Legislator AI AG
Kirchstrasse 6 · 8807 Freienbach SZ · Schweiz
UID: CHE-476.609.141 · legal@legislator.ch

Datenschutzerklärung von Legislator

Letzte Aktualisierung: 28. Oktober 2026

1. Geltungsbereich und verantwortliches Unternehmen

Diese Datenschutzerklärung erläutert, wie die **Legislator AI AG**, Kirchstrasse 6, 8807 Freienbach SZ, Schweiz, Unternehmens-Identifikationsnummer (UID) CHE-476.609.141 («Legislator», «wir», «uns» oder «unser»), Personendaten im Zusammenhang mit legislator.ch, der juristischen KI-Plattform von Legislator sowie unseren damit verbundenen Dienstleistungen (zusammen die «Dienste») bearbeitet. Für Anliegen zum Datenschutz und zum Berufsgeheimnis können Sie uns unter **legal@legislator.ch** kontaktieren.

Diese Datenschutzerklärung gilt für Website-Besucherinnen und -Besucher, potenzielle Kunden, einzelne Nutzerinnen und Nutzer, Vertreterinnen und Vertreter von Kundenorganisationen sowie sonstige natürliche Personen, deren Personendaten über die Dienste bearbeitet werden. Ein «Kunde» ist die natürliche oder juristische Person bzw. Organisation (wie beispielsweise eine Anwaltskanzlei, ein Notariat, eine Unternehmensrechtsabteilung oder eine andere Einheit), welche die Dienste bezieht oder nutzt. «Kundeninhalte» (Customer Content) bezeichnet sämtliche Materialien, die im Auftrag des Kunden auf die Plattform übermittelt, dort gespeichert oder über diese generiert werden, wie in Ziffer 3 näher beschrieben.

Wir bearbeiten Personendaten im Einklang mit dem Bundesgesetz über den Datenschutz vom 25. September 2020 (DSG; SR 235.1) und der Verordnung über den Datenschutz vom 31. August 2022 (DSV; SR 235.11) sowie der EU-Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, DSGVO), soweit diese auf die jeweilige Bearbeitung anwendbar ist. Diese Datenschutzerklärung erfüllt unsere gesetzlichen Informationspflichten (Art. 19 DSG; Art. 13 und 14 DSGVO). Sie ersetzt für sich genommen nicht den anwendbaren Auftragsbearbeitungsvertrag samt Zusatzvereinbarung zum Berufsgeheimnis («DPA»).

2. Unsere Rollen und die Kundenbeziehung

2.1. Bearbeitung für eigene Zwecke (Legislator als Verantwortliche)

Wir handeln als Verantwortliche (Art. 5 Bst. j DSG; Art. 4 DSGVO, soweit anwendbar) für diejenigen Personendaten, die wir verwenden, um Benutzerkonten und Abonnemente zu verwalten, unsere Geschäftsbeziehungen und die Rechnungsstellung abzuwickeln, unsere Website und Dienste zu betreiben und zu sichern, den administrativen Support zu leisten, geltende gesetzliche und buchhalterische Pflichten zu erfüllen sowie unsere Rechte zu wahren.

2.2. Bearbeitung im Auftrag von Kunden (Legislator als Auftragsbearbeiter und berufliche Hilfsperson)

Wir handeln als Auftragsbearbeiter (Art. 5 und Art. 9 DSG; Art. 28 DSGVO, sofern anwendbar) und im Verhältnis zu Berufsgeheimnisträgern aus dem Rechtsbereich als dem Berufsgeheimnis unterstehende Hilfsperson (im Sinne von Art. 321 Ziff. 1 des Schweizerischen Strafgesetzbuches (StGB) sowie Art. 13 Abs. 2 des Bundesgesetzes über die Freizügigkeit der Anwältinnen und Anwälte (BGFA)), wenn wir Personendaten in Kundeninhalten auf dokumentierte Weisung eines Kunden bearbeiten. Der Kunde bleibt der Verantwortliche und bestimmt die Zwecke sowie die wesentlichen Mittel dieser Bearbeitung. Wir legen die technischen und organisatorischen Vorkehrungen fest, die zur Erbringung der vereinbarten Dienste erforderlich sind, und setzen diese strikt im Rahmen dieser Weisungen und des DPA um. Handelt ein Kunde selbst als Auftragsbearbeiter für einen anderen Verantwortlichen, so handeln wir entsprechend als sein Unterauftragsbearbeiter.

Die Weisungen des Kunden umfassen die vereinbarte Dienstkonfiguration, die von autorisierten Nutzerinnen und Nutzern eingereichten Aufgaben (Tasks), Eingaben (Prompts) und Dateien sowie die Einstellungen zur Aufbewahrung, Freigabe und Löschung. Wir erwerben kein eigenständiges Recht zur Weiterverwendung von Kundeninhalten allein dadurch, dass diese an die Dienste übermittelt werden. Inhalte, die für den technischen Support zur Verfügung gestellt werden, unterliegen denselben strengen Beschränkungen; administrative

Korrespondenz im Zusammenhang mit einer Supportanfrage kann separat als Daten in eigener Verantwortlichkeit (als Verantwortliche) bearbeitet werden.

Der DPA legt die verbindlichen vertraglichen Regelungen betreffend dokumentierte Weisungen, das Berufsgeheimnis (Art. 321 StGB / Art. 13 BGFA), die Datensicherheit, die Genehmigung und Überwachung von Unterauftragsbearbeitern, die Unterstützung bei der Wahrnehmung von Betroffenenrechten, die Meldung von Sicherheitsvorfällen sowie die Rückgabe oder Löschung von Kundeninhalten fest. **Eine unterzeichnete Ausfertigung des Auftragsbearbeitungsvertrags und der Zusatzvereinbarung zum Berufsgeheimnis (DPA) kann unter legal@legislator.ch angefordert werden**. Diese Datenschutzerklärung schmälert weder unsere Pflichten noch weitergehende Schutzverpflichtungen, die mit einem Kunden in einem unterzeichneten DPA vereinbart wurden; ein solcher geht dieser Datenschutzerklärung vor.

3. Kategorien der bearbeiteten Personendaten und deren Quellen

3.1. Konto- und Verwaltungsdaten (Verantwortlicher)

Je nach Ihrer Interaktion mit uns bearbeiten wir die folgenden Kategorien von Personendaten:

Identitäts- und Kontaktdaten: Vorname, Nachname, (geschäftliche) E-Mail-Adresse, Name der Organisation oder Anwaltskanzlei, berufliche Funktion sowie weitere von Ihnen angegebene Kontaktinformationen.
Konto- und Abonnementinformationen: Benutzer- und Organisationskennungen, Zugriffsberechtigungen, Authentifizierungs- und Sitzungsinformationen, gewähltes Abonnementmodell, Abonnementstatus sowie Kontoeinstellungen (einschliesslich Präferenzen bezüglich diagnostischer Überprüfungen).
Abrechnungs- und Zahlungsinformationen: Rechnungsangaben, Rechnungen, Transaktionsreferenzen, Zahlungsstatus sowie Zahlungsverlauf des Abonnements. Zahlungskartendaten werden von Stripe direkt über dessen Zahlungsdienste bearbeitet.
Kommunikation: Anfragen, Demo-Anfragen, administrative Support-Korrespondenz, freiwilliges Feedback sowie Kommunikationspräferenzen.
Technische Metadaten und Nutzungsmetadaten: IP-Adressen, Browser- und Geräteinformationen, Zeitstempel, Login-, Sicherheits- und Zugriffsereignisse, Fehlercodes sowie Messwerte zur Dienstnutzung (wie Token-Zählerstände und Berechnungskosten). Metadaten, die einer bestimmbaren Benutzerin bzw. einem bestimmbaren Benutzer oder einem Konto zugeordnet sind, werden als administrative Personendaten behandelt, selbst wenn sie keinen Dokumenttext und keine Prompts enthalten.

Wir erheben diese Informationen direkt von Ihnen, von Ihrer Organisation oder deren autorisierten Nutzern, im Rahmen des technischen Betriebs der Dienste sowie von Dienstleistern, die in die Authentifizierung, die Kommunikation oder die Zahlungsabwicklung eingebunden sind, soweit dies für deren jeweilige Leistung erforderlich ist.

3.2. Kundeninhalte (Auftragsbearbeiter)

Kundeninhalte umfassen sämtliche Daten, die den Diensten über alle Plattformmodi hinweg (einschliesslich agentischer Modi wie Instant, Standard, Deep Research, Deep Research Fast, Deep Research Ultra, Memo, Suchmodi wie Gesetzgebung (Legislation) und Gerichtsentscheide (Court Decisions) sowie der Funktion AI Detector) zur Bearbeitung übermittelt werden, namentlich: Prompts, Fragen, Anweisungen, hochgeladene Dokumente (PDF, Word, Bilder, gescannte Dateien, Audiodateien), extrahierten Text (einschliesslich mittels OCR und Audiotranskription), Sachverhaltsdarstellungen, Notizen, Vorlagen, private Wissensquellen, interne Nachrichten, zugehörige Dateimetadaten, generierte Antworten, Entwürfe und sonstige Ergebnisse (Outputs). Dazu gehören auch gespeicherte Aufgaben (Tasks), Konversationsverläufe, Überarbeitungen sowie Vektordarstellungen (Embeddings), die aus diesem Material abgeleitet werden, um Such- und Abruffunktionen innerhalb der isolierten Umgebung des Kunden bereitzustellen.

Kundeninhalte können Personen identifizieren, die Legislator nicht direkt nutzen, einschliesslich Klientinnen und Klienten, Mitarbeitenden, Gegenparteien, Zeuginnen und Zeugen, Sachverständigen sowie Amtsträgerinnen und Amtsträgern, die in juristischen Akten erwähnt werden. Sie können besonders schützenswerte Personendaten gemäss Art. 5 Bst. c DSG (z. B. Gesundheitsdaten, Daten über straf-, steuer- oder verwaltungsrechtliche Verfahren),

besondere Kategorien personenbezogener Daten gemäss Art. 9 DSGVO oder Daten über strafrechtliche Verurteilungen und Straftaten gemäss Art. 10 DSGVO enthalten. Der Kunde bestimmt, welche Daten er übermittelt, und ist für die Einhaltung der für diese Daten geltenden gesetzlichen und berufsrechtlichen Voraussetzungen verantwortlich.

3.3. Öffentliche Rechtsquellen

Unsere juristische Referenzdatenbank enthält öffentlich zugängliche schweizerische Rechtsmaterialien (Erlasse des Bundes und der Kantone, publizierte Gerichtsentscheide sowie juristische Literatur) und zugehörige Zitationsangaben. Allfällige in diesen Materialien enthaltene Personendaten stammen aus den jeweiligen publizierten Quellen. Die privaten Dokumente und privaten Wissensquellen eines Kunden bleiben als Kundeninhalte strikt isoliert; sie werden niemals in die öffentliche Referenzdatenbank aufgenommen oder anderen Kunden zugänglich gemacht.

4. Zwecke und Rechtsgrundlagen der Bearbeitung als Verantwortliche

Wir verwenden Konto- und Verwaltungsdaten, um Konten einzurichten und zu verwalten, den Plattformzugang bereitzustellen, Abonnemente zu verwalten, Nutzungsgebühren zu berechnen, Zahlungen abzuwickeln und Anfragen zu beantworten (Art. 6 und Art. 31 Abs. 2 Bst. a DSG; soweit die DSGVO anwendbar ist, Art. 6 DSGVO zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Massnahmen sowie Art. 6 DSGVO zur Wahrung unseres berechtigten Interesses an der Bereitstellung und Verwaltung der Dienste für die Organisation).

Wir bearbeiten technische Metadaten und Nutzungsmetadaten, um die Verfügbarkeit der Infrastruktur aufrechtzuerhalten, Störungen zu diagnostizieren, Konten und Systeme abzusichern, Missbrauch oder unbefugten Zugriff zu verhindern und die Leistung der Dienste zu überwachen (Art. 7 und 8 DSG; Art. 6 DSGVO). Diese Tätigkeiten berechtigen in keinem Fall zur Weiterverwendung von Kundeninhalten für das Training oder die Entwicklung von Modellen.

Wir bearbeiten Geschäftskorrespondenz und versenden wesentliche Konto-, Sicherheits-, Abrechnungs- und Vertragsmitteilungen als notwendigen Bestandteil der Bereitstellung der Dienste. Soweit wir optionale Produktinformationen versenden, stützen wir uns auf eine Einwilligung, sofern diese erforderlich ist, oder, soweit nach anwendbarem Recht zulässig (Art. 6 DSGVO), auf unser berechtigtes Interesse, Geschäftskontakte über relevante Dienste von Legislator zu informieren. Sie können sich jederzeit gemäss den Anweisungen in der jeweiligen Mitteilung abmelden oder Widerspruch einlegen oder sich an **legal@legislator.ch** wenden.

Wir bearbeiten Daten, die für die Buchführung, die Einhaltung gesetzlicher Vorschriften (Compliance; insbesondere die zehnjährige Aufbewahrungspflicht gemäss Art. 958f des Schweizerischen Obligationenrechts (OR)) sowie die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind (Art. 31 Abs. 1 DSG; Art. 6 DSGVO). Schliesslich pflegen und indexieren wir öffentlich zugängliche Rechtsmaterialien gestützt auf unser berechtigtes Interesse an der Bereitstellung zuverlässiger juristischer Recherchefunktionen (Art. 31 Abs. 1 DSG; Art. 6 DSGVO) unter Abwägung mit den Rechten der betroffenen Personen.

5. Wie wir Kundeninhalte als Auftragsbearbeiter bearbeiten

Wir bearbeiten Kundeninhalte ausschliesslich zur Ausführung der vom Kunden angeforderten Aufgaben und dokumentierten Weisungen. Dies umfasst:

Das Empfangen und Aufbereiten hochgeladener Dateien;
Das Extrahieren und Strukturieren relevanter Texte und Informationen (was bei digitalen Standarddokumenten lokal auf unseren Schweizer Servern und bei der optischen Zeichenerkennung (OCR) von gescannten Bildern sowie der Audiotranskription über TLS-verschlüsselte API-Aufrufe an Google-Cloud-Gemini-Modelle in der EU unter Zero-Data-Retention-Bedingungen erfolgt);
Das Ausführen von Funktionen für die semantische Suche, das Embedding und das Reranking (welche vollständig auf unserer eigenen Schweizer Infrastruktur ausgeführt werden);
Das Durchführen von generativer KI-Inferenz und das Erzeugen der angeforderten Ergebnisse (Outputs);
Das Speichern der Aufgaben, Entwürfe und Verläufe, deren Aufbewahrung der Kunde auf unseren Schweizer Servern wählt, sowie das Ausführen von Freigabe- oder Löschanweisungen.

Wir beschränken das an einen externen KI-Inferenz-Anbieter übermittelte Material auf das für die angeforderte Aufgabe erforderliche Mass. Wir verwenden Kundeninhalte niemals zu Werbezwecken, für ein eigenständiges Profiling von natürlichen Personen (Art. 5 Bst. f und g DSG) oder zum Aufbau von Datensätzen für andere Kunden.

Um die Zuverlässigkeit der Plattform zu gewährleisten und technische Ausführungsfehler zu beheben (insbesondere wenn eine Aufgabe aufgrund eines Anwendungsabsturzes oder eines Fehlers bei der Verarbeitung von Anhängen nicht ausgeführt werden kann oder wenn ein Nutzer in einer Folgenachricht einen Fehler des Agenten meldet), betreiben wir einen automatisierten internen Diagnose-Workflow (AI Review): Markierte Aufgaben werden zunächst automatisch durch ein KI-Modell (wie etwa Gemini unter EU-Zero-Data-Retention-Bedingungen) anonymisiert, Original-Dateianhänge werden abgetrennt und Nutzerkennungen entfernt, sodass der Datensatz nicht mehr seinem Inhaber zugeordnet werden kann; das anonymisierte Protokoll wird mit einem dedizierten Schlüssel verschlüsselt und von einem Diagnose-KI-Agenten (wie etwa Gemini oder Claude) analysiert, um eine kurze Diagnosemeldung zu generieren, die ausschliesslich von unserem Head of IT zwecks Code-Korrektur geprüft wird. Anonymisierte Diagnosedatensätze werden unverzüglich gelöscht, sobald die Code-Überprüfung bestätigt, dass das Problem behoben ist, spätestens jedoch 7 Tage nach ihrer Erstellung. Wenn die Einstellung «Nach 24 Stunden löschen» (Delete after 24 hours) aktiviert ist, wird auf Aufgabendaten zu Diagnosezwecken niemals zugegriffen, und sie werden weder geprüft noch verwendet – auch nicht zur Untersuchung oder Behebung technischer Ausführungsfehler –, und nach dem manuellen oder automatischen Löschen der Aufgabe werden keine Diagnosekopien aufbewahrt.

6. Keine Verwendung von Kundeninhalten für das Modelltraining

Wir verwenden Kundeninhalte – einschliesslich Prompts, hochgeladener Dateien, mittels OCR oder Audiotranskription extrahierten Texten, gespeicherter Verläufe und generierter Ausgaben (Outputs) – nicht zum Trainieren, zum Fine-Tuning oder zur Verbesserung unserer eigenen KI-Modelle oder von KI-Modellen Dritter. Unsere verbindlichen Vereinbarungen mit Anbietern von KI-Inferenzdiensten (wie Google Cloud EMEA Limited und TensorX Ltd.) untersagen eine solche Verwendung von in unserem Auftrag bearbeiteten Kundeninhalten strikt, und wir ermächtigen keinen Anbieter jemals dazu, Kundeninhalte für das Modelltraining freizugeben (Opt-in).

7. Infrastruktur in der Schweiz und KI-Inferenz in der Europäischen Union

7.1. Unsere physische Infrastruktur in der Schweiz und das Ingress-Gateway

Wir betreiben die Kernplattform, sämtliche persistenten Plattformspeicher (wie die Kontodatenbank, gespeicherte Kundeninhalte, hochgeladene Dateien, Vorlagen, private Wissensquellen, Verläufe und Backups) sowie unsere Schweizer Rechtsdatenbank auf **unseren eigenen physischen Servern in der Schweiz**, die im Eigentum und unter der ausschliesslichen Kontrolle der Legislator AI AG stehen. Such-, Embedding- und Reranking-Modelle werden vollständig auf unserer Schweizer Hardware ausgeführt; wir nutzen für diese Komponenten keine Cloud-Speicheranbieter von Dritten oder externe Vektordatenbankdienste. Auf der Stufe des Netzwerkeingangs (Ingress) wird der verschlüsselte Client-Datenverkehr (TLS) über ein von der Amazon Web Services EMEA SARL in der Schweiz (Region Zürich) betriebenes Web-Reverse-Proxy-Gateway direkt an unsere physischen Server (On-Premises) in der Schweiz weitergeleitet, ohne dass am Gateway eine Speicherung von Kundeninhalten erfolgt.

Zur rechtlichen Klarstellung im Sinne der Wegleitung des Schweizerischen Anwaltsverbands (SAV-Wegleitung für den Umgang mit künstlicher Intelligenz, Ziff. 2.1 Abs. 2 Ziff. 2) gilt Folgendes: Obwohl die zugrunde liegenden physischen Server in der Schweiz im Eigentum der Legislator AI AG stehen, stellt die Nutzung der Dienste durch eine Anwaltskanzlei ein externes IT-Outsourcing und keine kanzleiinterne On-Premises-Installation dar, da Daten das interne Netzwerk der Anwaltskanzlei verlassen.

7.2. Transiente KI-Inferenz in der Europäischen Union unter Zero Data Retention (ZDR)

Für Aufgaben der generativen KI (sowie für OCR und Audiotranskription) ziehen wir **Google Cloud EMEA Limited** für die Modellfamilien Gemini und Anthropic Claude in unserer genehmigten Enterprise-Konfiguration sowie **TensorX Ltd.** für unabhängig gehostete Open-Weights-Modelle, einschliesslich DeepSeek, bei. Sämtliche für Kundeninhalte genutzten KI-Inferenz-Endpunkte befinden sich ausschliesslich in der **Europäischen Union**. Wiederholungsversuche

(Retries) bei Ausfällen oder Kontingentereignissen (Quota Events) werden strikt an denselben Modellanbieter innerhalb derselben EU-Region geleitet; unsere Anwendungsschicht blockiert jeglichen Fallback und jegliches Routing ausserhalb der genehmigten EU-Konfiguration (Fail-Closed).

Unsere Inferenzkonfiguration unterliegt unternehmensspezifischen Zusicherungen für **Zero Data Retention (ZDR)** sowie genehmigten Ausnahmen von der Prompt-Protokollierung zur Missbrauchsüberwachung von Google Cloud (bestätigt am 1. September 2026 für sämtliche Google-Cloud-Projekte der Legislator AI AG):

Sämtliche Daten werden über TLS-verschlüsselte Verbindungen übertragen.
Prompts, Dokumentinhalte und generierte Ausgaben werden ausschliesslich flüchtig im Arbeitsspeicher (RAM) bearbeitet, um die Antwort zu berechnen, und unmittelbar nach Abschluss der Anfrage aus dem Arbeitsspeicher gelöscht, mit **0 Tagen dauerhafter Inhaltsspeicherung** auf den Datenträgern des Anbieters.
Inhaltsprotokollierung (Content Logging), Prompt-Protokollierung zur Missbrauchsüberwachung (Abuse-Monitoring Prompt Logging) sowie anbieterseitiges Inhalts-Caching, das mit ZDR unvereinbar ist, sind deaktiviert.
TensorX Ltd. hostet eine unabhängige Kopie des jeweiligen Open-Weights-Modells (DeepSeek) auf dedizierter GPU-Infrastruktur in Irland und Finnland; durch die Auswahl dieses Modus werden Kundeninhalte niemals an die ursprünglichen Entwickler des Modells übermittelt. Der Anbieter gewährt Zusicherungen für **Zero Data Retention (ZDR)** bei der Inferenz und protokolliert keine Prompts.

8. Externe Web-Recherche (Google Grounding)

Die externe Webrecherche ist getrennt von Suchabfragen in der schweizerischen juristischen Referenzdatenbank von Legislator auf unserer Schweizer Infrastruktur. Wenn ein Kunde die Funktion «Deep Research» nutzt, empfängt der eingesetzte Dienst **Google Cloud Web Grounding for Enterprise** die Suchanfragen sowie allfällige in dieser Anfrage enthaltene Kontextinformationen. Web Grounding for Enterprise bietet vertragliche Zero-Data-Retention-Garantien (keine Speicherung von Kundendaten und keine Verwendung für das Modelltraining, im Gegensatz zu herkömmlichen Websuchdiensten).

9. Empfänger und Unterauftragsbearbeiter

Der Zugriff auf Personendaten ist auf diejenigen Personen beschränkt, die diese für die in dieser Datenschutzerklärung beschriebenen Zwecke benötigen. Zu den Empfängern gehören autorisierte Mitarbeitende von Legislator, die in **Anhang 1** aufgeführten Dienstleister sowie – sofern der Kunde Freigabefunktionen nutzt – die vom Kunden autorisierten Nutzer der Organisation. Dienstleister, die Kundeninhalte in unserem Auftrag bearbeiten (wie Google Cloud EMEA Limited, TensorX Ltd. und – ausschliesslich für den verschlüsselten Netzwerkeingang in der Schweiz – Amazon Web Services EMEA SARL), handeln als Unterauftragsbearbeiter auf der Grundlage verbindlicher Auftragsbearbeitungs- und Vertraulichkeitsvereinbarungen (Art. 9 DSG, Art. 7 DSV, Art. 28 DSGVO).

Mit der Annahme der Nutzungsbedingungen erteilt der Kunde der Legislator AI AG die allgemeine Genehmigung, Unterauftragsbearbeiter zur Bearbeitung von Personendaten im Auftrag des Kunden beizuziehen, einschliesslich der Hinzufügung oder des Austauschs von Unterauftragsbearbeitern. Jeder Unterauftragsbearbeiter muss denselben materiellen Datenschutz- und Vertraulichkeitspflichten unterworfen werden, die auch für Legislator gelten, soweit diese für die dem jeweiligen Unterauftragsbearbeiter übertragene Bearbeitung relevant sind. Legislator bleibt gegenüber dem Kunden für die Einhaltung dieser Pflichten durch ihre Unterauftragsbearbeiter haftbar.

Für administrative Hilfsdienste, die niemals Kundeninhalte, Prompts oder hochgeladene juristische Dateien erhalten, gilt Folgendes:

Mailgun und Resend (Plus Five Five, Inc.) erbringen Dienste für den administrativen E-Mail-Versand (Anmeldecodes und Benachrichtigungen). E-Mails zur Aufgabenbenachrichtigung und -freigabe enthalten ausschliesslich sichere Zugriffslinks (sogenannte Link-only-E-Mails) und niemals Prompts, hochgeladene Dokumente oder generierte Rechtstexte.
Stripe wickelt Abonnementzahlungen und Abrechnungsdaten ab (wobei Stripe für in Auftrag gegebene Zahlungstransaktionen als Auftragsbearbeiter und für seine eigenen Pflichten in den Bereichen Betrugsprävention, Regulierung und Compliance als eigenständiger Verantwortlicher handelt).

10. Internationale Datenbekanntgaben und Garantien (Art. 16 ff. DSG)

Unsere zentrale dauerhafte Datenspeicherung befindet sich ausschliesslich in der Schweiz. Die externe KI-Inferenz erfolgt in der Europäischen Union, wie in Ziffer 7 beschrieben.

Für jede grenzüberschreitende Bekanntgabe wenden wir die nach Art. 16 und Art. 19 Abs. 4 DSG sowie Kapitel V DSGVO erforderlichen Schutzmassnahmen (Garantien) an:

Angemessenheitsbeschlüsse (Art. 16 Abs. 1 DSG / Anhang 1 DSV; Art. 45 DSGVO): Übermittlungen in Mitgliedstaaten der Europäischen Union und des Europäischen Wirtschaftsraums stützen sich auf anerkannte Angemessenheitsfeststellungen.
Standardvertragsklauseln mit schweizerischen Anpassungen (Art. 16 Abs. 2 Bst. d DSG; Art. 46 DSGVO): Unser Rückgriff auf diese Garantien beschränkt sich auf Übermittlungen von Personendaten, die **für die Abwicklung von Kreditkartenzahlungen und die Zustellung administrativer E-Mails** erforderlich sind. Soweit Übermittlungen an Anbieter dieser Dienste nicht durch einen anwendbaren Angemessenheitsbeschluss abgedeckt sind, verwenden wir die vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) anerkannten EU-Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914 der Kommission) samt den nach schweizerischem Datenschutzrecht erforderlichen Anpassungen sowie allfälligen für die betreffende Übermittlung notwendigen zusätzlichen Garantien.
Swiss–U.S. und EU–U.S. Data Privacy Framework: Unser Rückgriff auf das jeweils anwendbare Data Privacy Framework beschränkt sich auf Übermittlungen an **US-amerikanische Anbieter von Kreditkartenzahlungen und administrativem E-Mail-Versand** (wie Stripe, Inc.), die über eine aktive Zertifizierung unter dem betreffenden Rahmenwerk verfügen, welche die übermittelten Daten abdeckt. Wir behandeln die Vereinigten Staaten nicht generell für alle Empfänger oder Übermittlungen als Staat mit angemessenem Datenschutzniveau.

11. Aufbewahrung und Löschung

11.1. Gespeicherte Aufgaben, Kundeninhalte und Transformations-Caches (Auftragsbearbeiter)

Gespeicherte Aufgaben, hochgeladene Dateien, Verläufe und Ausgaben bleiben während der vereinbarten Vertragslaufzeit auf unseren Schweizer Servern verfügbar, sofern der Kunde diese nicht vorzeitig löscht oder eine kürzere Aufbewahrungseinstellung wählt:

Manuelle Löschung («Löschen» / «Alle löschen») und Einstellung «Nach 24 Stunden löschen» (Delete after 24 hours): Der Kunde kann jederzeit die Schaltflächen «Löschen» (Delete) und «Alle löschen» (Delete all) verwenden oder für einzelne Aufgaben die optionale Einstellung **«Nach 24 Stunden löschen» (Delete after 24 hours)** aktivieren. Die Einstellung «Nach 24 Stunden löschen» (Delete after 24 hours) löscht die ausgewählte Aufgabe und alle damit verbundenen Inhalte automatisch **24 Stunden nach Erstellung der Aufgabe**. Bei einer manuellen Löschung werden die Inhalte der ausgewählten Aufgabe umgehend von unseren aktiven Schweizer Serversystemen und innerhalb von 24 Stunden von den Backup-Servern entfernt.

11.2. Konto- und Geschäftsunterlagen (Verantwortlicher)

Wir bewahren Kontodaten für die Dauer des Vertragsverhältnisses und darüber hinaus nur so lange auf, wie dies für die Schliessung des Kontos, die Erfüllung gesetzlicher Pflichten oder die Bearbeitung konkreter Rechtsansprüche erforderlich ist. Geschäftsbücher, Rechnungen und Buchungsbelege, die Art. 958f des Schweizerischen Obligationenrechts (OR) unterliegen, werden während **10 Jahren** ab dem Ende des betreffenden Geschäftsjahres aufbewahrt.

12. Datensicherheit, Verschlüsselung und menschlicher Zugriff

12.1. Technische und organisatorische Massnahmen (Art. 8 DSG)

Wir setzen technische und organisatorische Massnahmen um, die den Risiken und der Sensibilität juristischer Daten angemessen sind, darunter:

Verschlüsselung im Ruhezustand (Encryption at rest): Sämtliche auf unseren physischen Servern in der Schweiz gespeicherten Kundeninhalte (einschliesslich Dateien, Konversationen, Datenbanken, Suchindizes, Embeddings und Caches) werden im Ruhezustand mittels gängiger Verschlüsselungsverfahren symmetrisch verschlüsselt.
Verschlüsselung bei der Übertragung (Encryption in transit): Sämtliche Datenübertragungen zwischen Client-Systemen, unserem Schweizer Gateway, den Legislator-Servern und den Modellanbietern in der EU sind durch eine standardmässige TLS-Verschlüsselung geschützt.
Applikations- und Schnittstellenkontrollen: Middleware zur Verhinderung von Path-Traversal-Angriffen, strenge Eingabevalidierung ohne Protokollierung von Anfrageinhalten (Request Bodies), Bot-Filterung, unveränderbare (Append-only) Zugriffsprotokolle sowie eine strikte serverseitige Sandbox für die Werkzeugausführung (welche unautorisierte Tool-Aufrufe, Shell-Zugriffe, die Ausführung von Teilprozessen oder beliebige Netzwerkzugriffe verhindert).
Fail-Closed-Schutzmechanismen und Vorfallbewältigung (Incident Response): Wird eine genehmigte Ausnahmeregelung eines Anbieters widerrufen oder eine nicht freigegebene Route erkannt, schaltet die betroffene Funktion sofort ab (Fail-Closed), ohne Kundeninhalte anderweitig umzuleiten. Bei Verdacht auf einen Sicherheits- oder Vertraulichkeitsvorfall, der Kundeninhalte betrifft, isoliert unser Head of IT unverzüglich die betroffenen Dienste und **benachrichtigt die bezeichnete Kontaktperson der betroffenen Anwaltskanzlei innerhalb von 24 Stunden nach Kenntnisnahme** (unter Angabe von Zeitstempeln, betroffenen Aufgaben-IDs, Eindämmungsmassnahmen und einer Bestätigung der Verschlüsselungsintegrität), gefolgt von einem Bericht über die Ursachenanalyse und die Korrekturmassnahmen **innerhalb von 72 Stunden**.

12.2. Strenge Beschränkungen des Zugriffs durch Personen

Kundeninhalte werden im regulären Betrieb automatisiert bearbeitet. Ein menschlicher Zugriff auf Diagnose- oder Supportinformationen erfolgt nur, soweit dies zwingend erforderlich ist, um eine vom Kunden initiierte Supportanfrage zu bearbeiten oder einen technischen Fehler bzw. einen Sicherheitsvorfall im Rahmen der Weisungen des Kunden zu beheben (über das anonymisierte Verfahren gemäss Ziffer 5). Sämtliche autorisierten Mitarbeitenden unterliegen schriftlichen, fortbestehenden Vertraulichkeitspflichten sowie dem Berufsgeheimnis als Hilfspersonen nach Art. 321 StGB.

13. Berufsgeheimnis und rechtmässige Weisungen

Die Dienste sind auf die Unterstützung der professionellen juristischen Arbeit ausgerichtet. Soweit Legislator als Hilfsperson für eine Rechtsanwältin oder einen Rechtsanwalt, eine Notarin oder einen Notar oder einen anderen dem gesetzlichen Berufsgeheimnis unterstehenden Geheimnisträger (Art. 321 StGB, Art. 13 BGFA) tätig wird, regeln unser Auftragsbearbeitungsvertrag samt Zusatzvereinbarung zum Berufsgeheimnis («DPA») diese Pflichten über die gesamte Leistungskette hinweg. Wir bleiben für unsere eigenen gesetzlichen und vertraglichen Pflichten verantwortlich. Der Kunde ist dafür verantwortlich sicherzustellen, dass er zur Übermittlung von Kundeninhalten berechtigt ist, die erforderlichen Datenschutzinformationen gegenüber den betroffenen Personen bereitzustellen (Art. 19 DSG) sowie mandatsbezogene Geheimhaltungsbeschränkungen zu prüfen. Während der Beizug einer ordnungsgemäss verpflichteten Hilfsperson gemäss Art. 321 StGB und Art. 9 DSG grundsätzlich keine vorgängige Einwilligung jedes einzelnen Klienten erfordert, muss der Kunde prüfen, ob spezifische Geheimhaltungsvereinbarungen (NDAs) mit Klienten, vertragliche Cloud-/KI-Verbote oder Amtsgeheimnispflichten (Art. 320 StGB) eine ausdrückliche Ermächtigung durch den Klienten voraussetzen oder die Nutzung optionaler externer Funktionen (wie die externe Web-Recherche gemäss Ziffer 8) einschränken.

14. Cookies und ähnliche Technologien

Wir verwenden technisch zwingend erforderliche Cookies und gleichwertige Browserspeicherungen ausschliesslich für die Authentifizierung, die Sitzungsverwaltung, die Sicherheit sowie für wesentliche Plattformfunktionen. Wir setzen keine Werbe- oder Analyse-Tracking-Cookies von Drittanbietern ein. Sollten wir künftig optionale Analysefunktionen oder zusätzliche Cookies einführen, werden wir diese Datenschutzerklärung aktualisieren und, soweit erforderlich, vorgängig eine Einwilligung einholen.

15. Automatisierte Bearbeitung und Überprüfung von KI-Ergebnissen

Die Dienste nutzen automatisierte Bearbeitungsverfahren und grosse Sprachmodelle (Large Language Models, LLMs), um Ergebnisse für juristische Recherchen und Entwürfe zu erstellen. Legislator verwendet Kundeninhalte nicht für automatisierte Einzelentscheidungen, die für betroffene Personen mit einer Rechtsfolge verbunden sind oder sie erheblich beeinträchtigen, im Sinne von Art. 21 DSG oder Art. 22 DSGVO.

KI-generierte Ergebnisse sind unterstützende Hilfsmittel für die fachliche Beurteilung durch den Kunden und können Fehler, Auslassungen oder erfundene Zitate («Halluzinationen») enthalten. Gemäss Art. 12 Bst. a BGFA sowie der SAV-Wegleitung für den Umgang mit künstlicher Intelligenz (Ziff. 2.2–2.3) **bleibt der Kunde allein dafür verantwortlich, sämtliche KI-generierten Ergebnisse anhand der juristischen Originalquellen zu prüfen und zu verifizieren, bevor er sich darauf stützt**.

16. Rechte der betroffenen Personen und Anfragen

Gemäss dem DSG (Art. 25–29 und Art. 32 DSG) sowie, soweit anwendbar, der DSGVO (Art. 15–22 DSGVO) haben betroffene Personen – vorbehältlich der gesetzlichen Voraussetzungen und Ausnahmen – das Recht auf Auskunft und Information über die Bearbeitung ihrer Personendaten, auf Berichtigung unrichtiger Daten, auf Löschung («Recht auf Vergessenwerden») oder Unterlassung einer widerrechtlichen Bearbeitung, auf Einschränkung der Bearbeitung, auf Datenherausgabe oder -übertragung (Art. 28 DSG; Art. 20 DSGVO) sowie das Recht, einer auf berechtigten Interessen beruhenden Bearbeitung oder einer Bearbeitung zu Zwecken der Direktwerbung zu widersprechen und eine erteilte Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen.

Für Datenbearbeitungen, bei denen die Legislator AI AG als Verantwortliche auftritt, wenden Sie sich bitte an **legal@legislator.ch**. Wir antworten innerhalb der gesetzlichen Fristen: in der Regel innerhalb von 30 Tagen gemäss Art. 25 Abs. 7 DSG oder innerhalb eines Monats gemäss Art. 12 DSGVO (vorbehältlich zulässiger Fristverlängerungen).

Für Personendaten in Kundeninhalten (bei denen wir als Auftragsbearbeiter und Hilfsperson handeln) sind Gesuche an den verantwortlichen Kunden (z. B. die Anwaltskanzlei) zu richten. Wenn Sie uns bezüglich Kundeninhalten direkt kontaktieren, werden wir den Kunden unterstützen oder das Gesuch gemäss dem DPA an den Kunden weiterleiten, wobei wir das Berufsgeheimnis (Art. 321 StGB, Art. 13 BGFA) strikt wahren; wir legen niemals eigenmächtig Rechtsakten eines Kunden auf ein nicht verifiziertes Gesuch einer Drittpartei hin offen oder löschen diese.

Sie können ein Anliegen beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) unter https://www.edoeb.admin.ch vorbringen oder, sofern die DSGVO anwendbar ist, eine Beschwerde bei einer zuständigen EU-Aufsichtsbehörde einreichen.

17. Externe Websites und unabhängige Dienste

Rechtliche Quellenangaben, Suchergebnisse und sonstige Links können auf externe, von Dritten betriebene Websites führen. Wenn Sie diesen Links folgen oder unabhängig einen Dienst eines Drittanbieters nutzen, bearbeitet dieser Anbieter Daten gemäss seinen eigenen Datenschutzbestimmungen.

18. Änderungen dieser Datenschutzerklärung

Wir aktualisieren diese Datenschutzerklärung, wenn sich unsere Datenbearbeitung, unsere Dienste oder die anwendbaren gesetzlichen Anforderungen ändern. Die jeweils aktuelle Fassung ist jederzeit unter https://legislator.ch/privacy abrufbar und ersetzt alle früheren Fassungen.

Die englische Fassung dieser Datenschutzerklärung ist die massgebliche Fassung und geht im Falle von Abweichungen oder Widersprüchen gegenüber einer Übersetzung in eine andere Sprache vor.

Anhang 1 – Dienstleister, Unterauftragsbearbeiter und Bearbeitungsorte

Dieser Anhang bildet einen integrierenden Bestandteil der Datenschutzerklärung von Legislator.

1. Legislator AI AG (Betreiberin der Kernplattform – Eigene Infrastruktur)

Adresse: Kirchstrasse 6, 8807 Freienbach SZ, Schweiz (CHE-476.609.141).
Dienst & Daten: Kernplattform, Kontodatenbank, gespeicherte Kundeninhalte, Transformations-Caches, Schweizer Rechtsreferenzdatenbank, lokale Such-, Embedding- und Reranking-Modelle sowie tägliche Backups.
Bearbeitungsort: Schweiz (unternehmenseigene physische Server in der Schweiz, die im Eigentum und unter der Kontrolle der Legislator AI AG stehen).
Bedingungen & Garantien: Eigene physische Infrastruktur in der Schweiz; Verschlüsselung im Ruhezustand (Encryption at Rest); Aufbewahrung und Löschung (sofortige Löschung oder automatische Löschung nach 24 Stunden samt Backup-Bereinigung innert 24 Stunden) gemäss Ziffer 11.

2. Amazon Web Services EMEA SARL (Unterauftragsbearbeiter – Web-Reverse-Proxy-Gateway)

Adresse: 38 avenue John F. Kennedy, L-1855 Luxemburg.
Dienst & Daten: Web-Reverse-Proxy-Eingangs-Gateway, das TLS-verschlüsselte Prompts und Dateianhänge direkt an die eigenen physischen Server (On-Premises-Server) von Legislator in der Schweiz weiterleitet.
Bearbeitungsort: Schweiz (AWS Region Schweiz – Zürich eu-central-2).
Bedingungen & Garantien: Daten passieren das Gateway ausschliesslich in TLS-verschlüsselter Form; 0 Tage Aufbewahrung (keine Speicherung von Kundeninhalten). Angemessenheitsbeschluss für die Schweiz/EU (Art. 16 Abs. 1 DSG) sowie EU-Standardvertragsklauseln mit Schweizer Anpassungen (Art. 16 Abs. 2 Bst. d DSG).

3. Google Cloud EMEA Limited (Unterauftragsbearbeiter – Freigegebene KI-Inferenz, OCR & Audiotranskription)

Adresse: Velasco, Clanwilliam Place, Dublin 2, Irland.
Dienst & Daten: Transiente KI-Inferenz für genehmigte Gemini- und Anthropic-Claude-Modelle sowie OCR und Audiotranskription über die Gemini-API (Prompts, relevante Dokumenteninhalte, generierte Ausgaben und erforderliche Dienstmetadaten).
Bearbeitungsort: Europäische Union (genehmigte regionale EU-Rechenzentren in EU-Mitgliedstaaten, einschliesslich Belgien, der Niederlande, Deutschland, Finnland und Irland, mit strikter regionaler Routing-Durchsetzung).
Bedingungen & Garantien: Angemessenheitsbeschluss für EU-Mitgliedstaaten (Art. 16 Abs. 1 DSG / Anhang 1 DSV). Enterprise Zero Data Retention (ZDR – 0 Tage Inhaltsaufbewahrung) und genehmigte Ausnahme von der Prompt-Protokollierung zur Missbrauchsüberwachung (bestätigt am 1. September 2026 für alle Legislator-GCP-Projekte); striktes Verbot des Modelltrainings. Für jegliche administrativen oder Support-Metadaten, die einen Zugriff von ausserhalb des EWR/der Schweiz beinhalten: EU-Standardvertragsklauseln mit Schweizer Zusatz (Art. 16 Abs. 2 Bst. d DSG) sowie die Zertifizierung der Google LLC unter dem Swiss–U.S. und EU–U.S. Data Privacy Framework.

4. TensorX Ltd. (Unterauftragsbearbeiter – Open-Weights-KI-Inferenz)

Adresse: Unit 25, Classon House, Dundrum Business Park, Dublin 14, Irland.
Dienst & Daten: Transiente KI-Inferenz für unabhängig gehostete Open-Weights-Modelle, einschliesslich DeepSeek (Prompts, relevante Dokumenteninhalte, Ausgaben und Dienstmetadaten).
Bearbeitungsort: Europäische Union (Irland und Finnland) auf dedizierter souveräner GPU-Infrastruktur.
Bedingungen & Garantien: Angemessenheitsbeschluss für Irland und Finnland (Art. 16 Abs. 1 DSG / Anhang 1 DSV). Zero Data Retention (ZDR – 0 Tage Aufbewahrung von Inferenzinhalten) im flüchtigen Arbeitsspeicher (RAM)

mit sofortiger Löschung nach Abschluss der Anfrage; kein Modelltraining; keine Datenübermittlung an die ursprünglichen DeepSeek-Entwickler.

5. Google Cloud EMEA Limited (Unterauftragsbearbeiter – Web-Recherche)

Adresse: Velasco, Clanwilliam Place, Dublin 2, Irland (mit globaler Suchinfrastruktur der Google LLC).
Dienst & Daten: Web Grounding for Enterprise. Suchanfragen und Kontextinformationen, die übermittelt werden, wenn ein Nutzer aktiv die optionale externe Websuchfunktion auswählt (Ziffer 8).
Bearbeitungsort: Endpunkt in der Europäischen Union.
Bedingungen & Garantien: Vertragliche Zero Data Retention (0 Tage Aufbewahrung von Kundendaten und kein Modelltraining) gemäss den Bedingungen von Web Grounding for Enterprise; EU-Standardvertragsklauseln mit Schweizer Zusatz (Art. 16 Abs. 2 Bst. d DSG) sowie Zertifizierung der Google LLC unter dem Swiss–U.S. und EU–U.S. Data Privacy Framework für grenzüberschreitende Datenbekanntgaben.

6. Mailgun (Administrativer Dienstleister – E-Mail-Versand)

Rechtsträger: Mailgun Technologies, Inc. / Sinch Email (betrieben über den EU-Endpunkt api.eu.mailgun.net).
Dienst & Daten: Administrativer E-Mail-Versand ausschliesslich mit Empfänger-E-Mail-Adresse, Login-Code oder sicherem Zugangslink sowie Zustellungsmetadaten; keine Inhalte aus Rechtsakten, Prompts oder Dokumente.
Bearbeitungsort: Europäische Union (Deutschland, Irland und Belgien) für die Nachrichtenbearbeitung; Vereinigte Staaten für untergeordnete Konto-/Support-Metadaten.
Bedingungen & Garantien: Angemessenheit für die Bearbeitung in der EU (Art. 16 Abs. 1 DSG); EU-Standardvertragsklauseln mit Schweizer Anpassungen (Art. 16 Abs. 2 Bst. d DSG) sowie Swiss-U.S. Data Privacy Framework für die Übermittlung administrativer Metadaten. Administrative Aufbewahrung gemäss Ziffer 11.

7. Resend – Plus Five Five, Inc. (Administrativer Dienstleister – E-Mail-Versand)

Adresse: Plus Five Five, Inc., 2261 Market Street #5039, San Francisco, CA 94114, Vereinigte Staaten.
Dienst & Daten: Administrativer E-Mail-Versand, der ausschliesslich die E-Mail-Adresse der empfangenden Person, den Anmeldecode oder einen sicheren Zugangslink sowie Zustellmetadaten enthält; keine juristischen Akteninhalte, Prompts oder Dokumente.
Bearbeitungsort: Vereinigte Staaten für das E-Mail-Routing und die Speicherung zugehöriger administrativer Metadaten.
Bedingungen & Garantien: Vertragliche Zero Data Retention (0 Tage Aufbewahrung für E-Mail-Inhalte). EU-Standardvertragsklauseln mit schweizerischen Anpassungen (Art. 16 Abs. 2 Bst. d DSG). Administrative Aufbewahrung gemäss Ziffer 11 (die ZDR für KI-Inferenz gilt nicht für E-Mail-Zustellmetadaten).

8. Stripe (Administrativer Dienstleister und eigenständiger Verantwortlicher – Zahlungen & Abonnemente)

Rechtsträger: Stripe Payments Europe, Limited (1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Irland) und Stripe, Inc. (354 Oyster Point Blvd, South San Francisco, CA 94080, Vereinigte Staaten).
Dienst & Daten: Abrechnung, Zahlungsinformationen, Transaktionsreferenzen sowie Sicherheitsmetadaten zur Betrugsprävention; keine Prompts oder hochgeladenen juristischen Dateien.
Bearbeitungsort: Europäische Union (Irland und Deutschland) sowie Vereinigte Staaten.
Bedingungen & Garantien: Angemessenheitsbeschluss für die Bearbeitung in der EU (Art. 16 Abs. 1 DSG); aktive Zertifizierung der Stripe, Inc. unter dem Swiss–U.S. und EU–U.S. Data Privacy Framework sowie EU-Standardvertragsklauseln mit Schweizer Anpassungen (Art. 16 Abs. 2 Bst. d DSG). Gesetzliche 10-jährige Aufbewahrungspflicht für Buchungsbelege (Art. 958f OR).

Offizielle Links zum Datenschutz der Dienstleister:

Google Cloud: https://cloud.google.com/terms/data-processing-addendum
TensorX: https://tensorx.ai/dpa/ und https://tensorx.ai/privacy-policy/

Amazon Web Services (AWS): https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
Mailgun: https://www.mailgun.com/legal/privacy-policy/ und https://www.mailgun.com/legal/dpa/
Resend: https://resend.com/legal/dpa und https://resend.com/security/gdpr
Stripe: https://stripe.com/legal/dpa und https://stripe.com/privacy