

Lösch- und Aufbewahrungskonzept

Stand: 9. Juni 2026

1. Anbieter

Fiscova GmbH

Donaustraße 44
12043 Berlin
Deutschland

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

2. Zweck dieses Konzepts

Dieses Lösch- und Aufbewahrungskonzept beschreibt, wie Fiscova personenbezogene Daten löscht, anonymisiert, zurückgibt oder aufbewahrt.

Es gilt insbesondere für:

- die öffentliche Website fiscova.de,
- die Fiscova-Plattform unter <https://dashboard.fiscova.de>,
- Kunden-, Vertrags- und Abrechnungsdaten,
- Support- und Kommunikationsdaten,
- Daten, die Fiscova im Auftrag von Steuerkanzleien verarbeitet,
- technische Logs,
- Backups,
- interne Compliance-Dokumentation.

Das Konzept dient der Umsetzung des Grundsatzes der Speicherbegrenzung und der Anforderungen aus DSGVO, AVV, TOMs und Kundenverträgen.

3. Grundsätze

Fiscova verarbeitet und speichert personenbezogene Daten nur so lange, wie dies für den jeweiligen Zweck erforderlich ist oder gesetzliche Aufbewahrungspflichten bestehen.

Es gelten folgende Grundsätze:

- Daten werden zweckgebunden verarbeitet.

- Nicht mehr erforderliche Daten werden gelöscht oder anonymisiert.
- Gesetzliche Aufbewahrungspflichten bleiben unberührt.
- Kundendaten aus der Fiscova-Plattform werden nach Weisung des Kunden gelöscht, exportiert oder zurückgegeben.
- Löschungen müssen technisch nachvollziehbar und organisatorisch kontrollierbar sein.
- Backups werden nach definierten Fristen überschrieben oder gelöscht.
- Löschrufen werden regelmäßig überprüft und bei Änderungen der Systeme, Produkte oder Rechtslage angepasst.

4. Rollenklärung

4.1 Eigene Verantwortlichkeit von Fiscova

Fiscova ist für bestimmte Daten eigener Verantwortlicher, insbesondere bei:

- Website-Besuchern,
- Interessenten,
- Newsletter-Abonnenten,
- Demo-Anfragen,
- Kundenkontakten,
- Vertrags- und Abrechnungsdaten,
- Supportkommunikation,
- Plattformnutzerkonten, soweit Fiscova eigene Zwecke verfolgt,
- interner Verwaltung.

Für diese Daten entscheidet Fiscova über Löschung und Aufbewahrung.

4.2 Auftragsverarbeitung für Kanzleikunden

Soweit Fiscova Mandanten-, Kommunikations-, E-Mail-, Telefonie-, WhatsApp-, Vorgangs- oder Kanzleidaten im Auftrag einer Steuerkanzlei verarbeitet, entscheidet grundsätzlich die Kanzlei als Verantwortlicher über Löschung, Rückgabe und Aufbewahrung.

Fiscova unterstützt die Kanzlei nach Maßgabe der AVV, des Hauptvertrags und der technischen Möglichkeiten.

5. Löschrufen- und Aufbewahrungsfristen

5.1 Website-Serverlogs

Datenarten:

IP-Adresse, Zeitstempel, Browserinformationen, technische Zugriffsdaten, Referrer, Fehlerdaten.

Zweck:

Sicherheit, Fehleranalyse, Betrieb der Website.

Regelfrist:

7 bis 30 Tage, sofern keine längere Speicherung zur Untersuchung von Sicherheitsvorfällen erforderlich ist.

Löschung:

Automatisierte oder regelmäßige Löschung nach Ablauf der Frist.

5.2 Consent-Daten / Cookie-Einstellungen

Datenarten:

Consent-ID, Auswahl, Zeitstempel, technische Metadaten.

Zweck:

Nachweis und Umsetzung von Einwilligungen und Widerrufen.

Regelfrist:

Bis zu 12 Monate oder bis zur erneuten Consent-Abfrage, sofern keine längere Nachweiserforderlichkeit besteht.

Löschung:

Löschung oder Überschreibung bei neuer Consent-Entscheidung oder nach Ablauf der Nachweisfrist.

5.3 Kontaktformular- und Demo-Anfragen

Datenarten:

Name, E-Mail-Adresse, Telefonnummer, Kanzlei/Unternehmen, Nachricht, Anfragezeitpunkt, technische Metadaten.

Zweck:

Bearbeitung von Anfragen, Demo-Vereinbarung, vorvertragliche Kommunikation.

Regelfrist:

Bis zur abschließenden Bearbeitung und danach grundsätzlich bis zu 12 Monate nach dem letzten Kontakt.

Ausnahme:

Wenn aus der Anfrage ein Vertragsverhältnis entsteht oder gesetzliche Aufbewahrungspflichten greifen, gelten die entsprechenden Vertrags- und Geschäftsunterlagenfristen.

Löschung:

Regelmäßige Löschung aus Supabase, E-Mail-Postfächern und CRM-/Kontaktlisten, soweit keine Aufbewahrungspflichten entgegenstehen.

5.4 Newsletterdaten

Datenarten:

E-Mail-Adresse, Name, Kanzlei/Unternehmen, Anmeldezeitpunkt, Einwilligungsnachweis, Öffnungs- und Klickdaten, Abmeldestatus.

Zweck:

Newsletterversand, Nachweis der Einwilligung, Analyse der Newsletter-Nutzung.

Regelfrist:

Für die Dauer des Newsletter-Abonnements.

Nach Abmeldung:

Sperr- und Nachweisdaten werden so lange gespeichert, wie dies zur Dokumentation der Einwilligung, des Widerrufs und zur Vermeidung erneuter unzulässiger Zusendung erforderlich ist.

Löschung:

Aktive Newsletterdaten werden nach Abmeldung gelöscht oder auf eine Sperrliste reduziert.

5.5 HubSpot Meetings / Terminbuchungen

Datenarten:

Name, E-Mail-Adresse, Kanzlei/Unternehmen, Termin, Kommunikationsinhalte, technische Metadaten.

Zweck:

Terminvereinbarung, Durchführung von Demo- und Informationsgesprächen.

Regelfrist:

Bis zu 12 Monate nach dem letzten Kontakt, sofern kein Vertragsverhältnis entsteht.

Bei Vertragsverhältnis:

Speicherung nach Vertrags- und Geschäftsunterlagenfristen.

5.6 Website-Analytics und Marketingdaten

Datenarten:

Google-Analytics-Daten, Meta-Pixel-Events, Kampagnenparameter, technische Identifikatoren, Nutzungsereignisse.

Zweck:

Analyse, Kampagnenmessung, Conversion Tracking, Optimierung von Ads.

Regelfrist:

Nach den im jeweiligen Tool konfigurierten Aufbewahrungsfristen und nur auf Grundlage einer Einwilligung.

Löschung/Widerruf:

Bei Widerruf werden keine neuen einwilligungspflichtigen Trackingdaten erhoben. Bereits bei Drittanbietern verarbeitete Daten werden nach den jeweiligen Anbieterprozessen und Einstellungen gelöscht oder anonymisiert.

5.7 Plattformnutzerkonten

Datenarten:

Name, E-Mail-Adresse, Kanzleizugehörigkeit, Rolle, Berechtigungen, Login-Daten, Authentifizierungsergebnisse.

Zweck:

Bereitstellung der Plattform, Authentifizierung, Zugriffskontrolle, Sicherheit.

Regelfrist:

Für die Dauer der Plattformnutzung bzw. des Vertragsverhältnisses.

Nach Deaktivierung:

Nutzerkonten werden deaktiviert oder gelöscht, sobald sie nicht mehr erforderlich sind. Technische Nachweise und Sicherheitslogs können für eine begrenzte Zeit weiter gespeichert werden.

Empfohlene Frist:

Deaktivierte Nutzerkonten: Löschung oder Anonymisierung grundsätzlich innerhalb von 90 Tagen nach Wegfall der Berechtigung, sofern keine Nachweispflichten entgegenstehen.

5.8 Mandanten- und Kommunikationsdaten in der Plattform

Datenarten:

Mandantendaten, E-Mail-Inhalte, Anhänge, WhatsApp-Nachrichten, Telefoniedaten, Vorgangsdaten, Aufgaben, Bearbeitungsstatus, Kommunikationshistorie.

Zweck:

Bereitstellung der Fiscova-Plattform im Auftrag der Kanzlei.

Regelfrist:

Nach Weisung der Kanzlei, nach Produktkonfiguration und nach Hauptvertrag/AVV.

Standard bei Vertragsende:

Export, Rückgabe oder Löschung nach Weisung der Kanzlei.

Empfohlene Standardfrist nach Vertragsende:

Löschung produktiver Kundendaten grundsätzlich innerhalb von 30 bis 90 Tagen nach Vertragsende, sofern kein Export, keine offene Abrechnung, keine Rechtsverteidigung und keine gesetzliche Pflicht entgegensteht.

5.9 E-Mail-Inhalte und Anhänge

Datenarten:

E-Mail-Metadaten, Betreff, Inhalt, Anhänge, technische Header, Zuordnung zu Vorgängen/Mandanten.

Zweck:

Anzeige, Synchronisation, Strukturierung, KI-gestützte Unterstützung und Bearbeitung von Kanzleikommunikation.

Regelfrist:

Nach Weisung und Konfiguration der Kanzlei.

Grundsatz:

Gmail- und Outlook-Inhalte werden grundsätzlich synchronisiert bzw. angezeigt. Dauerhafte Speicherung erfolgt nur, soweit dies für die Plattformfunktion erforderlich oder von der Kanzlei konfiguriert wurde.

Schutz:

E-Mail-Inhalte und Anhänge werden verschlüsselt verarbeitet.

5.10 Audioaufnahmen und Transkripte

Datenarten:

Audioaufnahmen, Transkripte, Telefonnummern, Zeitstempel, Anrufmetadaten, Zuordnung zu Vorgängen/Mandanten.

Zweck:

Anrufbearbeitung, Dokumentation, Zusammenfassung, Zuordnung zu Vorgängen.

Grundsatz:

Audioaufnahmen und Transkripte sind standardmäßig deaktiviert.

Speicherung:

Nur bei Aktivierung und Einwilligung des jeweiligen Anrufers oder Mandanten.

Empfohlene Frist:

Audioaufnahmen: möglichst kurz, z. B. 7 bis 30 Tage, sofern nicht länger erforderlich oder durch die Kanzlei anders angewiesen.

Transkripte: nach Kanzlei-Konfiguration, z. B. 30, 90 oder 180 Tage.

Löschung:

Nach Ablauf der konfigurierten Frist oder auf Weisung der Kanzlei.

5.11 KI-Verarbeitungsdaten

Datenarten:

Kommunikationsinhalte, Vorgangsdaten, E-Mail-Inhalte, Anhängeauszüge, Transkripte, technische Metadaten.

Zweck:

Klassifikation, Zusammenfassung, Priorisierung und Strukturierung von Vorgängen.

Grundsatz:

Mandanten- und Kommunikationsdaten werden nicht zum Training allgemeiner KI-Modelle genutzt, soweit nicht ausdrücklich gesondert vereinbart.

Regelfrist:

KI-Eingaben und KI-Ausgaben werden nur so lange gespeichert, wie dies zur Bereitstellung der Plattformfunktion, zur Anzeige für die Kanzlei, zur Fehleranalyse oder zur Vertragserfüllung erforderlich ist.

Löschung:

Nach Weisung der Kanzlei, Produktkonfiguration oder Vertragsende.

5.12 Supportdaten und Supportzugriffslogs

Datenarten:

Supportanfragen, Ticketinhalte, technische Fehlerbeschreibungen, Kundenzuordnung, Supportzugriffslogs, zugreifende Person, Zeitpunkt, Zweck, Ticket-/Vorgangsbezug.

Zweck:

Support, Fehleranalyse, Nachvollziehbarkeit, Sicherheit, Nachweis.

Regelfrist Supportkommunikation:

Bis zu 24 Monate nach Abschluss des Supportfalls, sofern keine längere Speicherung erforderlich ist.

Regelfrist Supportzugriffslogs:

12 bis 24 Monate, sofern keine längere Speicherung zur Untersuchung von Sicherheitsvorfällen, zur Nachweisführung oder zur Rechtsverteidigung erforderlich ist.

Löschung:

Regelmäßige Löschung oder Anonymisierung nach Ablauf der Frist.

5.13 Technische System-, Sicherheits- und API-Logs

Datenarten:

IP-Adressen, Zeitstempel, API-Aufrufe, technische Fehler, Sicherheitsereignisse, Loginereignisse, Systemereignisse.

Zweck:

Betrieb, Sicherheit, Fehleranalyse, Missbrauchserkennung, Nachvollziehbarkeit.

Regelfrist:

30 bis 180 Tage, abhängig von System, Risiko und Sicherheitszweck.

Sicherheitsvorfälle:

Bei konkretem Verdacht oder Vorfall können relevante Logs länger gespeichert werden, soweit dies zur Untersuchung, Beweissicherung oder Rechtsverteidigung erforderlich ist.

5.14 Backups

Datenarten:

Sicherung relevanter Produktivdaten, insbesondere Datenbank- und Plattformdaten.

Zweck:

Wiederherstellung bei Datenverlust, Fehlern, Sicherheitsvorfällen oder technischen Störungen.

Frequenz:

Täglich automatisiert.

Aufbewahrungsdauer:

30 Tage.

Löschung:

Backups werden nach Ablauf der Aufbewahrungsdauer automatisch überschrieben oder gelöscht.

Hinweis:

Einzelne Daten können in Backups bis zum Ablauf der Backup-Aufbewahrungsdauer enthalten bleiben, auch wenn sie im Produktivsystem bereits gelöscht wurden. Wiederhergestellte Daten werden nach Möglichkeit erneut anhand der geltenden Löschvorgaben bereinigt.

5.15 Kundenvertrags- und Abrechnungsdaten

Datenarten:

Verträge, Angebote, Rechnungen, Zahlungsinformationen, Geschäftsbriefe, Kundenkommunikation, steuerlich relevante Unterlagen.

Zweck:

Vertragsdurchführung, Abrechnung, Buchhaltung, Nachweis, gesetzliche Pflichten.

Regelfrist:

Nach handels- und steuerrechtlichen Aufbewahrungspflichten, insbesondere sechs, acht oder zehn Jahre je nach Dokumentenart.

Löschung:

Nach Ablauf gesetzlicher Aufbewahrungsfristen, sofern keine weitere Aufbewahrung zur Rechtsverteidigung erforderlich ist.

5.16 Interne Compliance-Dokumentation

Datenarten:

AVV, TOMs, Unterauftragsverarbeiterlisten, Einwilligungsnachweise, Supportzugriffsnachweise, Datenschutzvorfallsdokumentation, Vertraulichkeitsverpflichtungen, Anbieterprüfungen.

Zweck:

Nachweis der Datenschutz- und Compliance-Anforderungen.

Regelfrist:

Für die Dauer des jeweiligen Vertragsverhältnisses und danach so lange, wie Nachweis-, Verjährungs- oder gesetzliche Aufbewahrungspflichten bestehen.

Löschung:

Nach Ablauf der Nachweis- und Aufbewahrungserfordernisse.

6. Löschprozesse

Fiscova setzt je nach System und Datenart unterschiedliche Löschprozesse ein:

- automatische Löschung,
- manuelle Löschung nach Prüfung,
- Deaktivierung,
- Anonymisierung,
- Export und anschließende Löschung,
- Überschreibung in Backups nach Ablauf der Backup-Frist.

Löschungen werden nach Möglichkeit so durchgeführt, dass Daten nicht ohne unverhältnismäßigen Aufwand wiederhergestellt werden können.

7. Löschung auf Kundenweisung

Soweit Fiscova Daten im Auftrag einer Kanzlei verarbeitet, erfolgt die Löschung nach Weisung der Kanzlei, nach Produktkonfiguration oder nach Vertragsende.

Der Kunde kann insbesondere verlangen:

- Löschung bestimmter Daten,
- Export bestimmter Daten,
- Löschung eines Nutzerkontos,
- Löschung von Audioaufnahmen oder Transkripten,
- Löschung von Vorgängen,
- Löschung oder Deaktivierung einer Integration,
- Löschung nach Vertragsende.

Fiscova kann eine Löschung ablehnen oder einschränken, soweit gesetzliche Pflichten, berechnigte Sicherungsinteressen, offene Abrechnungsfragen, Rechtsverteidigung oder technische Einschränkungen entgegenstehen.

8. Umgang mit Betroffenenanfragen

Geht eine Löschanfrage einer betroffenen Person bei Fiscova ein und betrifft sie Daten, für die Fiscova eigener Verantwortlicher ist, prüft Fiscova die Anfrage eigenständig.

Betrifft die Anfrage Daten, die Fiscova im Auftrag einer Kanzlei verarbeitet, leitet Fiscova die Anfrage grundsätzlich an die Kanzlei weiter oder stimmt die Bearbeitung mit der Kanzlei ab.

Fiscova entscheidet über Mandanten- und Kommunikationsdaten der Kanzlei nicht eigenständig, soweit die Verarbeitung im Auftrag erfolgt.

9. Löschung bei Vertragsende

Nach Beendigung des Vertrags mit einer Kanzlei gilt grundsätzlich:

1. Der Kunde erhält Gelegenheit zum Export seiner Daten, soweit technisch verfügbar und vertraglich vorgesehen.
2. Produktive Kundendaten werden nach Weisung des Kunden gelöscht oder zurückgegeben.
3. Ohne abweichende Weisung erfolgt die Löschung produktiver Kundendaten grundsätzlich innerhalb von 30 bis 90 Tagen nach Vertragsende.

4. Backups werden nach Ablauf der Backup-Aufbewahrungsdauer von 30 Tagen überschrieben oder gelöscht.
5. Vertrags-, Abrechnungs- und Nachweisdaten bleiben nach gesetzlichen Pflichten gespeichert.

10. Ausnahmen von der Löschung

Eine Löschung kann ganz oder teilweise aufgeschoben werden, wenn:

- gesetzliche Aufbewahrungspflichten bestehen,
- Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind,
- Sicherheitsvorfälle untersucht werden,
- Missbrauch oder unbefugte Nutzung aufgeklärt werden muss,
- offene Vertrags-, Support- oder Abrechnungsfragen bestehen,
- die Löschung technisch nur über Backup-Zyklen möglich ist.

In solchen Fällen wird die Verarbeitung auf den jeweiligen Zweck beschränkt.

11. Verantwortlichkeiten intern

Für die Umsetzung dieses Lösch- und Aufbewahrungskonzepts sind verantwortlich:

- Geschäftsführung für Datenschutz- und Compliance-Entscheidungen,
- technische Leitung für Umsetzung technischer Lösch- und Backup-Prozesse,
- Support/Operations für Bearbeitung von Kundenanfragen,
- zuständige Systemverantwortliche für Löschung in den jeweiligen Tools,
- Datenschutzkontakt für Koordination und Dokumentation.

12. Überprüfung und Aktualisierung

Dieses Konzept wird regelmäßig und anlassbezogen überprüft, insbesondere bei:

- Einführung neuer Funktionen,
- Einführung neuer Anbieter,
- Änderungen an Datenflüssen,
- Änderungen an gesetzlichen Anforderungen,
- Sicherheitsvorfällen,
- Kundenanforderungen,
- Änderungen an Backup-, Logging- oder Löschprozessen.

Änderungen werden dokumentiert.

13. Kontakt

Fragen zu Löschung, Aufbewahrung oder Datenschutz können gerichtet werden an:

datenschutz@fiscova.de