

— FÜR BETRIEBS- UND PERSONALRÄTE

Protokolle in einfach vollstrecken

einfach vollstrecken ist eine Software, mit der Unternehmen die Vollstreckung eigener titulierter Forderungen vorbereiten. Die Software bereitet vor. Ihre Nutzerinnen und Nutzer entscheiden und geben frei.

Diese Funktionsbeschreibung zeigt, welche Angaben die Software dabei über Nutzerinnen und Nutzer festhält, wer sie sehen kann und wie lange sie gespeichert bleiben. Sie gibt den Softwarestand vom 16.10.2026 wieder.

Zweck

Die Software führt zwei getrennte Protokolle:

- **Das Protokoll (Audit-Log)** gehört zu Ihrer Organisation. Es hält fest, wer wann Fälle und ihre Bestandteile angelegt, geändert oder gelöscht hat, wer Erklärungen bestätigt und wer Entwürfe freigegeben hat. Es dient dem Nachweis dieser Schritte, auch des Vier-Augen-Prinzips: Im Unternehmen kann niemand einen eigenen Entwurf freigeben.
- **Das Sicherheitsprotokoll** führt die Anbieterin für eigene Zwecke. Es hält Anmeldungen und Fehlversuche fest und dient der Erkennung von Angriffen und Missbrauch.

Beide Protokolle speichern Angaben zu einzelnen Nutzerinnen und Nutzern. Nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) hat der Betriebsrat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, mitzubestimmen bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. In öffentlich-rechtlich organisierten Unternehmen kann stattdessen das Personalvertretungsrecht gelten.

Überblick

Die beiden Protokolle im Vergleich

Merkmal	Protokoll (Audit-Log) Ihrer Organisation	Sicherheitsprotokoll der Anbieterin
Inhalt	Anlegen, Ändern, Löschen; Import von Fällen und Zahlungseingängen; Bestätigungen, Freigaben, Downloads, Datenexport, CSV-Exporte; Benutzer, Rollen, zweiter Faktor; Schlüssel und Schreibzugriffe der Programmschnittstelle; Empfangsadressen für Benachrichtigungen (Webhooks); Einstellungen, erste Verknüpfung und Ablehnungen bei der Anmeldung über das Unternehmenskonto (SSO); Tarif	Anmeldungen (auch über das Unternehmenskonto), Abmeldungen, Fehlversuche bei Anmeldung und zweitem Faktor, genutzte Wiederherstellungscodes
Einsicht	Rolle Inhaber über den Datenexport; Anbieterin ohne fallbezogene Inhalte	keine Ansicht in der Software; nicht im Datenexport
Aufbewahrung	bis drei Jahre nach der Löschung Ihrer Organisation; fallbezogene Inhalte mit dem Löschen des Falls unlesbar	90 Tage, danach tägliche Löschung
Schutz	fallbezogene Inhalte je Fall verschlüsselt; Hash-Kette gegen Änderungen	keine Inhalte, keine Codes; IP-Adresse nur gekürzt

Angaben in jedem Protokolleintrag

- laufende Nummer
- Zeitpunkt in koordinierter Weltzeit (UTC), auf die Mikrosekunde genau
- Nummer des Benutzerkontos, das die Handlung ausgelöst hat; leer, wenn niemand angemeldet ist, zum Beispiel bei zeitgesteuerten Abläufen. Zu Zugriffen über die Programmschnittstelle siehe den Abschnitt „Programmschnittstelle (API)“, zur Anmeldung über das Unternehmenskonto den Abschnitt „Anmeldung über das Unternehmenskonto (SSO)“.
- Organisation und, wenn der Eintrag zu einem Fall gehört, die Nummer des Falls
- Art des Ereignisses sowie Art und Nummer des betroffenen Datensatzes
- Inhalt: die geänderten Felder mit altem und neuem Wert oder Angaben zum Vorgang
- IP-Adresse, nur gekürzt: Bei IPv4 wird der letzte Block auf 0 gesetzt, bei IPv6 bleiben nur die ersten 48 Bit. Die Anbieterin kann die Speicherung für die ganze Software abschalten; dann wird keine IP-Adresse gespeichert.
- Prüfsumme des Eintrags und Prüfsumme des vorherigen Eintrags (Hash-Kette)

Die Rolle der handelnden Person steht nicht im einzelnen Eintrag. Wer wann welche Rolle erhält oder verliert, steht als eigener Eintrag im Protokoll.

Was die Software nicht protokolliert

- Lesende Zugriffe: Fälle öffnen, Listen ansehen, suchen, filtern, Vorschau öffnen, Abrufe über die Programmschnittstelle. Ausnahmen sind das Herunterladen eines freigegebenen PDF, das Erstellen eines Übermittlungspakets, der Datenexport und die CSV-Exporte unter „Berichte und Export“.
- Passwörter, Geheimnisse und Codes des zweiten Faktors, Wiederherstellungscodes. Bei einer Änderung steht nur der Vermerk „geändert“ im Protokoll.

- Den Datenschnappschuss eines Entwurfs. Im Protokoll steht nur sein Prüfwert. Bei Eingängen stehen Speicherort und Prüfwert der Datei nicht im Protokoll.
- Den Inhalt hochgeladener Import-Dateien und Kontoauszüge. Im Protokoll stehen nur die Zahlen des Vorgangs sowie die angelegten Fälle und gebuchten Zahlungen.
- Den Zeitpunkt der letzten Anmeldung im Benutzerkonto. Anmeldungen stehen nur im Sicherheitsprotokoll.

Rollen und Zugriff auf das Protokoll

Rollen in Ihrer Organisation

Rolle	Rechte in der Software	Zugriff auf das Protokoll
Inhaber	alle Rechte: Fälle ansehen und bearbeiten, Entwürfe erstellen, Entwürfe anderer Personen freigeben, Benutzer, Schlüssel der Programmschnittstelle, Empfangsadressen für Benachrichtigungen und die Anmeldung über das Unternehmenskonto verwalten, Datenexport	Auszug im Datenexport
Sachbearbeitung	Fälle ansehen und bearbeiten, Entwürfe erstellen	kein Zugriff
Freigabe (in der Software: „Freigabe (Vier-Augen)“)	Fälle ansehen, Entwürfe anderer Personen freigeben	kein Zugriff
Lesen (in der Software: „Nur lesen“)	Fälle ansehen	kein Zugriff

Eine Ansicht des Protokolls gibt es im Kundenbereich nicht. Den Auszug erhält nur die Rolle Inhaber mit dem Datenexport, den sie selbst auslöst. Er enthält je Eintrag die laufende Nummer, den Zeitpunkt (UTC), das Ereignis, den Namen des Benutzers, den betroffenen Datensatz und den Inhalt. Fallbezogene Inhalte sind darin lesbar, solange der Fall besteht. Gekürzte IP-Adressen und Prüfsummen enthält der Auszug nicht. Er umfasst nur Einträge der eigenen Organisation. Jeder Datenexport steht selbst als Eintrag im Protokoll.

Ereignisse im Protokoll

Die Tabelle zeigt, welche Ereignisse einen Eintrag erzeugen. Zu jedem Eintrag kommen die Angaben aus dem Abschnitt „Angaben in jedem Protokolleintrag“ hinzu. „Inhaber“ meint den Auszug im Datenexport (ohne gekürzte IP-Adressen und Prüfsummen). „Anbieterin“ meint die Plattformverwaltung der Anbieterin.

Ereignis – erfasste Angaben – wer sieht es – Aufbewahrung

Ereignis	Erfasste Angaben	Wer sieht es	Aufbewahrung
Fall anlegen, ändern, löschen	Geänderte Felder mit altem und neuem Wert, zum Beispiel Aktenzeichen, Status, Gläubigerangaben mit gesetzlicher Vertretung und Vertretungsregel, Bankangaben. Die Bestätigungen zum Fall mit Wortlaut, Benutzer und Zeitpunkt.	Inhaber: alle Angaben. Anbieterin: nur die Angaben des Eintragskopfs; der Inhalt bleibt verschlüsselt.	Eintrag bis drei Jahre nach Löschung der Organisation. Inhalt unlesbar, sobald der Fall gelöscht ist.

Ereignis	Erfasste Angaben	Wer sieht es	Aufbewahrung
Bestandteile eines Falls anlegen, ändern, löschen: Parteien, Titel, Forderungskonto (Buchungen), Zinsen laut Titel, Ereignisse zur Verjährung, Wiedervorlagen, Eingänge, Suchen in den Insolvenzbekanntmachungen	Geänderte Felder mit altem und neuem Wert. Bei Eingängen ohne Speicherort und Prüfwert der Datei. Erledigt die Software eine Wiedervorlage selbst, etwa nach Erfassen einer Drittschuldnererklärung, entsteht dafür kein eigener Eintrag.	wie beim Fall	wie beim Fall
Formular-Entwurf erstellen oder verwerfen	Formularart, Stichtag, Status, Benutzer, der den Entwurf erstellt hat, Antworten auf die Vorab-Abfragen, Prüfwert des Datenschnappschusses. Beim Verwerfen Benutzer und Zeitpunkt.	wie beim Fall	wie beim Fall
Entwurf freigeben	Formularart, Benutzer, der den Entwurf erstellt hat, Prüfwerte von Daten und PDF, verwendete Formularfassungen, bestätigte Erklärungen mit Wortlaut (jede einzeln bestätigt; darin auch, wer den Antrag oder Auftrag unterzeichnet, mit Namen), Name und Eigenschaft der erklärenden Person (gesetzliche Vertretung, bevollmächtigte Beschäftigte, Gläubiger selbst), Kennzeichen für Testdokument und für Selbstfreigabe (nur Privatpersonen).	wie beim Fall	wie beim Fall
Freigegebenes PDF herunterladen	Prüfwert des PDF. Weist die Software ein PDF ab, weil der Fall nach der Freigabe geändert wurde oder die Datei nicht mehr zur Prüfsumme passt, entsteht ebenfalls ein Eintrag.	wie beim Fall	wie beim Fall
Übermittlungspaket für die elektronische Einreichung erstellen	Namen der Dateien im Paket, Prüfwert des PDF; gegebenenfalls der Name der Person, die die Erklärungen bestätigt hat.	wie beim Fall	wie beim Fall
Benutzerkonto anlegen oder ändern, Einladung versenden	Name, E-Mail-Adresse und Status des Kontos mit altem und neuem Wert. Passwort und Geheimnisse des zweiten Faktors nur als „geändert“. Bei der Einladung der Bereich der Software.	Inhaber, soweit der Eintrag Ihrer Organisation zugeordnet ist. Anbieterin: alle Angaben.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.
Mitgliedschaft in der Organisation anlegen, ändern, entfernen	Benutzer, Rolle und Status mit altem und neuem Wert.	Inhaber. Anbieterin: alle Angaben.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.
Zweiten Faktor einrichten oder entfernen, Wiederherstellungscodes neu erzeugen	Verfahren (Authenticator-App, Passkey oder Code per E-Mail), Bereich der Software, Zahl der Passkeys. Nie Codes oder Geheimnisse.	wie beim Benutzerkonto	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.

Ereignis	Erfasste Angaben	Wer sieht es	Aufbewahrung
Fälle importieren (nur Unternehmen)	Zahl der Zeilen in der Datei, der angelegten Fälle und der fehlerhaften Zeilen. Jeder angelegte Fall erzeugt zusätzlich die Einträge wie beim Anlegen eines Falls, mit dem Benutzer, der den Import ausgelöst hat.	Inhaber. Anbieterin: alle Angaben.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.
Zahlungseingänge aus dem Kontoauszug buchen	Zahl der gebuchten Zahlungen und der eingelesenen Gutschriften. Jede gebuchte Zahlung erzeugt zusätzlich einen Eintrag wie beim Anlegen einer Buchung im Forderungskonto.	Inhaber. Anbieterin: alle Angaben.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.
Schlüssel der Programmschnittstelle anlegen oder widerrufen (nur Unternehmen)	Bezeichnung und Anfang des Schlüssels (die ersten elf Zeichen), beim Anlegen auch Rechte und Ablaufdatum; nie der vollständige Schlüssel. Benutzer ist die Person, die den Schlüssel anlegt oder widerruft. Ändern lässt sich ein Schlüssel nicht.	Inhaber. Anbieterin: alle Angaben.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.
Fall anlegen oder Zahlungseingang buchen über die Programmschnittstelle	Anfang des verwendeten Schlüssels. Als Benutzer steht die Person im Eintrag, die den Schlüssel angelegt hat. Zusätzlich entstehen die Einträge wie beim Anlegen eines Falls und seiner Bestandteile oder einer Buchung; darin ist die Nummer des Benutzerkontos leer, weil über die Schnittstelle niemand angemeldet ist.	wie beim Fall	wie beim Fall
Empfangsadresse für Benachrichtigungen (Webhooks) anlegen, löschen, abschalten oder wieder einschalten (nur Unternehmen)	Nummer der Empfangsadresse; beim Anlegen Adresse und gewählte Ereignisse, beim Löschen die Adresse, beim Abschalten der Grund. Nie der Signaturschlüssel. Ereignisse im Protokoll: webhook_angelegt, webhook_geloescht, webhook_deaktiviert, webhook_aktiviert. Benutzer ist die Person, die die Adresse anlegt, löscht oder wieder einschaltet. Abgeschaltet wird automatisch nach 50 Fehlversuchen in Folge; dann ist die Nummer des Benutzerkontos leer. Testmeldungen und einzelne Meldungen erzeugen keinen Eintrag.	Inhaber. Anbieterin: alle Angaben.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.

Ereignis	Erfasste Angaben	Wer sieht es	Aufbewahrung
Anmeldung über das Unternehmenskonto (SSO) einrichten, ändern oder entfernen (nur Unternehmen)	Beim Speichern Aussteller, Client-ID, E-Mail-Domains, ob die Anmeldung eingeschaltet ist, ob nur noch über das Unternehmenskonto angemeldet werden kann und ob das Client-Geheimnis geändert wurde; beim Entfernen der Aussteller. Nie das Client-Geheimnis. Ereignisse im Protokoll: sso_konfiguration_gespeichert, sso_konfiguration_geloescht. Benutzer ist die Person mit der Rolle Inhaber, die speichert oder entfernt.	Inhaber. Anbieterin: alle Angaben.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.
Benutzerkonto mit dem Unternehmenskonto verknüpfen, Anmeldung über das Unternehmenskonto ablehnen (nur Unternehmen)	Beim Verknüpfen die Nummer des Benutzerkontos, nicht die Kennung beim Anbieter. Beim Ablehnen der Grund („kein Mitglied“) und die Domain der E-Mail-Adresse, nie die vollständige Adresse. Ereignisse im Protokoll: sso_verknuepft, sso_abgelehnt. Verknüpft wird bei der ersten Anmeldung über das Unternehmenskonto, sobald der Anbieter sie bestätigt hat, noch vor der Abfrage des zweiten Faktors; Benutzer ist die Person, deren Konto verknüpft wird. Abgelehnt wird, wenn zum Unternehmenskonto kein Benutzerkonto mit Zugang zur Organisation gehört; dabei ist meist niemand angemeldet und die Nummer des Benutzerkontos leer. Andere Fehlschläge, etwa ein Abbruch beim Anbieter oder eine nicht eingetragene Domain, erzeugen keinen Eintrag.	Inhaber. Anbieterin: alle Angaben.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.
Datenexport erstellen	Zahl der Fälle, Prüfwert der Exportdatei.	Inhaber. Anbieterin: alle Angaben.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.
CSV-Export unter „Berichte und Export“	Art des Exports (Forderungsstände, Zahlungen oder Kosten) und Zahl der Zeilen.	Inhaber. Anbieterin: alle Angaben.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.
Löschung nach Vertragsende aufschieben	Neuer Löschtage.	Inhaber. Anbieterin: alle Angaben.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.

Ereignis	Erfasste Angaben	Wer sieht es	Aufbewahrung
Tarif buchen, wechseln oder kündigen (Unternehmen)	Tarif, Zahlungsintervall und ob die Einrichtung gebucht wurde; beim Wechsel alter und neuer Tarif; die Kündigung. Außerdem Änderungen des Vertragsstatus nach dem Abgleich mit dem Zahlungsdienstleister und monatlich die Zahl der aktiven und der zusätzlich abgerechneten Titel.	Inhaber. Anbieterin: alle Angaben.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.
Organisation anlegen oder ändern	Geänderte Stammdaten mit altem und neuem Wert, zum Beispiel Name, Anschrift und Registerangaben.	Inhaber. Anbieterin: alle Angaben.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.
Maßnahmen der Anbieterin und zeitgesteuerte Abläufe	Konto sperren oder wieder freigeben, zweiten Faktor zurücksetzen, eine Formularfunktion sperren, Fallschlüssel vernichten, Hinweis vor der Löschung und Löschung von Konten ohne Bestellung, Löschung der Daten nach Ablauf des Exportzeitraums. Erfasst werden Art der Maßnahme, Grund oder Auslöser und die Zahl betroffener Fälle oder Benutzer.	Anbieterin: alle Angaben. Inhaber, soweit der Eintrag Ihrer Organisation zugeordnet ist.	Eintrag und Inhalt bis drei Jahre nach Löschung der Organisation.

Anmeldungen und Abmeldungen stehen nicht in diesem Protokoll, sondern im Sicherheitsprotokoll, auch Anmeldungen über das Unternehmenskonto. Hier steht dazu nur, wann ein Benutzerkonto erstmals mit einem Unternehmenskonto verknüpft oder eine Anmeldung mangels Zugang zur Organisation abgelehnt wurde.

Programmschnittstelle (API)

Über die Programmschnittstelle (API) für Unternehmen kann die IT eigene Systeme anbinden: Fälle abrufen und anlegen, Forderungsstände abfragen, Zahlungseingänge buchen. Entwürfe und Freigaben nur im Kundenbereich: Über die Schnittstelle entsteht kein Entwurf, und nichts wird freigegeben.

- Schlüssel legt nur die Rolle Inhaber an, je Organisation, mit Rechten (Fälle und Forderungsstände lesen, Fälle anlegen, Zahlungseingänge buchen) und einem Ablaufdatum von höchstens zwei Jahren. Ein Widerruf wirkt sofort. Gehört die Person, die den Schlüssel angelegt hat, der Organisation nicht mehr an, gilt er nicht mehr.
- Jeder Schlüssel ist der Person zugeordnet, die ihn angelegt hat. Die Einträge zur Fallanlage und Zahlungsbuchung über die Schnittstelle stehen deshalb unter ihrem Namen im Protokoll; die zusätzlichen Einträge zu Fall, Bestandteilen und Buchung haben keine Benutzernummer. Bei Fällen ist sie in den Falldaten auch als Person vermerkt, die den Fall angelegt hat. Die Pflichtbestätigungen zum Fall gibt erst eine Person in der Fallakte ab; sie stehen unter deren Namen im Protokoll. Wer die Anfrage im angebundenen System ausgelöst hat, geht daraus nicht hervor.
- Die Seite „Programmschnittstelle“ zeigt der Rolle Inhaber je Schlüssel Bezeichnung, Anfang, Rechte, Ablaufdatum, Zeitpunkt der letzten Nutzung und Widerruf, nicht aber die Person, die ihn angelegt hat. Einzelne Abrufe hält die Software nicht fest. Die Antworten der Schnittstelle enthalten keine Angaben zu den Personen, die in der Software arbeiten.

Benachrichtigungen an Ihre Systeme (Webhooks)

- Empfangsadressen richtet nur die Rolle Inhaber auf der Seite „Programmschnittstelle“ ein: höchstens fünf je Organisation, nur öffentliche https-Adressen. Bei den gewählten Ereignissen sendet die Software eine Meldung dorthin: Fall angelegt, Zahlungseingang gebucht, Entwurf freigegeben, Wiedervorlage fällig (einmal, am Fälligkeitstag); dazu auf Knopfdruck eine Testmeldung. Wiedervorlagen nach Ihren erfassten Daten – sie ersetzen nicht Ihre eigene Fristenkontrolle. Eine Meldung ist keine Maßnahme: Die Software löst damit nichts aus, wählt nichts und entscheidet nichts.
- Eine Meldung enthält ihre Kennung, das Ereignis, den Zeitpunkt, das Aktenzeichen und technische Kennungen: bei Zahlungen Nummer der Buchung, Datum und Betrag, bei Freigaben Nummer des Entwurfs und Formularart, bei Wiedervorlagen Nummer, Art und Fälligkeitstag. Angaben zu den Personen, die in der Software arbeiten, enthält sie nicht: Wer einen Fall angelegt, eine Zahlung gebucht oder einen Entwurf freigegeben hat, geht aus der Meldung nicht hervor. Namen und Anschriften von Schuldnern enthält sie ebenfalls nicht.
- Zu jeder Meldung führt die Software ein Zustellprotokoll mit Kennung, Ereignis, Inhalt, Zahl der Versuche, Zeitpunkten, letztem Status und letztem Fehler. Scheitert die Zustellung, folgen bis zu sechs Wiederholungen; nach 50 Fehlversuchen in Folge schaltet die Software die Adresse ab. Zustellprotokolle löscht die Software nach 30 Tagen, mit einer gelöschten Empfangsadresse sofort. Sie sind nicht Teil des Datenexports und stehen nicht im Protokoll.
- Die Seite „Programmschnittstelle“ zeigt der Rolle Inhaber je Adresse die Ereignisse, die letzte erfolgreiche Zustellung und die Zahl offener und aufgegebenen Meldungen oder Tag und Grund einer Abschaltung. Gespeichert ist auch die Person, die die Adresse angelegt hat; angezeigt wird sie nicht. Eine eigene Ansicht der Empfangsadressen und der Zustellprotokolle hat die Plattformverwaltung der Anbieterin nicht; die Adresse sieht sie nur in den Protokolleinträgen zum Anlegen und Löschen. Mit den Zugängen nach Vertragsende werden die Empfangsadressen gelöscht.

Anmeldung über das Unternehmenskonto (SSO)

Unternehmen können einrichten, dass sich ihre Beschäftigten statt mit dem Passwort über einen eigenen Identitätsanbieter anmelden, der OpenID Connect unterstützt (Single Sign-on, SSO). Das Unternehmenskonto ersetzt nur das Passwort; den zweiten Faktor von einfach vollstrecken fragt die Software danach weiterhin ab.

- Die Anwendung beim Identitätsanbieter richtet die IT des Unternehmens ein. In der Software trägt nur die Rolle Inhaber auf der Seite „Anmeldung über Unternehmenskonto (SSO)“ Aussteller, Client-ID, Client-Geheimnis und E-Mail-Domains ein, schaltet die Anmeldung ein und wählt, ob die Passwort-Anmeldung gesperrt ist. Gesperrt ist sie dann für Mitglieder, die nur Organisationen mit dieser Einstellung angehören; wer in einer davon die Rolle Inhaber hat, behält sie als Notzugang. Gespeichert ist auch die Person, die die Einstellungen zuletzt geändert hat; angezeigt wird sie nicht.
- Anmelden kann sich nur, wer bereits Mitglied der Organisation ist; Konten legt die Software dabei nicht an. Beim ersten Mal ordnet sie das Unternehmenskonto über die E-Mail-Adresse zu, danach über die Kennung beim Anbieter (sub).
- Vom Identitätsanbieter erhält die Software eine Anmeldebestätigung mit der Kennung (sub), der E-Mail-Adresse oder dem Benutzernamen und je nach Einstellung des Anbieters weiteren Profilangaben wie dem Namen. Gespeichert wird davon nur die Kennung, in einer Verknüpfung mit Organisation, Benutzerkonto, Aussteller und dem Zeitpunkt, zu dem der Anbieter die Anmeldung zuletzt bestätigt hat. Jede weitere Bestätigung überschreibt diesen Zeitpunkt.

- Die Verknüpfungen zeigt die Software weder im Kundenbereich noch in der Plattformverwaltung an; sie sind nicht Teil des Datenexports. Gelöscht werden sie mit dem Benutzerkonto, spätestens mit den Zugängen der Organisation nach Vertragsende.
- Im Protokoll stehen nur die Einstellungen, die erste Verknüpfung und Ablehnungen (siehe Tabelle „Ereignisse im Protokoll“). Weitere Anmeldungen über das Unternehmenskonto stehen wie jede Anmeldung nur im Sicherheitsprotokoll.

Verschlüsselung und Löschung

Einträge, die zu einem Fall gehören, speichern ihren Inhalt verschlüsselt. Jeder Fall erhält einen eigenen, zufällig erzeugten Schlüssel mit 256 Bit. Verschlüsselt wird mit dem Verfahren AES-256-GCM. Die Nummer des Falls ist in die Verschlüsselung eingebunden. Ein verschlüsselter Inhalt lässt sich deshalb keinem anderen Fall unterschieben. Die Fallschlüssel liegen ihrerseits mit dem Hauptschlüssel der Anwendung verschlüsselt in der Datenbank.

Löschung durch Vernichtung des Schlüssels

- Wird ein Fall gelöscht, vernichtet die Software seinen Schlüssel. Die Einträge bleiben stehen, ihr Inhalt ist nicht mehr lesbar. Das Löschen und die Vernichtung des Schlüssels stehen selbst als Einträge im Protokoll; der Vermerk über die Vernichtung enthält keinen Fallinhalt.
- Wird eine Organisation gelöscht, vernichtet die Software die Schlüssel aller ihrer Fälle.
- Im laufenden Betrieb lassen sich Fälle mit freigegebenen Formularen nicht löschen. Sie bleiben als Nachweis erhalten, bis die Daten der Organisation gelöscht werden: nach Vertragsende und Ablauf des Exportzeitraums oder – bei einem Konto, für das nie ein Paket oder Tarif gebucht wurde – 6 Monate nach dem Anlegen. Mit der Löschung werden auch ihre Schlüssel vernichtet.
- In Datensicherungen kann ein vernichteter Schlüssel noch enthalten sein, bis die Sicherung gelöscht wird. Datensicherungen bewahrt die Anbieterin höchstens 30 Tage auf.
- Die Angaben des Eintragskopfs sind nicht verschlüsselt und bleiben lesbar: Zeitpunkt, Nummer des Benutzerkontos, Organisation, Nummer des Falls, Ereignis und Datensatz.

Einträge ohne Fallbezug

- Einträge zu Benutzerkonten, Mitgliedschaften und Rollen, zur Organisation, zum zweiten Faktor, zum Datenexport, zu CSV-Exporten, zu Importen, zu Schlüsseln der Programmschnittstelle, zu Empfangsadressen für Benachrichtigungen, zur Anmeldung über das Unternehmenskonto und zum Tarif sind nicht je Fall verschlüsselt.
- Protokolleinträge einer gelöschten Organisation entfernt die Software drei Jahre nach der Löschung; andere Protokolleinträge löscht sie nicht. Die Manipulationssicherung des Protokolls bleibt dabei erhalten (siehe „Schutz vor Manipulation“).
- Entfernt der Inhaber eine Person aus der Organisation, bleibt ihr Benutzerkonto bestehen. Die Einträge zu ihren Handlungen bleiben ebenfalls im Protokoll.
- Werden die Daten der Organisation nach Vertragsende gelöscht, werden auch Benutzerkonten ohne weitere Mitgliedschaft gelöscht. Die Einträge bleiben mit der Nummer des Benutzerkontos im Protokoll, bis sie drei Jahre nach der Löschung entfernt werden.

Schutz vor Manipulation

- Einträge werden nur angefügt. Ändern sperrt die Software selbst und zusätzlich die Datenbank. Löschen lässt die Datenbank nur zu, wenn für den Eintrag zuvor ein Vermerk mit seiner laufenden Nummer und seinen Prüfsummen angelegt wurde – das geschieht nur bei der Entfernung drei Jahre nach Löschung einer Organisation. Auch dieser Vermerk trägt eine Prüfsumme mit dem geheimen Schlüssel.
- Jeder Eintrag trägt eine Prüfsumme (HMAC-SHA256) über seinen Inhalt und die Prüfsumme des vorherigen Eintrags. So entsteht eine Kette. Wird ein Eintrag verändert, entfernt oder eingeschoben, passt die Kette nicht mehr. Für fristgerecht entfernte Einträge prüft die Software die Kette über den Vermerk weiter.
- Für die Prüfsumme nutzt die Software einen eigenen geheimen Schlüssel. Wer nur Zugriff auf die Datenbank hat, kann veränderte Einträge deshalb nicht mit passenden Prüfsummen versehen.
- Die laufende Nummer macht Lücken sichtbar. Ein gesonderter Kettenkopf speichert die letzte Nummer und die letzte Prüfsumme. So fällt auch das Entfernen der jüngsten Einträge auf.
- Die Software prüft die ganze Kette täglich. Die Anbieterin kann die Prüfung in ihrer Plattformverwaltung zusätzlich jederzeit auslösen.
- Die Prüfsumme läuft über den verschlüsselten Inhalt. Nach der Vernichtung eines Fallschlüssels lässt sich die Kette deshalb weiter prüfen.

Sicherheitsprotokoll

Das Sicherheitsprotokoll führt die Anbieterin getrennt vom Protokoll Ihrer Organisation. Zweck ist die Erkennung von Angriffen und Missbrauch. Es enthält keine Fallinhalte, keine Passwörter und keine Codes.

Ereignisse im Sicherheitsprotokoll

Ereignis	Erfasste Angaben
Anmeldung, Abmeldung	Benutzer, technische Kennung des Zugangs (für alle Anmeldungen dieselbe, auch über das Unternehmenskonto)
Fehlgeschlagene Anmeldung	Benutzer, wenn die eingegebene E-Mail-Adresse zu einem Konto gehört. Sonst nur der Teil der E-Mail-Adresse nach dem @-Zeichen, nie die vollständige Adresse.
Sperre nach zu vielen Fehlversuchen	nur der Teil der eingegebenen E-Mail-Adresse nach dem @-Zeichen
Zweiter Faktor fehlgeschlagen	Benutzer, Verfahren, Bereich der Software, Vorgang (Anmeldung oder Einrichtung), ob ein Wiederherstellungscode eingegeben wurde
Wiederherstellungscode genutzt	Benutzer, Zahl der verbleibenden Codes

- Zu jedem Eintrag speichert die Software den Zeitpunkt und die gekürzte IP-Adresse, gekürzt wie im Protokoll Ihrer Organisation.
- Anmeldungen über das Unternehmenskonto stehen hier wie Anmeldungen mit Passwort; der Eintrag unterscheidet die beiden Wege nicht. Fehlschläge beim Unternehmenskonto, etwa ein Abbruch beim Anbieter, stehen nicht im Sicherheitsprotokoll, ein danach fehlgeschlagener zweiter Faktor schon.
- Aufbewahrung: 90 Tage. Ältere Einträge löscht die Software täglich.
- Einsicht: Die Software hat keine Ansicht des Sicherheitsprotokolls, weder im Kundenbereich noch in der Plattformverwaltung. Es ist nicht Teil des Datenexports.

Zusätzlich speichert das Benutzerkonto den Zeitpunkt der letzten Anmeldung. Jede Anmeldung überschreibt ihn. Die Anbieterin sieht ihn in der Benutzerliste ihrer Plattformverwaltung. Im Kundenbereich wird er nicht angezeigt.

Zugriff durch die Anbieterin

Die Anbieterin betreibt die Software. Mitarbeitende der Anbieterin mit Zugang zur Plattformverwaltung sehen:

- die Protokolleinträge aller Organisationen in Liste und Einzelansicht mit laufender Nummer, Zeitpunkt, Ereignis, E-Mail-Adresse des Benutzers, Organisation, Datensatz, Nummer des Falls und gekürzter IP-Adresse. Die Liste lässt sich nach E-Mail-Adresse durchsuchen und nach Ereignis und Organisation filtern.
- die Inhalte von Einträgen ohne Fallbezug, zum Beispiel einen Rollenwechsel.
- die Benutzerliste mit Name, E-Mail-Adresse, Organisationen, Status, eingerichtetem zweitem Faktor und letzter Anmeldung.

Fallbezogene Inhalte zeigt die Plattformverwaltung nicht an. Dort steht nur der Hinweis, dass der Inhalt verschlüsselt ist. Auf Fallakten gibt es in der Plattformverwaltung keinen Zugriff. Auch in der Plattformverwaltung lassen sich Protokolleinträge weder ändern noch löschen.

Zum Stand dieser Beschreibung gibt es keinen Supportzugriff auf Falldaten.

Auswertungen über einzelne Beschäftigte

Die Software enthält keine Berichte, Kennzahlen oder Ranglisten zu einzelnen Nutzerinnen und Nutzern. Die Übersicht „Ihre Forderungen“ zählt und summiert nur Fälle, Beträge, Drittschuldnererklärungen und Wiedervorlagen der ganzen Organisation. Die Seite „Berichte und Export“ zeigt Monatswerte der ganzen Organisation für die letzten zwölf Monate (Zahlungseingänge, neue Fälle, Entwürfe, Freigaben) und liefert CSV-Dateien mit den Forderungsständen je Fall und den Zahlungen und Kosten im gewählten Zeitraum. Beides enthält keine Angaben zu den Personen, die in der Software arbeiten. Die Seite steht allen Rollen offen, die Fälle ansehen dürfen.

Angaben zu einzelnen Personen erscheinen an diesen Stellen:

- In der Fallakte zeigt die Liste der Formular-Entwürfe, wer einen Entwurf erstellt und wer ihn freigegeben hat, jeweils mit Datum und Uhrzeit. Diese Liste sehen alle Rollen, die den Fall ansehen dürfen.
- Die Benutzerverwaltung zeigt der Rolle Inhaber Name, E-Mail-Adresse, Rolle und Status jeder Person und ob ein zweiter Faktor eingerichtet ist.
- Der Datenexport der Rolle Inhaber enthält den Auszug des Protokolls. In den Falldaten stehen dort zudem die Nummern der Benutzerkonten, die einen Fall angelegt, Angaben bestätigt, Entwürfe erstellt, freigegeben oder verworfen, Eingänge erfasst, Suchen in den Insolvenzbekanntmachungen dokumentiert oder Wiedervorlagen erledigt haben.
- Der Datenexport ist ein ZIP-Archiv mit maschinenlesbaren Dateien (JSON). Eine Auswertung außerhalb der Software ist damit technisch möglich.
- Die Plattformverwaltung der Anbieterin zeigt Angaben wie im vorigen Abschnitt beschrieben.

Hinweis

Bitte stimmen Sie die Einführung mit Ihrem Betriebs- oder Personalrat ab. Dieses Dokument beschreibt Funktionen der Software. Es ist keine Rechtsberatung.

Quellen und Stand

- § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG), Mitbestimmungsrechte, in der Fassung der Bekanntmachung vom 25.09.2001 (BGBl. I S. 2518) mit späteren Änderungen:
gesetze-im-internet.de/betrvg/_87.html
- Angaben zur Software: Kundenbereich mit Anmeldung über das Unternehmenskonto (SSO), Programmschnittstelle mit Benachrichtigungen (Webhooks) und Plattformverwaltung von einfach vollstrecken, Softwarestand vom 16.10.2026

Stand: 16.10.2026

Software, keine Rechtsberatung. Diese Funktionsbeschreibung ersetzt keine rechtliche Beratung zur Mitbestimmung.

Kontaktformular: einfach-vollstrecken.de/kontakt

E-Mail: kontakt@einfach-vollstrecken.de

einfach vollstrecken ist ein Angebot der Einfach Elterngeld GmbH, Pennricher Straße 31, 01157 Dresden.