

VENDOCERTA-MATERIALIEN

Sicherheit & RODO

Der Datenschutz in VendoCerta ist über das gesamte Produkt verteilt: wie die Historie geschrieben wird, wer welches Dokument sehen darf, wie die Bankverbindung verschlüsselt wird, und was eine Rolle absichtlich nicht darf. Diese Übersicht fasst es an einem Ort zusammen.

5

Rollen mit
Aufgabentrennung

5

Regeln, die keine Rolle
umgeht

AES-256

Verschlüsselung
sensibler Daten

Sechs Fragen, die zuerst kommen.

Können die Daten bei uns bleiben?

Ja. VendoCerta wird auf einer Infrastruktur installiert, die Sie kontrollieren.

Wie werden sensible Daten geschützt?

AES-256-GCM im Ruhezustand; das Aufdecken erfordert eine erneute Passworteingabe und einen in der Historie gespeicherten Grund.

Wer hat Zugriff auf was?

Rollen mit echter Aufgabentrennung. Niemand ändert die eigene Rolle.

Gibt es einen zweiten Faktor bei der Anmeldung?

Ja, verpflichtend für Rollen mit Zugriff auf Geschäftsdaten.

Kann eine Person allein die Bankverbindung eines Lieferanten ändern?

Nein. Vier Stufen, getrennte Rollen, mindestens zwei Personen.

Lässt sich die Audit-Historie nachträglich ändern?

Nein. Keine Bearbeitungs- oder Löschfunktion in der Oberfläche, in keiner Rolle, auch nicht für den Eigentümer.

Ein Eintrag lässt sich weder ändern noch löschen. Auch nicht vom Eigentümer.

Jede gespeicherte Aktion wird zu einem Eintrag: Anmeldung, Statusänderung eines Lieferanten, Dokumentenentscheidung, gesendete Einladung, heruntergeladene Datei. VendoCerta hat nirgendwo eine Funktion zum Bearbeiten oder Löschen eines Eintrags und überschreibt nie ein bestehendes Ereignis.

Vorher und nachher, bei jeder Datenänderung

Jeder Eintrag trägt: wer, was, wann — und bei einer Änderung auch, wie die Werte auf beiden Seiten aussahen.

Auch Ablehnungen werden gespeichert

Versucht jemand, etwas ohne Berechtigung zu öffnen, ist dieser Versuch ein Eintrag. Wiederholte Versuche sind damit sichtbar, nicht still.

Eine gefilterte Ansicht ist ein Link

Filter landen in der Seitenadresse, sodass ein bestimmter Ausschnitt der Historie als Adresse an einen Kollegen — oder Prüfer — weitergegeben werden kann.

Eigene Aufbewahrungsfrist — und wir sagen das offen

Die Anzahl der Tage unten am Bildschirm der Audit-Historie ist nicht dasselbe Feld wie im Einstellungsbildschirm. Die Aufbewahrungsfrist der Audit-Historie ist eine eigene Einstellung, die derzeit nicht über die Oberfläche geändert werden kann, und eine Änderung des anderen Feldes wirkt sich nicht darauf aus.

Die einzige Operation, deren Erleichterung das Produkt verweigert.

Die Änderung der Lieferanten-Bankverbindung besteht aus vier Stufen und einer Regel, wer sie abschließen darf. Alles andere in VendoCerta ist darauf ausgelegt, Reibung zu entfernen; dies ist darauf ausgelegt, sie zu erhalten.

Verschlüsselt ab dem Moment der Speicherung

Die Kontonummer liegt nie als Klartext in der Datenbank — AES-256-GCM im Ruhezustand, ab dem Moment der Speicherung.

Das Aufdecken kostet drei Dinge

Die Berechtigung für sensible Daten, die erneute Passwordeingabe trotz Anmeldung und die Angabe eines Grundes, der in der Historie landet. Der Grund wird gespeichert; die Nummer nie. Die Nummer verschwindet nach 45 Sekunden vom Bildschirm.

Duplikate werden angezeigt, nicht versteckt

Steht dieselbe Kontonummer bereits bei einem anderen Lieferanten, muss die Warnung bewusst verworfen werden, bevor eine Freigabe überhaupt möglich wird.

Fünf Rollen, und die überraschende ist Absicht.

Der Systemadministrator hält die Installation gesund — Konfiguration, Diagnose, Sicherungen — und hat keinerlei Einblick in Lieferanten, Dokumente, Vorgänge oder Bankverbindungen. Genau das Gegenteil des Geschäftsadministrators, der die Lieferantenseite führt und keine Sicherung wiederherstellen kann.

BERECHTIGUNG	EIGENTÜMER	GESCHÄFTSADMINISTRATOR	SYSTEMADMINISTRATOR	PRÜFER	BEOBACHTER
Sieht Lieferanten und Dokumente	✓	✓	—	✓	✓
Fügt Lieferanten hinzu und bearbeitet sie	✓	✓	—	—	—
Prüft Dokumente und entscheidet über die Freigabe	✓	✓	—	✓	—
Sieht sensible Dokumente (Zahlungsdaten)	✓	✓	—	—	—
Verwaltet Benutzer und Rollen	✓	✓	✓	—	—
Stellt eine Sicherung wieder her	✓	—	—	—	—

Regeln, die keine Rolle umgehen kann

- Niemand — auch nicht der Eigentümer — kann die eigene Rolle ändern.
- Ein Administrator kann kein Konto mit der Rolle Eigentümer erstellen oder herabstufen.
- Das letzte Eigentümerkonto lässt sich weder herabstufen noch deaktivieren, sodass das Unternehmen nie ohne jemanden mit vollen Rechten dasteht.
- Zwei-Faktor-Authentifizierung ist verpflichtend und nicht überspringbar für Eigentümer, Geschäftsadministrator, Systemadministrator und Prüfer. Der Beobachter kann sie aktivieren, muss aber nicht.
- Eine fehlgeschlagene Anmeldung verrät nie, ob die Adresse oder das Passwort falsch war, sodass der Bildschirm nicht genutzt werden kann, um zu prüfen, ob ein Konto existiert.

Was gespeichert wird, wer darauf zugreifen kann und wie lange.

Sensible Dokumente erfordern eine eigene Berechtigung

Gewöhnliche Lieferantendokumente sieht jeder mit Zugriff auf die Karte. Als sensibel markierte Dokumente — meist mit Zahlungsbezug — erfordern eine zusätzliche Berechtigung, in der Praxis nur Eigentümer und Administrator. Ein Versuch ohne diese endet mit einer Ablehnung, und die Ablehnung wird gespeichert.

Dateien haben nie eine feste Adresse

Der Download läuft über einen digital signierten Link, der wenige Minuten gültig und an Ihr Unternehmen gebunden ist. Ihn aus einem anderen Kontext zu öffnen, bringt nichts. Jeder Download einer sensiblen Datei wird gesondert protokolliert.

Aufbewahrung: standardmäßig sieben Jahre

Die Einstellung für Dokumente und Aufbewahrung steht standardmäßig auf 2555 Tage, entsprechend typischer Einkaufsprüfungsanforderungen, und kann jederzeit geändert werden. Ehrlich gesagt: Sie speichert heute Ihre Richtlinie und wird künftige Bereinigungen antreiben — nichts wird automatisch gelöscht, nur weil eine Frist abgelaufen ist.

Einladungen laufen ab, ein erneutes Senden macht sie ungültig

Der Einladungslink ist ein zufälliges Token mit begrenzter Gültigkeit, standardmäßig eine Woche — bewusst nicht einmalig, damit ein Lieferant zu einem unvollständigen Formular über denselben Link zurückkehren kann. Eine neue Einladung macht die vorherige sofort ungültig, selbst wenn sie schon geöffnet wurde — derzeit die einzige Möglichkeit, einen Link zu sperren; es gibt keinen separaten Widerrufsbutton.

Bankdaten im Ruhezustand verschlüsselt

AES-256-GCM ab dem Moment der Speicherung. Der angegebene Grund für das Aufdecken der Nummer landet in der Audit-Historie; die Nummer selbst nie.

Support-Bericht ohne Daten

Der Diagnose-Tab im Systemzentrum erstellt einen Bericht für den technischen Support mit Versionen, Zählern und maskierten Log-Zeilen — nie Dokumenteninhalte, Bankdaten oder personenbezogene Lieferantendaten.

Fragen, die ein Prüfer als Erstes stellt.

Ist VendoCerta ein Cloud-Dienst, dem wir Daten anvertrauen?

Nein. Die Installation erfolgt auf einer Maschine, die Sie kontrollieren. PostgreSQL, Dateispeicher und Mail-Vorschau laufen als portable Binärdateien innerhalb des Projektordners — nichts wird unter Windows installiert, ohne Administratorrechte, Docker optional. Internet wird beim ersten Start benötigt, um diese Dienste herunterzuladen; danach gehört die Installation Ihnen.

Erhalten wir technische Dokumentation über diese Seite hinaus?

Ja. Die Installation enthält ein Sicherheitsmodell und ein Bedrohungsmodell als Dokumente im Repository — dieselben Quellen, aus denen diese Seite entstand. Fragen Sie die Person, die Ihre Installation betreut, oder uns über das Demo-Formular, mit dem Hinweis, dass es für eine Sicherheitsprüfung ist.

Worauf hat der KI-Assistent Zugriff?

Nur auf das, was die fragende Person ohnehin sehen darf, und er führt nie eine Aktion ohne deren ausdrückliche Bestätigung aus — die Berechtigungen werden im Moment des Klicks erneut gegen die klickende Person geprüft. Er kann keinen Lieferanten freigeben, ablehnen oder sperren, keine Rolle ändern und nichts löschen.

Umgeht ein Passwort-Reset die Zwei-Faktor-Authentifizierung?

Nein. Für Rollen, bei denen der zweite Faktor verpflichtend ist, gilt das auf jedem Weg zum Konto, auch nach einem Reset.

Wohin gehen E-Mails während der Pilotphase?

An eine lokale Vorschau-Mailbox auf der Installation selbst, nicht an echte Empfänger — sodass der Pilot nicht versehentlich einem Lieferanten schreiben kann. Der Installations-Tab im Systemzentrum zeigt an, welche Mailbox eine bestimmte Installation tatsächlich verwendet.