienste. Für die Website elvida.app gilt eine separate Datenschutzerklärung.

1. Allgemeines

C. Camenzind GmbH, Betreiberin der ELVIDA-App ("wir"/"uns"), ist dem Schutz Ihrer Personendaten verpflichtet. Diese Erklärung beschreibt:

- welche Personendaten wir erheben und bearbeiten,
- zu welchem Zweck und auf welcher Rechtsgrundlage,
- an wen wir Daten weitergeben,
- wie lange wir Daten speichern,
- welche Rechte Ihnen zustehen.

Personendaten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen (z.B. Name, E-Mail-Adresse, IP-Adresse).

2. Datenverantwortlicher

C. Camenzind GmbH
Furrenstrasse 5
6442 Gersau
Schweiz

Kontakt Datenschutz:

E-Mail: info@elvida.app

Bei Fragen zur Verarbeitung Ihrer Personendaten wenden Sie sich bitte an uns unter der oben genannten Adresse.

3. Erhebung und Verarbeitung von Personendaten

3.1 Registrierung und Kontodaten

Bei der Erstellung eines ELVIDA-Kontos erheben wir:

- E-Mail-Adresse

- Passwort (verschlüsselt gespeichert)
- Zeitpunkt der Registrierung
- Spracheinstellung

Zweck: Bereitstellung der App-Funktionalitäten, Authentifizierung

Rechtsgrundlage: Vertragserfüllung (Art. 13 FADP / Art. 6 Abs. 1 lit. b DSGVO)

Speicherdauer: Bis zur Kontolöschung

3.2 Dokumentenuploads und -speicherung

Sie können Dokumente in die ELVIDA-App hochladen. Dabei verarbeiten wir:

- Hochgeladene Dokumente (Verträge, Rechnungen, Versicherungen etc.)
- Metadaten (Dateiname, Titel, Dokumentdatum, OCR-Text, Textlänge, KI-Zusammenfassung)

Zweck: Verschlüsselte Speicherung und Organisation Ihrer persönlichen Verwaltungsunterlagen

Rechtsgrundlage: Vertragserfüllung (Art. 13 FADP / Art. 6 Abs. 1 lit. b DSGVO)

Speicherdauer: Bis zur Löschung durch Sie oder Kontolöschung

Sicherheit und Verschlüsselung:

Dokumenteninhalte (PDF-Dateien, Bilder), OCR-Texte und KI-generierte Zusammenfassungen werden mit AES-GCM-256 verschlüsselt gespeichert. Technische Metadaten (z.B. Zeitstempel, Dateigröße, Speicherort) sowie kryptographische Parameter (Initialisierungsvektoren, Schlüsselversionen) werden unverschlüsselt gespeichert, sind jedoch für den Dateninhalt nicht rekonstruierbar.

Komponente	Technische Umsetzung
Algorithmus	AES-GCM (Authenticated Encryption)
Schlüssellänge	256-bit
IV (Initialisierungsvektor)	12 Bytes (96-bit), pro Verschlüsselung eindeutig
Authentifizierungs-Tag	16 Bytes (128-bit) zur Integritätsprüfung
Schlüsselableitung	Nutzer-ID als Schlüsselmaterial (Key Version 1); zukünftig PBKDF2 mit SHA-256 und 100.000 Iterationen (Key Version 2+)

Speicherung in der Datenbank:

- encrypted_metadata – Base64-verschlüsselter Text
- metadata_encryption_iv – Base64-IV
- metadata_encryption_tag – Base64-Authentifizierungs-Tag
- metadata_encryption_key_version – Schlüsselversion

Wichtig:

- Die Verschlüsselung erfolgt server-seitig mit schlüsselgeleitetem Zugriff
- Das ELVIDA-Team hat keinen routine-mässigen Zugriff auf Ihre Dokumenteninhalte
- Bei Verlust Ihres Passworts können wir Ihre Daten nicht wiederherstellen – Sie müssen Ihr Konto zurücksetzen (siehe Abschnitt 9)
- Die KI-Analyse zur Extraktion von Fristen und Informationen erfolgt über die OpenAI API (siehe Abschnitt 4) und ist in unseren AGB als Produktfeature festgelegt

3.3 Versicherungssituation (App-Verhalten)

Wir erheben unidentifizierbare Daten zur Verbesserung unserer Dienste:

- Interaktionen im ELVIDA Dashboard (geklickte Features, genutzte Funktionen)
- App-Performance-Daten (Ladezeiten, Fehler)
- Aggregierte Nutzungsstatistiken

Zweck: Verbesserung der App-Funktionalität, Fehlerbehebung

Rechtsgrundlage: Berechtigtes Interesse (Art. 13 FADP / Art. 6 Abs. 1 lit. f DSGVO)

Hinweis: Diese Daten sind nicht mit Ihrer Person verknüpfbar (Pseudonymisierung).

3.4 Zahlungsdaten

Für kostenpflichtige Funktionen verarbeiten wir über Stripe:

- Zahlungsinformationen (Kreditkartennummer wird nicht von uns gespeichert)
- Rechnungsadresse
- Transaktionshistorie

Zweck: Abwicklung von Zahlungen

Rechtsgrundlage: Vertragserfüllung (Art. 13 FADP / Art. 6 Abs. 1 lit. b DSGVO)

Speicherdauer: 10 Jahre (gesetzliche Aufbewahrungspflicht)

Hinweis: Zahlungsdaten werden direkt von Stripe verarbeitet. Wir speichern keine vollständigen Kreditkartendaten.

3.5 Kommunikation

Für Transaktions-E-Mails (z.B. Passwort-Reset, Dokumentenbenachrichtigungen) und Marketing:

- E-Mail-Adresse
- Öffnungs- und Klickraten (anonymisiert)

Zweck: Service-Kommunikation und Marketing (nur mit Einwilligung)

Rechtsgrundlage: Vertragserfüllung (Transaktionsmails) / Einwilligung (Marketing)

Speicherdauer: Bis zur Abmeldung

4. KI-Verarbeitung (OpenAI)

Wir nutzen die OpenAI API für die KI-gestützte Analyse Ihrer Dokumente innerhalb der ELVIDA-App. Diese Funktion ist ein integraler Bestandteil unseres Produkts und in unseren AGB festgelegt.

Detail	Beschreibung
Anbieter	OpenAI, L.L.C., 3180 18th Street, San Francisco, CA 94110, USA
Verarbeitete Daten	Inhalte hochgeladener Dokumente (z.B. Vertragstexte, Rechnungsdetails)
Zweck	Extraktion von Fristen, Beträgen, Vertragsparteien und wichtigen Informationen für den ELVIDA AI-Agenten
Rechtsgrundlage	Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO / Art. 13 FADP) – Die KI-Analyse ist ein vertragswesentliches Produktfeature gemäss unserer AGB

Datenschutz und Speicherung bei OpenAI:

- Anonymisierte Übertragung: Dokumenteninhalte werden zur Analyse an einen externen LLM-Provider (USA) übermittelt. Die Übertragung erfolgt verschlüsselt. Wir minimieren personenbezogene Daten in Metadaten (Titel, Beschreibungen); die Verarbeitung durch den Provider unterliegt strikten Vertragsauflagen ohne Nutzung für Trainingszwecke.
- Keine Speicherung zu Trainingszwecken: OpenAI verwendet Ihre Daten nicht zum Training von KI-Modellen oder zur Verbesserung ihrer Dienste.
- Temporäre Speicherung aus Sicherheitsgründen: Dokumenteninhalte werden ausschliesslich zur sofortigen Analyse an OpenAI übermittelt und maximal 30 Tage zu Sicherheitszwecken (Fraud Prevention, Abuse Detection) vorgehalten. Danach werden sie automatisch gelöscht.
- Löschung auf Anfrage: Wir senden OpenAI alle 30 Tage eine Löschanfrage für alle verarbeiteten Daten. Bei Ihrem konkreten Löschverlangen (siehe Abschnitt 9) fordern wir die sofortige Löschung bei OpenAI explizit an.
- Keine dauerhafte Speicherung: OpenAI speichert keine Kopien Ihrer Dokumente nach Ablauf der 30-tägigen Sicherheitsfrist.

Weitere Informationen:

[OpenAI API Data Usage Policies](#)

5. Internationale Datenübermittlung

Wir übermitteln Personendaten in Länder ausserhalb der Schweiz und des EWR:

Empfänger	Standort	Zweck	Garantien
-----------	----------	-------	-----------

Exoscale (A1 Digital)	Schweiz	Verschlüsselte Dokumentenspeicherung	Keine Übermittlung (Schweizer Server)
Stripe, Inc.	USA	Zahlungsabwicklung	Standardvertragsklauseln (SCC)
OpenAI, L.L.C.	USA	KI-Analyse von Dokumenten	Standardvertragsklauseln (SCC) + Zero-Retention
Loops Labs Inc.	USA	E-Mail-Versand (Transaktionen/Marketing)	Standardvertragsklauseln (SCC)

Für Übermittlungen in die USA (OpenAI, Stripe, Loops) wurde ein Transfer Impact Assessment (TIA) durchgeführt. Zusätzlich zu den Standardvertragsklauseln (SCC) setzen wir folgende ergänzende Massnahmen ein:

- OpenAI: Daten werden verschlüsselt übermittelt; keine Speicherung zu Trainingszwecken vertraglich ausgeschlossen
- Stripe/Loops: Pseudonymisierung sensibler Daten wo möglich

Die USA verfügen nicht über ein dem Schweizer bzw. EU-Datenschutzrecht gleichwertiges Datenschutzniveau. Die Übermittlung erfolgt auf Grundlage von Standardvertragsklauseln gemäss Art. 16 FADP bzw. Art. 46 DSGVO.

6. Auftragsverarbeiter

Wir setzen folgende Dienstleister als Auftragsverarbeiter ein:

Dienstleister	Tätigkeit	Standort	Vertrag
Exoscale (A1 Digital)	Cloud-Speicher für Dokumente	Schweiz	Auftragsverarbeitungsvertrag (AVV)
Stripe, Inc.	Zahlungsabwicklung	USA	Auftragsverarbeitungsvertrag (AVV)
OpenAI, L.L.C.	KI-Verarbeitung	USA	Auftragsverarbeitungsvertrag (AVV)
Loops Labs Inc.	E-Mail-Versand	USA	Auftragsverarbeitungsvertrag (AVV)

Alle Auftragsverarbeiter sind vertraglich zur Einhaltung datenschutzrechtlicher Vorgaben verpflichtet.

7. Datensicherheit

Wir setzen folgende technische und organisatorische Massnahmen zum Schutz Ihrer Daten ein:

Massnahme	Beschreibung
Verschlüsselung (AES-GCM)	Alle Dokumente und Metadaten werden mit AES-GCM (256-bit) verschlüsselt gespeichert
Authentifizierte Verschlüsselung	AES-GCM stellt sicher, dass Daten nicht manipuliert werden können (Authentifizierungs-Tag)
Schlüsselableitung	Schlüssel werden aus Nutzer-ID abgeleitet (zukünftig PBKDF2 mit 100.000 Iterationen)
Verschlüsselte Übertragung	SSL/TLS für alle Datenübertragungen
Zugriffsbeschränkungen	Zugriff nur für autorisierte Personen (2FA)
Zugriffsprotokollierung	Logbuch aller Zugriffsversuche
Pseudonymisierung	Nutzungsdaten werden pseudonymisiert verarbeitet
Regelmässige Sicherheitsupdates	Aktualisierung aller Systeme
Backups	Regelmässige, verschlüsselte Backups bei Exoscale

8. Speicherdauer und Löschung

Datenkategorie	Aufbewahrungsdauer	Grundlage
Kontodaten	Bis zur Kontolöschung	Vertragserfüllung

Dokumente	Bis zur Löschung durch Nutzer/Kontolöschung	Vertragserfüllung
Zahlungsdaten	10 Jahre	Gesetzliche Pflicht
Nutzungsdaten (anonym)	2 Jahre	Berechtigtes Interesse
Transaktions-E-Mails	2 Jahre	Vertragserfüllung
Marketing-Einwilligungen	Bis zur Abmeldung	Einwilligung

Automatische Löschung: Nach Kontolöschung werden alle personenbezogenen Daten innerhalb von 30 Tagen automatisch gelöscht (Ausnahme: Zahlungsdaten gemäss gesetzlicher Aufbewahrung).

9. Ihre Rechte

Ihnen stehen folgende Rechte zu:

Recht	Beschreibung
Auskunft	Information über Ihre gespeicherten Personendaten
Berichtigung	Korrektur unrichtiger Daten
Löschung	Löschung Ihrer Daten ("Recht auf Vergessenwerden")
Einschränkung	Einschränkung der Verarbeitung
Widerspruch	Widerspruch gegen die Verarbeitung
Datenübertragbarkeit	Export Ihrer Daten (z.B. Dokumente)
Widerruf	Jederzeitiger Widerruf der Einwilligung

Ausübung Ihrer Rechte:

Kontaktieren Sie uns unter info@elvida.app.

Wichtig zur Löschung:

- Sie können Ihr Konto jederzeit in den App-Einstellungen löschen

- Bei Kontolöschung werden alle Ihre Dokumente, Metadaten und personenbezogenen Daten unwiderruflich gelöscht
- Bei Löschanfragen fordern wir sofort die Löschung bei OpenAI an (E-Mail an OpenAI Support mit Ihrer Nutzer-ID zur Identifikation)
- Für die Löschung müssen wir Ihre Identität verifizieren (z.B. über Ihre registrierte E-Mail-Adresse)

Hinweis: Bei Verlust Ihres Passworts können wir Ihre verschlüsselten Daten nicht wiederherstellen. Sie müssen Ihr Konto zurücksetzen, wodurch alle Daten gelöscht werden.

Beschwerde: [Schweizerische Datenschutz- und Öffentlichkeitsbeauftragte \(EDÖB\)](#)

10. Datenlecks und Sicherheitsvorfälle

Im Falle eines Datenlecks oder Sicherheitsvorfalls, der Ihre Personendaten betrifft, benachrichtigen wir:

- Die Schweizerische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) innerhalb von 72 Stunden, sofern das Risiko für Ihre Rechte und Freiheiten hoch ist
 - Sie als betroffene Person unverzüglich, wenn das Datenleck ein hohes Risiko für Ihre Rechte und Freiheiten darstellt
-

11. Automatisierte Entscheidungsfindung

Wir verwenden keine ausschliesslich auf automatisierter Verarbeitung beruhende Entscheidungsfindung, die rechtliche Wirkungen entfaltet oder Sie erheblich beeinträchtigt (Art. 21 FADP / Art. 22 DSGVO).

12. Änderungen dieser Datenschutzerklärung

Wir behalten uns vor, diese Datenschutzerklärung anzupassen. Die aktuelle Version ist stets in der App und auf elvida.app/datenschutz verfügbar.

13. Anwendbares Recht und Gerichtsstand

Diese Datenschutzerklärung unterliegt schweizerischem Recht. Ausschliesslicher Gerichtsstand für alle Streitigkeiten ist Gersau, Schweiz.

2. Déclaration de protection des données de l'application ELVIDA

Dernière révision : Février 2026

Statut du document : Cette déclaration de protection des données est disponible au format PDF dans l'application ELVIDA sous « Paramètres > Données & Compte ».

Champ d'application : Cette déclaration de protection des données s'applique à l'application ELVIDA et aux services associés. Pour le site web elvida.app, une déclaration de protection des données distincte s'applique.

1. Généralités

C. Camenzind GmbH, exploitante de l'application ELVIDA (« nous »), s'engage à protéger vos données personnelles. Cette déclaration décrit :

- quelles données personnelles nous collectons et traitons,
 - à quelle fin et sur quelle base juridique,
 - à qui nous transmettons les données,
 - combien de temps nous conservons les données,
 - quels droits vous avez. Les données personnelles sont toutes les informations relatives à une personne identifiée ou identifiable (par exemple nom, adresse e-mail, adresse IP).
-

2. Responsable du traitement des données

C. Camenzind GmbH Furrenstrasse 5 6442 Gersau Suisse Contact protection des données : E-mail : info@elvida.app Pour toute question concernant le traitement de vos données personnelles, veuillez nous contacter à l'adresse ci-dessus.

3. Collecte et traitement des données personnelles

3.1 Inscription et données de compte

Lors de la création d'un compte ELVIDA, nous collectons :

- Adresse e-mail
- Mot de passe (stocké de manière cryptée)
- Date d'inscription

- Paramètre de langue Finalité : Fourniture des fonctionnalités de l'application, authentification Base juridique : Exécution du contrat (art. 13 LPD / art. 6 par. 1 let. b RGPD) Durée de conservation : Jusqu'à la suppression du compte

3.2 Téléchargement et stockage de documents

Vous pouvez télécharger des documents dans l'application ELVIDA. Nous traitons alors :

- Documents téléchargés (contrats, factures, assurances, etc.)
- Métadonnées (nom de fichier, titre, date du document, texte OCR, longueur du texte, résumé IA) Finalité : Stockage crypté et organisation de vos documents administratifs personnels Base juridique : Exécution du contrat (art. 13 LPD / art. 6 par. 1 let. b RGPD) Durée de conservation : Jusqu'à la suppression par vous ou suppression du compte

Les contenus de documents (fichiers PDF, images), les textes OCR et les résumés générés par IA sont stockés cryptés avec AES-GCM-256. Les métadonnées techniques (p.ex. horodatages, taille de fichier, emplacement de stockage) ainsi que les paramètres cryptographiques (vecteurs d'initialisation, versions de clé) sont stockés non cryptés, mais ne permettent pas de reconstituer le contenu des données.

Composant	Mise en œuvre technique
Algorithme	AES-GCM (chiffrement authentifié)
Longueur de clé	256 bits
IV (vecteur d'initialisation)	12 octets (96 bits), unique par cryptage
Tag d'authentification	16 octets (128 bits) pour la vérification d'intégrité
Dérivation de clé	ID utilisateur comme matériel de clé (Version de clé 1) ; à l'avenir PBKDF2 avec SHA-256 et 100 000 itérations (Version de clé 2+)

Stockage dans la base de données :

- encrypted_metadata – Texte crypté en Base64
- metadata_encryption_iv – IV en Base64
- metadata_encryption_tag – Tag d'authentification en Base64
- metadata_encryption_key_version – Version de clé

Important :

- Le cryptage s'effectue côté serveur avec accès guidé par clé
- L'équipe ELVIDA n'a pas accès de routine au contenu de vos documents
- En cas de perte de votre mot de passe, nous ne pouvons pas restaurer vos données – vous devez réinitialiser votre compte (voir section 9)
- L'analyse IA pour l'extraction d'échéances et d'informations s'effectue via l'API OpenAI (voir section 4) et est définie comme fonctionnalité produit dans nos CGV

3.3 Situation d'assurance (comportement dans l'app)

Nous collectons des données non identifiables pour améliorer nos services :

- Interactions dans le tableau de bord ELVIDA (fonctionnalités cliquées, fonctions utilisées)
- Données de performance de l'application (temps de chargement, erreurs)
- Statistiques d'utilisation agrégées Finalité : Amélioration des fonctionnalités de l'application, correction d'erreurs Base juridique : Intérêt légitime (art. 13 LPD / art. 6 par. 1 let. f RGPD) Remarque : Ces données ne sont pas associables à votre personne (pseudonymisation).

3.4 Données de paiement

Pour les fonctionnalités payantes, nous traitons via Stripe :

- Informations de paiement (le numéro de carte de crédit n'est pas stocké par nous)
- Adresse de facturation
- Historique des transactions Finalité : Traitement des paiements Base juridique : Exécution du contrat (art. 13 LPD / art. 6 par. 1 let. b RGPD) Durée de conservation : 10 ans (obligation légale de conservation) Remarque : Les données de paiement sont traitées directement par Stripe. Nous ne stockons pas les données complètes des cartes de crédit.

3.5 Communication

Pour les e-mails transactionnels (par exemple réinitialisation de mot de passe, notifications de documents) et le marketing :

- Adresse e-mail
- Taux d'ouverture et de clics (anonymisés) **Finalité** : Communication de service et marketing (uniquement avec consentement) **Base juridique** : Exécution du contrat (e-mails transactionnels) / Consentement (marketing) **Durée de conservation** : Jusqu'à la désinscription

4. Traitement IA (OpenAI)

Nous utilisons l'API OpenAI pour l'analyse IA de vos documents au sein de l'application ELVIDA. Cette fonction est une partie intégrante de notre produit et est définie dans nos CGV.

Détail	Description
Fournisseur	OpenAI, L.L.C., 3180 18th Street, San Francisco, CA 94110, USA
Données traitées	Contenus des documents téléchargés (par exemple textes de contrats, détails de factures)

Finalité	Extraction d'échéances, montants, parties contractantes et informations importantes pour l'agent IA ELVIDA
Base juridique	Exécution du contrat (art. 6 par. 1 let. b RGPD / art. 13 LPD) – L'analyse IA est une fonctionnalité produit essentielle au contrat selon nos CGV

Protection des données et stockage chez OpenAI :

- Les contenus des documents sont transmis à un fournisseur LLM externe (USA) pour analyse. La transmission s'effectue cryptée. Nous minimisons les données personnelles dans les métadonnées (titres, descriptions) ; le traitement par le fournisseur est soumis à des exigences contractuelles strictes sans utilisation à des fins de formation.
- Aucun stockage à des fins de formation : OpenAI n'utilise pas vos données pour entraîner des modèles d'IA ou améliorer ses services.
- Stockage temporaire pour des raisons de sécurité : Les contenus de documents sont transmis à OpenAI exclusivement pour analyse immédiate et conservés maximum 30 jours à des fins de sécurité (prévention de fraude, détection d'abus). Ils sont ensuite automatiquement supprimés.
- Suppression sur demande : Nous envoyons à OpenAI toutes les 30 jours une demande de suppression de toutes les données traitées. Lors de votre demande de suppression spécifique (voir section 9), nous demandons explicitement la suppression immédiate chez OpenAI.
- Aucun stockage permanent : OpenAI ne conserve aucune copie de vos documents après l'expiration du délai de sécurité de 30 jours.

Informations complémentaires : [OpenAI API Data Usage Policies](#)

5. Transferts internationaux de données

Nous transmettons des données personnelles vers des pays en dehors de la Suisse et de l'EEE:

Destinataire	Lieu	Finalité	Garanties
Exoscale (A1 Digital)	Suisse	Stockage crypté de documents	Aucun transfert (serveurs suisses)
Stripe, Inc.	USA	Traitement des paiements	Clauses contractuelles types (CCT)
OpenAI, L.L.C.	USA	Analyse IA de documents	Clauses contractuelles types (CCT) + Zero-Retention
Loops Labs Inc.	USA	Envoi d'e-mails (transactions/marketing)	Clauses contractuelles types (CCT)

Pour les transferts vers les USA (OpenAI, Stripe, Loops), une évaluation d'impact du transfert (EIT) a été effectuée. En complément des clauses contractuelles types (CCT), nous mettons en œuvre les mesures supplémentaires suivantes :

- OpenAI : Les données sont transmises cryptées ; aucun stockage à des fins de formation est exclu contractuellement
- Stripe/Loops : Pseudonymisation des données sensibles lorsque possible

Les USA ne disposent pas d'un niveau de protection des données équivalent à la législation suisse ou européenne. Le transfert s'effectue sur la base de clauses contractuelles types conformément à l'art. 16 LPD et à l'art. 46 RGPD.

6. Sous-traitants

Nous utilisons les prestataires suivants comme sous-traitants :

Prestataire	Activité	Lieu	Contrat
Exoscale (A1 Digital)	Stockage cloud pour documents	Suisse	Contrat de sous-traitance
Stripe, Inc.	Traitement des paiements	USA	Contrat de sous-traitance
OpenAI, L.L.C.	Traitement IA	USA	Contrat de sous-traitance
Loops Labs Inc.	Envoi d'e-mails	USA	Contrat de sous-traitance

Tous les sous-traitants sont contractuellement tenus de respecter les exigences de protection des données.

7. Sécurité des données

Nous mettons en œuvre les mesures techniques et organisationnelles suivantes pour protéger vos données :

Mesure	Description
Cryptage (AES-GCM)	Tous les documents et métadonnées sont stockés cryptés avec AES-GCM (256 bits)

Cryptage authentifié	AES-GCM garantit que les données ne peuvent pas être manipulées (tag d'authentification)
Dérivation de clé	Les clés sont dérivées de l'ID utilisateur (à l'avenir PBKDF2 avec 100 000 itérations)
Transmission cryptée	SSL/TLS pour toutes les transmissions de données
Restrictions d'accès	Accès uniquement pour personnes autorisées (2FA)
Journalisation des accès	Registre de toutes les tentatives d'accès
Pseudonymisation	Les données d'utilisation sont traitées de manière pseudonymisée
Mises à jour de sécurité régulières	Mise à jour de tous les systèmes
Sauvegardes	Sauvegardes régulières cryptées chez Exoscale

8. Durée de conservation et suppression

Catégorie de données	Durée de conservation	Fondement
Données de compte	Jusqu'à la suppression du compte	Exécution du contrat
Documents	Jusqu'à la suppression par l'utilisateur/suppression du compte	Exécution du contrat
Données de paiement	10 ans	Obligation légale
Données d'utilisation (anonymes)	2 ans	Intérêt légitime
E-mails transactionnels	2 ans	Exécution du contrat
Consentements marketing	Jusqu'à la désinscription	Consentement

Suppression automatique : Après suppression du compte, toutes les données personnelles sont automatiquement supprimées dans un délai de 30 jours (exception : données de paiement selon l'obligation légale de conservation).

9. Vos droits Vous disposez des droits suivants :

Droit	Description
Accès	Information sur vos données personnelles stockées
Rectification	Correction de données inexactes
Effacement	Suppression de vos données (« droit à l'oubli »)
Limitation	Limitation du traitement
Opposition	Opposition au traitement
Portabilité	Export de vos données (par exemple documents)
Révocation	Révocation à tout moment du consentement

Exercice de vos droits : Contactez-nous à info@elvida.app.

Important concernant la suppression :

- Vous pouvez supprimer votre compte à tout moment dans les paramètres de l'application
- Lors de la suppression du compte, tous vos documents, métadonnées et données personnelles sont irrévocablement supprimés
- Lors des demandes de suppression, nous demandons immédiatement la suppression chez OpenAI (e-mail au support OpenAI avec votre ID utilisateur pour identification)
- Pour la suppression, nous devons vérifier votre identité (par exemple via votre adresse e-mail enregistrée)

Remarque : En cas de perte de votre mot de passe, nous ne pouvons pas restaurer vos données cryptées. Vous devez réinitialiser votre compte, ce qui entraîne la suppression de toutes les données.

Réclamation : [Préposée fédérale à la protection des données et à la transparence \(PFPDT\)](#)

10. Fuites de données et incidents de sécurité

En cas de fuite de données ou d'incident de sécurité affectant vos données personnelles, nous informons :

- La Préposée fédérale à la protection des données et à la transparence (PFPDT) dans un délai de 72 heures, si le risque pour vos droits et libertés est élevé
 - Vous en tant que personne concernée sans délai, si la fuite de données présente un risque élevé pour vos droits et libertés
-

11. Prise de décision automatisée

Nous n'utilisons pas de prise de décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques ou vous affectant de manière significative (art. 21 LPD / art. 22 RGPD).

12. Modifications de cette déclaration de protection des données

Nous nous réservons le droit de modifier cette déclaration de protection des données. La version actuelle est toujours disponible dans l'application et sur elvida.app/datenschutz.

13. Droit applicable et lieu de juridiction

Cette déclaration de protection des données est soumise au droit suisse. Le lieu de juridiction exclusif pour tous les litiges est Gersau, Suisse.

3. Informativa sulla protezione dei dati dell'app ELVIDA

Ultima revisione: Febbraio 2026

Stato del documento: Questa informativa sulla protezione dei dati è disponibile in formato PDF nell'applicazione ELVIDA in "Impostazioni > Dati & Account".

Ambito di applicazione: Questa informativa sulla protezione dei dati si applica all'app ELVIDA e ai servizi ad essa collegati. Per il sito web elvida.app si applica un'informativa sulla protezione dei dati separata.

1. Generalità

C. Camenzind GmbH, gestore dell'app ELVIDA ("noi"), è impegnata nella protezione dei vostri dati personali. La presente dichiarazione descrive:

- quali dati personali raccogliamo e trattiamo,
- a quale scopo e su quale base giuridica,
- a chi trasmettiamo i dati,
- per quanto tempo conserviamo i dati,
- quali diritti vi spettano. I dati personali sono tutte le informazioni relative a una persona identificata o identificabile (ad esempio nome, indirizzo e-mail, indirizzo IP).

2. Titolare del trattamento dei dati

C. Camenzind GmbH Furrenstrasse 5 6442 Gersau Svizzera Contatto protezione dati: E-mail: info@elvida.app Per qualsiasi domanda relativa al trattamento dei vostri dati personali, vi preghiamo di contattarci all'indirizzo sopra indicato.

3. Raccolta e trattamento dei dati personali

3.1 Registrazione e dati dell'account

Durante la creazione di un account ELVIDA raccogliamo:

- Indirizzo e-mail
- Password (memorizzata in forma criptata)
- Data di registrazione

- Impostazione della lingua Finalità: Fornitura delle funzionalità dell'app, autenticazione
Base giuridica: Esecuzione del contratto (art. 13 LPD / art. 6 co. 1 lett. b GDPR) Durata di conservazione: Fino alla cancellazione dell'account

3.2 Caricamento e archiviazione dei documenti

Potete caricare documenti nell'app ELVIDA. Trattiamo quindi:

- Documenti caricati (contratti, fatture, assicurazioni, ecc.)
- Metadati (nome del file, titolo, data del documento, testo OCR, lunghezza del testo, riassunto IA) Finalità: Archiviazione criptata e organizzazione dei vostri documenti amministrativi personali Base giuridica: Esecuzione del contratto (art. 13 LPD / art. 6 co. 1 lett. b GDPR) Durata di conservazione: Fino alla cancellazione da parte vostra o alla cancellazione dell'account

I contenuti dei documenti (file PDF, immagini), i testi OCR e i riassunti generati dall'IA sono archiviati crittografati con AES-GCM-256. I metadati tecnici (ad es. timestamp, dimensione del file, posizione di archiviazione) nonché i parametri crittografici (vettori di inizializzazione, versioni delle chiavi) sono archiviati non crittografati, ma non consentono di ricostruire il contenuto dei dati.

Componente	Implementazione tecnica
Algoritmo	AES-GCM (crittografia autenticata)
Lunghezza della chiave	256 bit
IV (vettore di inizializzazione)	12 byte (96 bit), unico per ogni crittografia
Tag di autenticazione	16 byte (128 bit) per la verifica dell'integrità
Derivazione della chiave	ID utente come materiale chiave (Versione chiave 1); in futuro PBKDF2 con SHA-256 e 100.000 iterazioni (Versione chiave 2+)

Archiviazione nel database:

- encrypted_metadata – Testo criptato in Base64
- metadata_encryption_iv – IV in Base64
- metadata_encryption_tag – Tag di autenticazione in Base64
- metadata_encryption_key_version – Versione della chiave

Importante:

- La crittografia avviene lato server con accesso guidato dalla chiave
- Il team ELVIDA non ha accesso di routine al contenuto dei vostri documenti
- In caso di perdita della vostra password, non possiamo ripristinare i vostri dati – dovete reimpostare il vostro account (vedi sezione 9)
- L'analisi IA per l'estrazione di scadenze e informazioni avviene tramite l'API OpenAI (vedi sezione 4) ed è definita come funzionalità del prodotto nelle nostre CGV

3.3 Situazione assicurativa (comportamento nell'app)

Raccogliamo dati non identificabili per migliorare i nostri servizi:

- Interazioni nella dashboard ELVIDA (funzionalità cliccate, funzioni utilizzate)
- Dati sulle prestazioni dell'app (tempi di caricamento, errori)
- Statistiche di utilizzo aggregate Finalità: Miglioramento delle funzionalità dell'app, correzione degli errori Base giuridica: Interesse legittimo (art. 13 LPD / art. 6 co. 1 lett. f GDPR) Nota: Questi dati non sono associabili alla vostra persona (pseudonimizzazione).

3.4 Dati di pagamento

Per le funzionalità a pagamento, trattiamo tramite Stripe:

- Informazioni di pagamento (il numero della carta di credito non è memorizzato da noi)
- Indirizzo di fatturazione
- Cronologia delle transazioni Finalità: Elaborazione dei pagamenti Base giuridica: Esecuzione del contratto (art. 13 LPD / art. 6 co. 1 lett. b GDPR) Durata di conservazione: 10 anni (obbligo legale di conservazione) Nota: I dati di pagamento sono trattati direttamente da Stripe. Non memorizziamo i dati completi delle carte di credito.

3.5 Comunicazione

Per le e-mail transazionali (ad esempio reimpostazione password, notifiche documenti) e il marketing:

- Indirizzo e-mail
- Tassi di apertura e clic (anonimizzati) Finalità: Comunicazione di servizio e marketing (solo con consenso) Base giuridica: Esecuzione del contratto (e-mail transazionali) / Consenso (marketing) Durata di conservazione: Fino alla disiscrizione

4. Trattamento IA (OpenAI)

Utilizziamo l'API OpenAI per l'analisi IA dei vostri documenti all'interno dell'app ELVIDA. Questa funzione è parte integrante del nostro prodotto ed è definita nelle nostre CGV.

Dettaglio	Descrizione
Fornitore	OpenAI, L.L.C., 3180 18th Street, San Francisco, CA 94110, USA
Dati trattati	Contenuti dei documenti caricati (ad esempio testi di contratti, dettagli delle fatture)
Finalità	Estrazione di scadenze, importi, parti contraenti e informazioni importanti per l'agente IA ELVIDA

Base giuridica	Esecuzione del contratto (art. 6 co. 1 lett. b GDPR / art. 13 LPD) – L'analisi IA è una funzionalità del prodotto essenziale per il contratto secondo le nostre CGV
----------------	---

Protezione dei dati e archiviazione presso OpenAI:

- I contenuti dei documenti vengono trasmessi a un provider LLM esterno (USA) per l'analisi. La trasmissione avviene crittografata. Minimizziamo i dati personali nei metadati (titoli, descrizioni); il trattamento da parte del provider è soggetto a rigorose esigenze contrattuali senza utilizzo per scopi di formazione.
- Nessuna archiviazione per scopi di formazione: OpenAI non utilizza i vostri dati per addestrare modelli di IA o migliorare i propri servizi.
- Archiviazione temporanea per motivi di sicurezza: I contenuti dei documenti sono trasmessi a OpenAI esclusivamente per analisi immediata e conservati al massimo 30 giorni per scopi di sicurezza (prevenzione delle frodi, rilevamento degli abusi). Successivamente vengono automaticamente cancellati.
- Cancellazione su richiesta: Inviaamo a OpenAI ogni 30 giorni una richiesta di cancellazione di tutti i dati trattati. In caso di vostra specifica richiesta di cancellazione (vedi sezione 9), richiediamo esplicitamente la cancellazione immediata presso OpenAI.
- Nessuna archiviazione permanente: OpenAI non conserva copie dei vostri documenti dopo la scadenza del termine di sicurezza di 30 giorni.

Ulteriori informazioni: [OpenAI API Data Usage Policies](#)

5. Trasferimenti internazionali di dati

Trasmettiamo dati personali verso paesi al di fuori della Svizzera e dello Spazio economico europeo (SEE):

Destinatario	Luogo	Finalità	Garanzie
Exoscale (A1 Digital)	Svizzera	Archiviazione criptata dei documenti	Nessun trasferimento (server svizzeri)
Stripe, Inc.	USA	Elaborazione dei pagamenti	Clausole contrattuali tipo (CCT)
OpenAI, L.L.C.	USA	Analisi IA dei documenti	Clausole contrattuali tipo (CCT) + Zero-Retention
Loops Labs Inc.	USA	Invio di e-mail (transazioni/marketing)	Clausole contrattuali tipo (CCT)

Per i trasferimenti verso gli USA (OpenAI, Stripe, Loops) è stata effettuata una valutazione d'impatto del trasferimento (DPIA). In aggiunta alle clausole contrattuali tipo (CCT), implementiamo le seguenti misure supplementari:

- OpenAI: I dati sono trasmessi in forma criptata; nessuna archiviazione per scopi di formazione è esclusa contrattualmente
- Stripe/Loops: Pseudonimizzazione dei dati sensibili ove possibile

Gli USA non dispongono di un livello di protezione dei dati equivalente alla legislazione svizzera o europea. Il trasferimento avviene sulla base di clausole contrattuali tipo ai sensi dell'art. 16 LPD e dell'art. 46 GDPR.

6. Responsabili del trattamento

Utilizziamo i seguenti fornitori come responsabili del trattamento:

Fornitore	Attività	Luogo	Contratto
Exoscale (A1 Digital)	Archiviazione cloud per documenti	Svizzera	Contratto di trattamento dati
Stripe, Inc.	Elaborazione dei pagamenti	USA	Contratto di trattamento dati
OpenAI, L.L.C.	Trattamento IA	USA	Contratto di trattamento dati
Loops Labs Inc.	Invio di e-mail	USA	Contratto di trattamento dati

Tutti i responsabili del trattamento sono obbligati contrattualmente a rispettare i requisiti di protezione dei dati.

7. Sicurezza dei dati

Implementiamo le seguenti misure tecniche e organizzative per proteggere i vostri dati:

Misura	Descrizione
Crittografia (AES-GCM)	Tutti i documenti e i metadati sono archiviati con crittografia AES-GCM (256 bit)
Crittografia autenticata	AES-GCM garantisce che i dati non possano essere manipolati (tag di autenticazione)

Derivazione della chiave	Le chiavi sono derivate dall'ID utente (in futuro PBKDF2 con 100.000 iterazioni)
Trasmissione criptata	SSL/TLS per tutte le trasmissioni di dati
Restrizioni di accesso	Accesso solo per persone autorizzate (2FA)
Registrazione degli accessi	Registro di tutti i tentativi di accesso
Pseudonimizzazione	I dati di utilizzo sono trattati in forma pseudonimizzata
Aggiornamenti di sicurezza regolari	Aggiornamento di tutti i sistemi
Backup	Backup regolari criptati presso Exoscale

8. Durata di conservazione e cancellazione

Categoria di dati	Durata di conservazione	Fondamento
Dati dell'account	Fino alla cancellazione dell'account	Esecuzione del contratto
Documenti	Fino alla cancellazione da parte dell'utente/cancellazione dell'account	Esecuzione del contratto
Dati di pagamento	10 anni	Obbligo legale
Dati di utilizzo (anonimi)	2 anni	Interesse legittimo
E-mail transazionali	2 anni	Esecuzione del contratto
Consensi marketing	Fino alla disiscrizione	Consenso

Cancellazione automatica: Dopo la cancellazione dell'account, tutti i dati personali vengono automaticamente cancellati entro 30 giorni (eccezione: dati di pagamento secondo l'obbligo legale di conservazione).

9. I vostri diritti

Avete i seguenti diritti:

Diritto	Descrizione
Accesso	Informazione sui vostri dati personali archiviati
Rettifica	Correzione di dati inesatti
Cancellazione	Cancellazione dei vostri dati ("diritto all'oblio")
Limitazione	Limitazione del trattamento
Opposizione	Opposizione al trattamento
Portabilità	Esportazione dei vostri dati (ad esempio documenti)
Revoca	Revoca in qualsiasi momento del consenso

Esercizio dei vostri diritti: Contattateci all'indirizzo info@elvida.app.

Importante per la cancellazione:

- Può cancellare il suo account in qualsiasi momento nelle impostazioni dell'applicazione
- Alla cancellazione dell'account, tutti i vostri documenti, metadati e dati personali vengono irrevocabilmente cancellati
- In caso di richieste di cancellazione, richiediamo immediatamente la cancellazione presso OpenAI (e-mail al supporto OpenAI con il vostro ID utente per l'identificazione)
- Per la cancellazione, dobbiamo verificare la vostra identità (ad esempio tramite il vostro indirizzo e-mail registrato)

Nota: In caso di perdita della vostra password, non possiamo ripristinare i vostri dati criptati.

Dovete reimpostare il vostro account, il che comporta la cancellazione di tutti i dati.

Reclamo: [Autorità federale della protezione dei dati e della trasparenza \(AFPDT\)](#)

10. Violazioni dei dati e incidenti di sicurezza

In caso di violazione dei dati o incidente di sicurezza che interessi i vostri dati personali, informiamo:

- L'Autorità federale della protezione dei dati e della trasparenza (AFPDT) entro 72 ore, se il rischio per i vostri diritti e libertà è elevato
- Voi in qualità di persona interessata senza indugio, se la violazione dei dati presenta un rischio elevato per i vostri diritti e libertà

11. Processo decisionale automatizzato

Non utilizziamo processi decisionali basati esclusivamente su un trattamento automatizzato che producano effetti giuridici o vi colpiscano in modo significativo (art. 21 LPD / art. 22 GDPR).

12. Modifiche alla presente informativa sulla protezione dei dati

Ci riserviamo il diritto di modificare la presente informativa sulla protezione dei dati. La versione attuale è sempre disponibile nell'app e su elvida.app/datenschutz.

13. Diritto applicabile e foro competente

La presente informativa sulla protezione dei dati è soggetta al diritto svizzero. Il foro competente esclusivo per tutte le controversie è Gersau, Svizzera.

4. ELVIDA App Privacy Policy

Last revised: February 2026

Document status: This privacy policy is available as a PDF in the ELVIDA App under "Settings > Data & Account".

Scope: This privacy policy applies to the ELVIDA App and related services. For the website elvida.app, a separate privacy policy applies.

1. General

C. Camenzind GmbH, operator of the ELVIDA App ("we"/"us"), is committed to protecting your personal data. This statement describes:

- what personal data we collect and process,
 - for what purpose and on what legal basis,
 - to whom we transfer data,
 - how long we store data,
 - what rights you have. Personal data is any information relating to an identified or identifiable person (e.g., name, email address, IP address).
-

2. Data Controller

C. Camenzind GmbH Furrenstrasse 5 6442 Gersau Switzerland Data protection contact: Email: info@elvida.app For questions regarding the processing of your personal data, please contact us at the address above.

3. Collection and Processing of Personal Data

3.1 Registration and Account Data

When creating an ELVIDA account, we collect:

- Email address
- Password (stored encrypted)
- Registration date
- Language setting Purpose: Provision of app functionalities, authentication Legal basis: Contract performance (Art. 13 FADP / Art. 6(1)(b) GDPR) Retention period: Until account deletion

3.2 Document Uploads and Storage

You can upload documents to the ELVIDA App. We process:

- Uploaded documents (contracts, invoices, insurance, etc.)
- Metadata (filename, title, document date, OCR text, text length, AI summary) Purpose: Encrypted storage and organization of your personal administrative documents Legal basis: Contract performance (Art. 13 FADP / Art. 6(1)(b) GDPR) Retention period: Until deletion by you or account deletion

Document contents (PDF files, images), OCR texts, and AI-generated summaries are stored encrypted with AES-GCM-256. Technical metadata (e.g., timestamps, file size, storage location) as well as cryptographic parameters (initialization vectors, key versions) are stored unencrypted, but do not allow reconstruction of the data content.

Component	Technical Implementation
Algorithm	AES-GCM (Authenticated Encryption)
Key length	256-bit
IV (Initialization Vector)	12 bytes (96-bit), unique per encryption
Authentication Tag	16 bytes (128-bit) for integrity verification
Key Derivation	User ID as key material (Key Version 1); future PBKDF2 with SHA-256 and 100,000 iterations (Key Version 2+)

Database Storage:

- encrypted_metadata – Base64 encrypted text
- metadata_encryption_iv – Base64 IV
- metadata_encryption_tag – Base64 authentication tag
- metadata_encryption_key_version – Key version

Important:

- Encryption occurs server-side with key-guided access
- The ELVIDA team has no routine access to your document contents
- If you lose your password, we cannot restore your data – you must reset your account (see Section 9)
- AI analysis for deadline and information extraction is performed via the OpenAI API (see Section 4) and is defined as a product feature in our T&Cs

3.3 Insurance situation (app behavior)

We collect non-identifiable data to improve our services:

- Interactions in the ELVIDA Dashboard (clicked features, used functions)
- App performance data (load times, errors)

- Aggregated usage statistics Purpose: Improvement of app functionality, error correction Legal basis: Legitimate interest (Art. 13 FADP / Art. 6(1)(f) GDPR) Note: This data is not linkable to your person (pseudonymization).

3.4 Payment Data

For paid features, we process via Stripe:

- Payment information (credit card number is not stored by us)
- Billing address
- Transaction history Purpose: Payment processing Legal basis: Contract performance (Art. 13 FADP / Art. 6(1)(b) GDPR) Retention period: 10 years (statutory retention obligation) Note: Payment data is processed directly by Stripe. We do not store complete credit card data.

3.5 Communication

For transactional emails (e.g., password reset, document notifications) and marketing:

- Email address
- Open and click rates (anonymized) Purpose: Service communication and marketing (only with consent) Legal basis: Contract performance (transactional emails) / Consent (marketing) Retention period: Until unsubscribe

4. AI Processing (OpenAI)

We use the OpenAI API for AI-assisted analysis of your documents within the ELVIDA App. This function is an integral part of our product and defined in our T&Cs.

Detail	Description
Provider	OpenAI, L.L.C., 3180 18th Street, San Francisco, CA 94110, USA
Processed Data	Contents of uploaded documents (e.g., contract texts, invoice details)
Purpose	Extraction of deadlines, amounts, contracting parties, and important information for the ELVIDA AI Agent
Legal basis	Contract performance (Art. 6(1)(b) GDPR / Art. 13 FADP) – AI analysis is an essential product feature under our T&Cs

Data Protection and Storage at OpenAI:

- Document contents are transmitted to an external LLM provider (USA) for analysis. Transmission occurs encrypted. We minimize personal data in metadata (titles,

descriptions); processing by the provider is subject to strict contractual requirements without use for training purposes.

- No storage for training purposes: OpenAI does not use your data to train AI models or improve its services.
- Temporary storage for security reasons: Document contents are transmitted to OpenAI exclusively for immediate analysis and retained for a maximum of 30 days for security purposes (fraud prevention, abuse detection). They are then automatically deleted.
- Deletion upon request: We send OpenAI a deletion request every 30 days for all processed data. Upon your specific deletion request (see Section 9), we explicitly request immediate deletion at OpenAI.
- No permanent storage: OpenAI does not retain copies of your documents after the 30-day security period expires.

Further Information: [OpenAI API Data Usage Policies](#)

5. International Data Transfers

We transfer personal data to countries outside Switzerland and the EEA:

Recipient	Location	Purpose	Safeguards
Exoscale (A1 Digital)	Switzerland	Encrypted document storage	No transfer (Swiss servers)
Stripe, Inc.	USA	Payment processing	Standard Contractual Clauses (SCCs)
OpenAI, L.L.C.	USA	AI document analysis	Standard Contractual Clauses (SCCs) + Zero-Retention
Loops Labs Inc.	USA	Email delivery (transactions/marketing)	Standard Contractual Clauses (SCCs)

For transfers to the USA (OpenAI, Stripe, Loops), a Transfer Impact Assessment (TIA) has been conducted. In addition to Standard Contractual Clauses (SCCs), we implement the following supplementary measures:

- OpenAI: Data is transmitted encrypted; no storage for training purposes contractually excluded
- Stripe/Loops: Pseudonymization of sensitive data where possible

The USA does not have a level of data protection equivalent to Swiss or EU data protection law. The transfer is based on Standard Contractual Clauses pursuant to Art. 16 FADP and Art. 46 GDPR.

6. Processors

We use the following service providers as processors:

Service Provider	Activity	Location	Contract
Exoscale (A1 Digital)	Cloud storage for documents	Switzerland	Data Processing Agreement (DPA)
Stripe, Inc.	Payment processing	USA	Data Processing Agreement (DPA)
OpenAI, L.L.C.	AI processing	USA	Data Processing Agreement (DPA)
Loops Labs Inc.	Email delivery	USA	Data Processing Agreement (DPA)

All processors are contractually obligated to comply with data protection requirements.

7. Data Security

We implement the following technical and organizational measures to protect your data:

Measure	Description
Encryption (AES-GCM)	All documents and metadata are stored with AES-GCM (256-bit) encryption
Authenticated Encryption	AES-GCM ensures data cannot be manipulated (authentication tag)
Key Derivation	Keys are derived from user ID (future PBKDF2 with 100,000 iterations)
Encrypted Transmission	SSL/TLS for all data transmissions
Access Restrictions	Access only for authorized persons (2FA)
Access Logging	Log of all access attempts
Pseudonymization	Usage data is processed pseudonymously
Regular Security Updates	Updating all systems
Backups	Regular encrypted backups at Exoscale

8. Retention Periods and Deletion

Data Category	Retention Period	Basis
Account data	Until account deletion	Contract performance
Documents	Until deletion by user/account deletion	Contract performance
Payment data	10 years	Statutory obligation
Usage data (anonymous)	2 years	Legitimate interest
Transactional emails	2 years	Contract performance
Marketing consents	Until unsubscribe	Consent

Automatic Deletion: After account deletion, all personal data is automatically deleted within 30 days (exception: payment data per statutory retention).

9. Your Rights

You have the following rights:

Right	Description
Access	Information about your stored personal data
Rectification	Correction of inaccurate data
Erasure	Deletion of your data ("right to be forgotten")
Restriction	Restriction of processing
Objection	Objection to processing
Data Portability	Export of your data (e.g., documents)
Withdrawal	Withdrawal of consent at any time

Exercising Your Rights: Contact us at info@elvida.app.
Important for Deletion:

- You can delete your account at any time in the App settings
- Upon account deletion, all your documents, metadata, and personal data are irrevocably deleted
- Upon deletion requests, we immediately request deletion at OpenAI (email to OpenAI Support with your user ID for identification)
- For deletion, we must verify your identity (e.g., via your registered email address)

Note: If you lose your password, we cannot restore your encrypted data. You must reset your account, which deletes all data.

Complaint: [Swiss Federal Data Protection and Information Commissioner \(FDPIC\)](#)

10. Data Breaches and Security Incidents

In the event of a data breach or security incident affecting your personal data, we notify:

- The Swiss Federal Data Protection and Information Commissioner (FDPIC) within 72 hours, if the risk to your rights and freedoms is high
 - You as the affected person without undue delay, if the data breach presents a high risk to your rights and freedoms
-

11. Automated Decision-Making

We do not use automated decision-making based solely on automated processing that produces legal effects or significantly affects you (Art. 21 FADP / Art. 22 GDPR).

12. Changes to This Privacy Policy

We reserve the right to adapt this privacy policy. The current version is always available in the app and at elvida.app/datenschutz.

13. Applicable Law and Jurisdiction

This privacy policy is subject to Swiss law. The exclusive place of jurisdiction for all disputes is Gersau, Switzerland.