Technische und organisatorische Maßnahmen

Stand: 9. Juni 2026

Anlage zur Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

1. Verantwortliche Stelle / Auftragsverarbeiter

Fiscova GmbH
Donaustraße 44
12043 Berlin
Deutschland

Vertreten durch die Geschäftsführer Sebastian Ternes und Tobias Wedel
Handelsregister: Amtsgericht Berlin-Charlottenburg, HRB 283761 B

Diese technischen und organisatorischen Maßnahmen beschreiben die Sicherheitsmaßnahmen von Fiscova für die Verarbeitung personenbezogener Daten im Rahmen der Fiscova-Plattform.

2. Ziel der Maßnahmen

Fiscova verarbeitet personenbezogene Daten für Steuerkanzleien, insbesondere Kommunikations-, Mandanten-, Nutzer-, E-Mail-, Telefonie-, WhatsApp-, Aufgaben- und Vorgangsdaten.

Ziel dieser Maßnahmen ist es, ein angemessenes Schutzniveau sicherzustellen, insbesondere im Hinblick auf:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit der Systeme
- Schutz vor unbefugtem Zugriff
- Schutz vor Verlust oder Veränderung
- Mandantentrennung
- sichere Verarbeitung von Kanzlei- und Mandantendaten
- Unterstützung der Anforderungen aus Art. 28 und Art. 32 DSGVO

3. Infrastruktur und Hosting

Die Fiscova-Plattform wird nach aktueller Konfiguration über folgende Infrastruktur betrieben:

- Cloudflare für DNS, CDN, WAF und Connector-Funktionen
- Hetzner für Frontend-Hosting
- Hetzner für Backend-Hosting
- PostgreSQL-Datenbank auf Hetzner-Infrastruktur
- Hetzner S3-kompatibler Storage für Dateien und Anhänge
- Serverstandort der wesentlichen Hetzner-Infrastruktur: Nürnberg, Deutschland
- Clerk für Authentifizierung und Nutzerverwaltung
- Sipgate für Telefonie
- Amazon Bedrock in der Region Frankfurt für bestimmte KI-Funktionen
- Deepslate als externer KI-Dienst mit Sitz in Deutschland

Fiscova ist auf eine möglichst EU-nahe Verarbeitung ausgelegt. Wesentliche Plattformkomponenten werden nach aktueller Konfiguration in Deutschland betrieben.

4. Zutrittskontrolle

Ziel: Verhinderung des unbefugten physischen Zutritts zu Systemen, auf denen personenbezogene Daten verarbeitet werden.

Maßnahmen:

- Fiscova betreibt keine eigenen Rechenzentren.
- Physische Sicherheit der Serverinfrastruktur wird durch die jeweiligen Infrastruktur- und Hostinganbieter gewährleistet.
- Wesentliche Plattformkomponenten werden bei Hetzner betrieben.
- Fiscova prüft eingesetzte Anbieter im Rahmen der Dienstleisterauswahl und dokumentiert diese in der Unterauftragsverarbeiterliste.
- Zugriff auf Büroräume und Arbeitsgeräte von Fiscova ist auf berechtigte Personen beschränkt.
- Arbeitsgeräte sind gegen unbefugte Nutzung zu schützen.

5. Zugangskontrolle

Ziel: Verhinderung der unbefugten Nutzung von Systemen, Anwendungen und Konten.

Maßnahmen:

- Nutzerkonten sind individuell zugeordnet.
- Der Login zur Fiscova-Plattform erfolgt aktuell über E-Mail-Adresse und Passwort.
- Passwortdaten werden nicht im Klartext gespeichert.

- Zugriff auf Administrationssysteme ist auf berechtigte Personen beschränkt.
- Administrative Zugänge werden nur an Personen vergeben, die diese für ihre Tätigkeit benötigen.
- Zugangsdaten dürfen nicht geteilt werden.
- Beim Ausscheiden von Mitarbeitenden oder Wegfall einer Berechtigung werden Zugänge entzogen oder angepasst.
- Multi-Faktor-Authentifizierung für Plattformnutzer ist aktiviert.
- Für interne Administrationszugänge werden zusätzliche Schutzmaßnahmen eingesetzt, soweit technisch verfügbar und erforderlich.

6. Zugriffskontrolle

Ziel: Sicherstellung, dass berechtigte Nutzer nur auf die Daten zugreifen können, die sie zur Aufgabenerfüllung benötigen.

Maßnahmen:

- Rollen- und rechtebasierte Zugriffskonzepte innerhalb der Plattform.
- Trennung von Kanzleien und Mandantenbereichen durch Tenant- bzw. Kanzleizuordnung.
- Zugriff auf Kundendaten durch Fiscova nur zweckgebunden, insbesondere für Support, Fehleranalyse, Sicherheit oder Betrieb.
- Supportzugriffe erfolgen nach dem Need-to-know-Prinzip.
- Administrative Zugriffe sind auf berechtigte Personen beschränkt.
- Berechtigungen werden bei Rollenänderungen, Austritt oder Wegfall der Erforderlichkeit angepasst.
- Zugriff auf Produktivsysteme ist auf notwendige Personen begrenzt.
- Datenbank-, Storage- und Infrastrukturzugriffe sind intern nur für berechtigte technische Rollen vorgesehen.
- Soweit möglich und angemessen, erfolgen Supportzugriffe nach vorheriger Anfrage oder Freigabe durch den Kunden.
- Supportzugriffe auf Kundendaten werden protokolliert.

7. Trennungskontrolle

Ziel: Getrennte Verarbeitung von Daten unterschiedlicher Kunden und Zwecke.

Maßnahmen:

- Logische Trennung von Kanzleien innerhalb der Plattform.
- Zuordnung von Daten zu Kanzlei-, Nutzer-, Vorgangs- oder Mandantenkontexten.
- Rollen- und Berechtigungssystem zur Einschränkung von Zugriffen.
- Getrennte Behandlung von Website-Daten und Plattformdaten.
- Keine Marketingtracking-Technologien im Dashboard.

- Keine Produktanalytics im Dashboard nach aktueller Konfiguration.
- Keine Nutzung von Mandanten- und Kommunikationsdaten zum Training allgemeiner KI-Modelle, soweit nicht ausdrücklich gesondert vereinbart.
- Test-, Entwicklungs- und Produktivdaten werden getrennt verarbeitet.
- Echtdaten sollen in Entwicklungs- oder Testumgebungen nur verwendet werden, wenn dies erforderlich und zulässig ist.

8. Weitergabekontrolle

Ziel: Schutz personenbezogener Daten bei Übertragung, Weitergabe und Zugriff durch Dritte.

Maßnahmen:

- Verschlüsselte Übertragung über TLS, soweit technisch unterstützt.
- Einsatz dokumentierter Dienstleister und Unterauftragsverarbeiter.
- Abschluss von Vereinbarungen zur Auftragsverarbeitung mit relevanten Dienstleistern, soweit erforderlich.
- Unterauftragsverarbeiter werden in einer Unterauftragsverarbeiterliste geführt.
- Drittlandübermittlungen erfolgen nur auf geeigneter Grundlage, insbesondere Angemessenheitsbeschluss, EU-Standardvertragsklauseln oder sonstige zulässige Transfermechanismen.
- Export- und Schnittstellenfunktionen werden auf berechtigte Nutzer und vereinbarte Zwecke beschränkt.
- API-Zugriffe und Integrationen werden über Authentifizierungs- und Berechtigungsmechanismen abgesichert.
- E-Mail-, Telefonie-, WhatsApp- und KI-Anbieter werden nur eingesetzt, soweit sie für die Plattformfunktion erforderlich sind.

9. Eingabekontrolle und Nachvollziehbarkeit

Ziel: Nachvollziehbarkeit von relevanten Eingaben, Änderungen, Zugriffen und Supporthandlungen.

Maßnahmen:

- Verarbeitung technischer System- und Sicherheitslogs, soweit für Betrieb, Sicherheit und Fehleranalyse erforderlich.
- Protokollierung relevanter Login- und Authentifizierungsereignisse, soweit technisch verfügbar.
- Protokollierung technischer API- und Verbindungsvorgänge, soweit für Betrieb und Sicherheit erforderlich.
- Dokumentation von Supportfällen.
- Protokollierung von Supportzugriffen auf Kundendaten.

- Supportzugriffslogs enthalten insbesondere Zeitpunkt, zugreifende Person, betroffenen Kunden, Zweck bzw. Supportgrund und, soweit vorhanden, Ticket- oder Vorgangsbezug.
- Fehlermeldungen und Sicherheitsereignisse werden intern analysiert.
- Logs werden nur so lange gespeichert, wie dies für Betrieb, Sicherheit, Fehleranalyse und Nachweiszwecke erforderlich ist.
- Administrative Änderungen und sicherheitsrelevante Vorgänge werden, soweit technisch umgesetzt, nachvollziehbar dokumentiert.

10. Auftragskontrolle

Ziel: Sicherstellung, dass personenbezogene Daten nur nach Weisung des Kunden verarbeitet werden.

Maßnahmen:

- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit Kunden.
- Dokumentierte Beschreibung von Gegenstand, Art, Zweck und Dauer der Verarbeitung.
- Verarbeitung von Kundendaten nur nach Vertrag, Produktkonfiguration oder dokumentierter Weisung.
- Interne Beschränkung von Supportzugriffen auf erforderliche Zwecke.
- Protokollierung von Supportzugriffen auf Kundendaten.
- Prüfung und Dokumentation eingesetzter Unterauftragsverarbeiter.
- Verpflichtung eingesetzter Personen auf Vertraulichkeit.
- Prozesse zur Bearbeitung von Betroffenenanfragen in Abstimmung mit dem Kunden.
- Prozesse zur Meldung von Datenschutzverletzungen an betroffene Kunden.

11. Verfügbarkeitskontrolle

Ziel: Schutz vor zufälligem Verlust oder Zerstörung und Sicherstellung der Wiederherstellbarkeit.

Maßnahmen:

- Betrieb wesentlicher Plattformkomponenten über professionelle Hosting- und Infrastrukturprovider.
- Schutz vor bestimmten Angriffen durch Cloudflare WAF und CDN-Funktionen.
- Technische Maßnahmen zur Absicherung von Datenbank und Storage.
- Regelmäßige automatisierte Backups relevanter Produktivdaten.
- Backup-Frequenz: täglich.
- Backup-Aufbewahrungsdauer: 30 Tage.
- Backups werden zugriffsbeschränkt gespeichert.
- Wiederherstellungsprozesse sind dokumentiert bzw. werden im Rahmen des Betriebs weiter formalisiert.
- Wiederherstellungstests werden regelmäßig durchgeführt und dokumentiert; ein Wiederherstellungstest wurde durchgeführt.

- Daten in Backups werden nach dem geltenden Backup- und Löschkonzept überschrieben oder gelöscht.
- Kritische Störungen werden priorisiert bearbeitet.
-

12. Integritätskontrolle

Ziel: Schutz personenbezogener Daten vor unbeabsichtigter oder unbefugter Veränderung.

Maßnahmen:

- Berechtigungskonzepte für schreibende und administrative Zugriffe.
- Technische Zugriffsbeschränkungen auf Datenbank, Storage und Backend.
- Nutzung versionierter Softwareentwicklung und kontrollierter Deployments.
- Beschränkung produktiver Änderungen auf berechtigte Personen.
- Schutz von Schnittstellen durch Authentifizierung und Autorisierung.
- Fehlerhafte oder sicherheitsrelevante Änderungen werden analysiert und korrigiert.
- Produktivsysteme werden nicht für unkontrollierte Tests verwendet.
- Backups dienen zusätzlich der Wiederherstellung bei unbeabsichtigter Veränderung oder Verlust von Daten.

13. Verschlüsselung und Schutz gespeicherter Inhalte

Ziel: Schutz von Inhaltsdaten gegen unbefugte Kenntnisnahme.

Maßnahmen:

- Verschlüsselte Übertragung von Daten über TLS, soweit technisch unterstützt.
- Verschlüsselte Speicherung von E-Mail-Inhalten und Anhängen.
- Verwendung eigener Verschlüsselungsschlüssel für gespeicherte E-Mail-Inhalte und Anhänge.
- Die Verschlüsselungsschlüssel werden aktuell über geschützte Umgebungsvariablen der Produktivinfrastruktur verwaltet.
- Zugriff auf Umgebungsvariablen und Entschlüsselungsmechanismen ist auf berechtigte technische Rollen beschränkt.
- API-Schlüssel, Zugangsdaten und Secrets dürfen nicht im Quellcode gespeichert werden.
- Hetzner S3 Buckets sind nach aktueller Konfiguration nicht öffentlich zugänglich.
- Zugriff auf Dateien und Anhänge erfolgt nur über geschützte bzw. signierte Zugriffsmechanismen.
- Eine weitergehende Dokumentation zur Schlüsselverwaltung, Rotation und Zugriffskontrolle wird gepflegt bzw. weiterentwickelt.

14. Mandantendaten, Audio und Transkripte

Ziel: Schutz besonders sensibler Kommunikations- und Mandantendaten.

Maßnahmen:

- Audioaufnahmen und Transkripte sind standardmäßig deaktiviert.
- Speicherung von Audioaufnahmen und Transkripten erfolgt nur, wenn die Funktion aktiviert ist und eine entsprechende Einwilligung des Anrufers oder Mandanten vorliegt.
- E-Mail-Inhalte und Anhänge werden verschlüsselt verarbeitet.
- Gmail- und Outlook-Inhalte werden grundsätzlich synchronisiert bzw. angezeigt; dauerhafte Speicherung erfolgt nur, soweit dies für die Plattformfunktion erforderlich oder durch die Kanzlei konfiguriert wurde.
- Mandanten- und Kommunikationsdaten werden nicht zum Training allgemeiner KI-Modelle genutzt, soweit nicht ausdrücklich gesondert vereinbart.
- KI-Verarbeitung erfolgt zur Bereitstellung vereinbarter Plattformfunktionen.
- Supportzugriffe auf Mandanten- und Kommunikationsdaten werden zweckgebunden durchgeführt und protokolliert.

15. Datenschutzfreundliche Voreinstellungen

Ziel: Datenminimierung und Schutz durch Voreinstellungen.

Maßnahmen:

- Keine Marketingtracking-Technologien im Dashboard.
- Keine Produktanalytics im Dashboard nach aktueller Konfiguration.
- Audioaufnahmen und Transkripte standardmäßig deaktiviert.
- Rollenbasierte Zugriffsvergabe.
- Verarbeitung nur der für die jeweilige Funktion erforderlichen Daten.
- Kundendaten werden nicht für allgemeines KI-Training verwendet.
- Zugriffe auf Kundendaten erfolgen zweckgebunden und werden bei Supportzugriffen protokolliert.
- Website-Daten und Plattformdaten werden getrennt betrachtet und dokumentiert.

16. Vertraulichkeit und Personal

Ziel: Sicherstellung, dass Personen mit Datenzugriff zur Vertraulichkeit verpflichtet sind.

Maßnahmen:

- Personen mit Zugriff auf Kundendaten werden zur Vertraulichkeit verpflichtet.
- Mitarbeitende, Gründer, Werkstudenten und sonstige eingesetzte Personen werden über den vertraulichen Umgang mit Kanzlei- und Mandantendaten informiert.

- Zugriff auf Kundendaten wird nur gewährt, soweit dies zur jeweiligen Aufgabe erforderlich ist.
- Sensibilisierung für besondere Vertraulichkeit von Steuerkanzlei- und Mandantendaten.
- Verpflichtung zur Meldung von Sicherheitsvorfällen oder Verdachtsfällen.
- Nach Ende der Tätigkeit sind Zugänge zu entziehen und Vertraulichkeitspflichten bleiben bestehen.
- Supportzugriffe werden dokumentiert, um interne Nachvollziehbarkeit sicherzustellen.

17. Incident Response und Datenschutzverletzungen

Ziel: Schnelle Erkennung, Bearbeitung und Meldung von Sicherheits- und Datenschutzvorfällen.

Maßnahmen:

- Interner Prozess zur Behandlung von Sicherheits- und Datenschutzvorfällen.
- Bewertung von Vorfällen nach Art, Umfang, betroffenen Daten und Risiko.
- Unverzügliche Information betroffener Kunden, wenn eine Datenschutzverletzung im Rahmen der Auftragsverarbeitung festgestellt wird.
- Unterstützung der Kunden bei Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.
- Dokumentation festgestellter Datenschutzverletzungen.
- Ergreifen angemessener Sofortmaßnahmen zur Begrenzung möglicher Schäden.
- Nachbereitung relevanter Vorfälle zur Verbesserung der Schutzmaßnahmen.
- Nutzung vorhandener Logs, insbesondere technischer Logs und Supportzugriffslogs, zur Analyse von Vorfällen.

18. Löschung und Datenrückgabe

Ziel: Sicherstellung, dass Daten nicht länger als erforderlich verarbeitet werden.

Maßnahmen:

- Löschung oder Rückgabe von Kundendaten nach Vertragsende gemäß AVV, Hauptvertrag und Weisung des Kunden.
- Unterstützung von Datenexporten, soweit technisch verfügbar und vertraglich vorgesehen.
- Löschung oder Anonymisierung von Daten, wenn der Zweck entfällt und keine Aufbewahrungspflichten entgegenstehen.
- Kontakt-, Support- und Vertragsdaten werden nach jeweiligen gesetzlichen oder vertraglichen Aufbewahrungsanforderungen gespeichert.
- Daten in Backups werden nach dem geltenden Backup- und Löschkonzept überschrieben oder gelöscht.
- Löschprozesse werden abhängig von Systemreife und Produktumfang weiter dokumentiert und automatisiert.

19. Entwicklung, Deployment und technische Änderungen

Ziel: Sichere Entwicklung und kontrollierte Änderung der Plattform.

Maßnahmen:

- Nutzung von Code-Hosting und Versionskontrolle.
- Änderungen an der Plattform erfolgen über kontrollierte Entwicklungs- und Deployment-Prozesse.
- Produktivzugriffe und Deployments sind auf berechtigte Personen beschränkt.
- Kritische Änderungen sollen vor Veröffentlichung geprüft werden.
- Secrets, API-Schlüssel und Zugangsdaten sollen nicht im Quellcode gespeichert werden.
- Sicherheitsrelevante Fehler werden priorisiert behoben.
- Eingesetzte Abhängigkeiten und Dienste werden regelmäßig im Rahmen des Entwicklungsprozesses überprüft.
- Änderungen mit Auswirkungen auf Datenschutz oder Sicherheit werden gesondert bewertet.

20. Regelmäßige Überprüfung und Weiterentwicklung

Ziel: Sicherstellung, dass die TOMs dem Stand der Technik und dem Risiko angemessen bleiben.

Maßnahmen:

- Regelmäßige Überprüfung der eingesetzten technischen und organisatorischen Maßnahmen.
- Anpassung der Maßnahmen bei Änderungen der Plattform, Infrastruktur, Anbieter oder Risiken.
- Überprüfung der Unterauftragsverarbeiterliste bei Anbieterwechseln.
- Prüfung neuer Funktionen auf Datenschutz- und Sicherheitsauswirkungen.
- Weiterentwicklung von MFA, Logging, Backup, Lösch- und Zugriffskonzepten.
- Dokumentation wesentlicher Änderungen an den TOMs.
- Regelmäßige oder anlassbezogene Überprüfung der Backup- und Supportzugriffsprozesse.

21. Aktuelle geplante Verbesserungen

Folgende Maßnahmen sind geplant oder werden weiter ausgebaut:

- Laufende Überprüfung und Härtung der bereits aktivierten Multi-Faktor-Authentifizierung für Plattformnutzer.
- Weitere Schärfung der Dokumentation zur Schlüsselverwaltung.
- Weitere Formalisierung des Backup- und Wiederherstellungskonzepts.
- Weitere Formalisierung des Supportzugriffsprozesses.
- Weitere Dokumentation von Löschfristen je Datenkategorie.
- Ausbau der Auditierbarkeit administrativer Zugriffe.
- Ergänzung weiterer interner Security- und Datenschutzrichtlinien.

Diese geplanten Maßnahmen stellen keine bereits vollständig umgesetzten Zusicherungen dar, sondern beschreiben die aktuelle Sicherheits-Roadmap von Fiscova.