OPEXGUARD

Sicherheit, Nachvollziehbarkeit und Betrieb der OpexGuard-Plattform

Was gilt, wie wir es sicherstellen und wie Sie es prüfen können.

OpexGuard GbR · Stand 24.09.2026 · info@opexguard.de
Jede Aussage in diesem Dokument ist gegen den Quellcode und die Infrastruktur der Plattform geprüft.

Inhalt

Wer es genauer wissen will – Hash-Kette, WORM, Umschlagverschlüsselung, Row-Level Security, Sicherung, Standorte –, findet die technische Dokumentation unter **www.opexguard.de/technik**.

Jedes Kapitel folgt demselben Dreischritt: **Was gilt** – ein Fakt. **Wie wir das sicherstellen** – der Mechanismus. **Wie Sie es prüfen** – der Weg, es nachzuvollziehen. Was erst mit dem Produktivstart dazukommt, steht am Ende des Kapitels unter „Nächste Schritte“.

KAPITEL 1

Jede Änderung hat einen Namen, eine Uhrzeit und ein Vorher und Nachher.

Wenn ein Vorgang vor einem Prüfer, einem Carrier oder einem Gericht landet, zählt nicht, was im System steht, sondern ob sich belegen lässt, wie es dorthin kam. Deshalb protokolliert die Plattform jede Änderung – und die Protokolle prüfen sich selbst.

Das Protokoll

WAS GILT

Jede Änderung an Sendungen, Vorgängen, Dokumenten, Claims und Stammdaten wird festgehalten: welches Objekt, welche Aktion, welcher Nutzer in welcher Rolle, wann – und der alte und der neue Wert jedes geänderten Feldes.

WIE WIR DAS SICHERSTELLEN

Das Protokoll entsteht nicht in der Oberfläche, sondern beim Speichern in der Datenbank. Es gibt keinen Weg, eine Änderung an ihm vorbei zu schreiben – auch nicht für uns. Jeder Eintrag trägt eine Korrelationsnummer, mit der sich zusammengehörige Änderungen einer Aktion wiederfinden lassen.

WIE SIE ES PRÜFEN

In der Plattform sehen Sie den Verlauf jeder Sendung, jedes Vorgangs und jedes Dokuments; das vollständige Protokoll Ihres Mandanten liefert die Schnittstelle. Den Export als JSON lösen Ihre Administratoren selbst aus – ohne Umweg über uns.

Die Kette

Ein Protokoll, das sich nachträglich ändern ließe, wäre keines. Deshalb hängt jeder Eintrag am vorherigen.

WAS GILT

Jeder Eintrag trägt einen Hash (SHA-256), der den Inhalt des Eintrags und den Hash des vorherigen Eintrags einschließt – je Mandant eine eigene Kette. Wird ein Eintrag verändert oder entfernt, passt die Kette an dieser Stelle nicht mehr.

WIE WIR DAS SICHERSTELLEN

Der Hash entsteht im selben Schritt wie der Eintrag selbst, beim Speichern in der Datenbank. Auch archivierte Einträge behalten ihre Hashes; der jüngste Eintrag in der Datenbank zeigt auf den letzten im Archiv.

WIE SIE ES PRÜFEN

Der Export Ihres Protokolls enthält zu jedem Eintrag seinen Hash und den seines Vorgängers.

Die Prüfung

Eine Kette nützt nur, wenn jemand sie nachrechnet. Das tut die Plattform jede Nacht – und Sie können es selbst tun.

WAS GILT

Eine Integritätsprüfung rechnet die Kette nach und benennt jedes gebrochene Glied. Sie läuft jede Nacht automatisch, das Ergebnis wird gespeichert, und bei einem Bruch werden wir alarmiert.

WIE WIR DAS SICHERSTELLEN

Die Prüfung endet nicht an der Archivgrenze: Vor dem Archivieren wird die Kette geprüft, bei Bedarf das Archiv mitgelesen und die Prüfsumme der Woche nachgerechnet. Geprüft wird je Mandant – Ihre Kette, nicht eine Stichprobe über alle.

WIE SIE ES PRÜFEN

Sie können die Kette selbst nachrechnen: Der Export trägt je Zeile die Hashes und die Version des Kettenverfahrens. Prüfung und Export lösen Ihre Administratoren in der Plattform selbst aus.

Was nicht im Protokoll steht

- **Zugangsgeheimnisse.** API-Schlüssel, Einladungscodes und Carrier-Zugangsdaten tauchen nie im Protokoll auf – auch nicht als Hash. Sie werden ausgelassen, nicht maskiert.
- **Rauschen.** Technische Zeitstempel und Suchindizes ändern sich bei fast jedem Speichern und beweisen nichts; sie würden die eigentliche Änderung zudecken.
- **Tracking-Ereignisse und Verbrauchszähler.** Sie sind eigene, nur anfügende Ströme. Das Änderungsprotokoll beweist Änderungen – es zählt nicht.
- **Fremde Mandanten.** Das Protokoll ist wie alle Daten auf Datenbankebene getrennt: Ihr Mandant sieht nur seine eigenen Einträge.

Aufbewahrung

WAS GILT

Einträge bleiben 90 Tage in der Datenbank. Danach verschiebt sie ein nächtlicher Lauf – je Mandant und Tag – in einen eigenen, getrennten Archivspeicher; wöchentlich wird dort eine Prüfsumme über die Woche abgelegt. Adressen von Absendern und Empfängern stehen im Archiv nur als Prüfsumme, im Klartext allein in den 90 Tagen in der Datenbank – damit das unveränderliche Archiv zur Anonymisierung nach 180 Tagen passt.

WIE WIR DAS SICHERSTELLEN

Der Lauf lädt hoch, liest das Hochgeladene zurück und löscht erst dann in der Datenbank – ein Archiv wird nie mit einer unvollständigen Fassung überschrieben. Der Archivspeicher liegt in der EU, ist geografisch redundant gespeichert und nur über Identitäten erreichbar; es gibt keinen Kontoschlüssel, den man kopieren könnte.

WIE SIE ES PRÜFEN

Der Export umfasst Datenbank und Archiv – archivierte Einträge Ihres Mandanten sind darin enthalten.

KAPITEL 2

Ein Beleg wird erst dann zum Beweis, wenn seine Herkunft feststeht.

Ein PDF in einem Ordner beweist wenig. Es zählt, woher es kam, wann, zu welcher Sendung es gehört – und dass es seitdem unverändert ist. Genau das hält die Plattform zu jeder Datei fest und packt es auf Knopfdruck zusammen.

Herkunft und Weg

WAS GILT

Zu jedem Dokument steht fest, woher es stammt – Abruf beim Carrier, Upload durch einen Menschen oder Anhang einer E-Mail –, ob es automatisch oder von Hand beschafft wurde, von wem, wann, und zu welcher Sendung es gehört.

WIE WIR DAS SICHERSTELLEN

Diese Angaben entstehen beim Ablegen, nicht später von Hand. Der Upload eines Ablieferbelegs setzt zugleich den Beleg-Status der Sendung: Beleg und Sachstand können nicht auseinanderlaufen.

WIE SIE ES PRÜFEN

In der Sendungsansicht steht zu jeder Datei Herkunft, Kanal, Zeitpunkt und Person – ohne Nachfrage bei uns.

Die Prüfsumme

WAS GILT

Jede Datei trägt die Prüfsumme (SHA-256) ihres Originals – je Version, in der Anwendung sichtbar und kopierbar.

WIE WIR DAS SICHERSTELLEN

Die Prüfsumme wird beim Hochladen über die Datei gerechnet, wie sie ankommt. Was Sie herunterladen, ist byteidentisch zu dem, was hochgeladen wurde – das ist gemessen, nicht angenommen.

WIE SIE ES PRÜFEN

Laden Sie den Beleg herunter und bilden Sie die Prüfsumme mit einem Standardwerkzeug selbst. Stimmt sie mit der angezeigten überein, ist das Original unverändert.

Versionen statt Überschreiben

WAS GILT

Ein Dokument wird nicht ersetzt, sondern bekommt eine neue Version; ältere Stände bleiben abrufbar. Löschen gibt es nicht – ein Dokument lässt sich archivieren, die Datei bleibt.

WIE WIR DAS SICHERSTELLEN

Jede Version trägt ihre eigene Prüfsumme und ihren eigenen Eintrag im Änderungsprotokoll. Wer wann welche Fassung abgelegt hat, steht damit fest.

WIE SIE ES PRÜFEN

Der Verlauf am Dokument zeigt jede Version mit Zeitpunkt und Person; jede Version lässt sich einzeln herunterladen.

Aufbewahrungsfristen

WAS GILT

Die Plattform setzt die Aufbewahrungsfrist beim Hochladen anhand der Dokumentart und überwacht sie. Bis zum Ablauf wird das Dokument nicht endgültig gelöscht; archivieren – also aus den Arbeitslisten nehmen – bleibt möglich, die Datei bleibt abrufbar.

WIE WIR DAS SICHERSTELLEN

Welche Frist gilt, entscheidet die Funktion des Dokuments, nicht sein Name – dasselbe Dokument kann je nach Verwendung unter eine andere Frist fallen. Typisch sind in Deutschland zehn Jahre für zollrelevante Unterlagen und bestimmte Bücher, acht Jahre für Rechnungen und Buchungsbelege, sechs Jahre für Handels- und Geschäftsbriefe; für Lieferscheine, Ablieferbelege und Versandlabels gibt es keine einheitliche Frist. Die Fristen beginnen erst mit Ablauf des jeweiligen Kalenderjahres, im Einzelfall laufen sie länger.

WIE SIE ES PRÜFEN

Am Dokument steht, bis wann es aufzubewahren ist. Ein archiviertes Dokument bleibt bis dahin abrufbar; endgültig entfernt wird es erst nach Fristende. Welche Frist zu welcher Dokumentart in Ihrem Haus passt, stimmen wir mit Ihnen ab.

Das Prüfpaket

Die Frage „Können Sie das für den Prüfer zusammenstellen?“ ist bei uns ein Klick, keine Aufgabe.

WAS GILT

Zu jeder Sendung erzeugt die Plattform ein Paket: die Sendung mit ihren Daten, der vollständige Verlauf, die zugehörigen Einträge aus dem Änderungsprotokoll, alle Dokumentversionen – und ein Manifest mit den Prüfsummen.

WIE WIR DAS SICHERSTELLEN

Das Paket entsteht im Moment der Anforderung aus den Originaldaten, nicht aus einer Zusammenfassung. Es ist ein gewöhnliches ZIP-Archiv und bleibt ohne OpexGuard lesbar.

WIE SIE ES PRÜFEN

Erzeugen Sie das Paket für eine beliebige Sendung und geben Sie es weiter – an Ihren Prüfer, Ihren Carrier oder Ihren Anwalt. Ihre Prüferrolle kann das selbst.

Nächste Schritte

- Unveränderlichkeit im Speicher (WORM) je Dokument – heute wirkt die Aufbewahrungsfrist in der Anwendung, nicht im Speicher: mit dem Produktivstart.

KAPITEL 3

Wo Ihre Daten liegen, wie sie geschützt sind – und warum wir es so gebaut haben.

Sicherheit ist bei uns keine Liste von Häkchen, sondern eine Reihe von Entscheidungen. Hier stehen sie – mit dem Grund, warum wir sie so getroffen haben, und dem Weg, wie Ihre IT sie nachprüfen kann.

Ein Ort

WAS GILT	WIE WIR DAS SICHERSTELLEN	WIE SIE ES PRÜFEN
Daten und Anwendung laufen auf Microsoft Azure in der Region Schweden-Mitte: Datenbank, Anwendung, Dokumentenspeicher und Archiv. Die Oberfläche selbst – statische Dateien ohne Kundendaten – liefert ein globales Content Delivery Network aus.	Die gesamte Umgebung ist als Code beschrieben und wird daraus aufgebaut – nicht von Hand. Die Region steht darin als Vorgabe für jede Komponente; ein Aufbau woanders wäre eine sichtbare Änderung im Code, kein Versehen. So bleibt die Antwort auf „Wo liegen meine Daten?“ ein Satz.	Auf Anfrage erhalten Sie die Liste der Azure-Dienste je Komponente mit Region – so, dass Ihr Datenschutzbeauftragter sie übernehmen kann.

Verschlüsselung und Schlüssel

WAS GILT	WIE WIR DAS SICHERSTELLEN	WIE SIE ES PRÜFEN
Gespeicherte Daten sind durch Azure verschlüsselt, die Übertragung erfolgt ausschließlich über HTTPS mit TLS 1.2 oder neuer. Zugangsdaten zu Carrier-Konten werden zusätzlich auf Anwendungsebene mit AES-256 verschlüsselt.	Der Schlüssel dafür liegt im Azure Key Vault, nie im Code und nie in einer Konfigurationsdatei. Die Anwendung greift über ihre eigene Identität darauf zu; es gibt kein Geheimnis, das jemand abschreiben könnte. Der Tresor ist gegen endgültiges Löschen geschützt. Ohne den Schlüssel sind die Carrier-Zugangsdaten auch für jemanden mit Datenbankzugriff wertlos.	Auf Anfrage zeigen wir den Aufbau: welche Identität welchen Schlüssel nutzen darf – und dass es keine zweite Kopie gibt.

Identität statt Passwörter

WAS GILT

Menschen melden sich über Microsoft Entra ID an, mit Multi-Faktor-Authentifizierung Ihres Unternehmens. Systeme nutzen API-Schlüssel, die je Kunde vergeben und jederzeit widerrufbar sind.

WIE WIR DAS SICHERSTELLEN

Wir speichern keine Passwörter – es gibt also keine zu verlieren. Ein API-Schlüssel wird beim Anlegen einmal angezeigt; bei uns liegt nur sein Hash (SHA-256). Anfragen je Schlüssel sind ratenbegrenzt, und Notfallzugänge werden bei Fehlversuchen gedrosselt.

WIE SIE ES PRÜFEN

Legen Sie in der Plattform einen Schlüssel an und widerrufen Sie ihn wieder – die Wirkung ist sofort, und beides steht im Protokoll.

Speicher ohne Kontoschlüssel

WAS GILT

Kein Speicherkonto der Plattform lässt sich mit einem Kontoschlüssel öffnen, und kein Blob ist öffentlich erreichbar.

WIE WIR DAS SICHERSTELLEN

Der Zugriff auf Dokumente und Archive läuft ausschließlich über die Identität der Anwendung mit genau der Rolle, die sie braucht. Ein Kontoschlüssel wäre ein einzelnes Geheimnis, das alles öffnet – deshalb ist er in der Infrastruktur abgeschaltet, nicht nur ungenutzt.

WIE SIE ES PRÜFEN

Auf Anfrage erhalten Sie den Auszug aus der Infrastruktur-Beschreibung, der genau das festlegt.

Sicherungen

WAS GILT	WIE WIR DAS SICHERSTELLEN	WIE SIE ES PRÜFEN
Die Datenbank wird täglich gesichert; Sicherungen werden 14 Tage aufbewahrt, und innerhalb dieser Frist lässt sich jeder Zeitpunkt wiederherstellen.	Die Sicherung ist Teil des verwalteten Datenbankdienstes von Azure und der Infrastruktur-Beschreibung – sie hängt nicht davon ab, dass jemand daran denkt. Dass sie trägt, wird geübt: Bei der letzten dokumentierten Übung am 22. September 2026 war die Anwendung nach der Wiederherstellung vollständig, mit allen Tabellen bis zum gewählten Zeitpunkt.	Auf Anfrage nennen wir Ihnen Aufbewahrung und Verfahren im Detail und zeigen das Protokoll der letzten Übung.

Wie Software zu uns in den Betrieb kommt

WAS GILT	WIE WIR DAS SICHERSTELLEN	WIE SIE ES PRÜFEN
Jede Änderung an der Plattform durchläuft einen automatisierten Build mit Tests, bevor sie in eine Umgebung gelangt. Der Build ist zugleich das Schwachstellen-Tor: Enthält eine Abhängigkeit eine bekannte Sicherheitslücke, schlägt er fehl – auf dem Server ab mittlerer, in der Oberfläche ab hoher Schwere –, dazu ein wöchentlicher Prüflauf.	Es gibt keinen Weg, Software am Build vorbei in den Betrieb zu bringen. Was nicht baut oder testet, wird nicht ausgeliefert – und was eine bekannte Lücke mitbringt, baut nicht. Wird die Gesundheitsprüfung nach einer Auslieferung rot, rollt sie automatisch zurück. Einmal pro Woche wird die Anwendung ohnehin mit aktuellem Basis-Image neu gebaut und in der Entwicklungsumgebung ausgerollt; in die Produktivumgebung kommt ein Stand nur mit einer Freigabe.	Auf Anfrage zeigen wir Ihnen den Ablauf und ein Beispiel für einen abgebrochenen Build.

Überwachung und Betreiberzugriff

- **Gesundheitsprüfung.** Jede Komponente meldet ihren Zustand über einen Prüfpunkt; fällt er auf Rot, startet die Anwendung automatisch neu. Telemetrie und Protokolle laufen je Umgebung in

Application Insights und Log Analytics zusammen.

- **Alarmierung.** Verfügbarkeit, Fehlerquote, Datenbank und Warteschlange werden überwacht. Ein Ausfall meldet sich per E-Mail an zwei Personen auf unserer Seite – erprobt mit einem Testalarm, nicht nur eingerichtet.
- **Wartung kündigen wir an.** Steht eine geplante Wartung an, erscheint ein Hinweis über der Anwendung – sichtbar bis zum angekündigten Ende.
- **Zwei benannte Personen.** Zugriff auf Produktivdaten haben ausschließlich benannte Identitäten – zwei Personen, keine geteilten Konten. Geheimnisse liegen nur im Key Vault.
- **Einrichtungszugänge im Protokoll.** Schlüssel, mit denen wir eine Umgebung einrichten, sind gedrosselt und jede Nutzung wird protokolliert.

KAPITEL 4

Ihre Daten sehen nur Sie. Auch bei uns.

Mehrere Kunden auf einer Plattform sind nur dann vertretbar, wenn die Trennung nicht von der Sorgfalt eines Entwicklers abhängt. Bei uns zieht die Datenbank die Grenze – und die Anwendung prüft bei jedem Start, dass sie hält.

Die Grenze zieht die Datenbank

WAS GILT	WIE WIR DAS SICHERSTELLEN	WIE SIE ES PRÜFEN
Jede Tabelle mit Kundendaten ist durch Row-Level Security in PostgreSQL geschützt: Eine Abfrage liefert nur Zeilen des eigenen Mandanten – beim Lesen wie beim Schreiben, auch für das Änderungsprotokoll.	Die Anwendung arbeitet mit einer Datenbankrolle, die fremde Zeilen gar nicht sehen kann. Ein vergessener Filter in der Anwendung wird dadurch zu einem leeren Ergebnis, nicht zu einer Datenpanne. Die Regeln sind Teil der Datenbankmigrationen und damit versioniert.	Der Selbsttest (nächster Abschnitt) ist der Beweis, der bei jedem Start neu erbracht wird.

Der Selbsttest

WAS GILT	WIE WIR DAS SICHERSTELLEN	WIE SIE ES PRÜFEN
Bei jedem Start prüft die Anwendung, ob die Mandantentrennung greift. Schlägt der Test fehl, startet sie nicht.	Eine Umgebung, in der die Trennung nicht wirkt, liefert keine Kundendaten aus – lieber keine Plattform als eine ohne Grenze. Das gilt in jeder Umgebung, auch in einer, die bei Ihnen läuft.	Auf Anfrage zeigen wir Ihnen den Test und sein Ergebnis.

Rollen

- **Vier Rollen und eine für Systeme.** Betreiber, Mandanten-Admin, Benutzer und Prüfer, dazu Integration für Systeme über die Schnittstelle; weitere Rollen richten wir für Sie ein. Die Oberfläche prüft Rechte, nie Rollennamen.
- **Prüfer sehen alles und ändern nichts.** Die Rolle „Prüfer“ liest Sendungen, Vorgänge und Dokumente, kann das Änderungsprotokoll Ihres Mandanten exportieren und das Prüfpaket je Sendung erzeugen – für Wirtschaftsprüfer, Zoll oder ein internes Audit, ohne Umweg über uns.

- **Die Betreiberrolle ist unveränderlich.** Ihre Rechte lassen sich nicht zur Laufzeit erweitern oder beschneiden; bei jedem Start gleicht die Anwendung sie mit dem Stand der Software ab.
- **Betreiberzugriffe stehen im Protokoll.** Verwaltungszugänge, mit denen wir eine Umgebung einrichten, laufen über eigene Schlüssel, sind gedrosselt und werden protokolliert. Auf Produktivdaten greifen nur zwei benannte Personen zu.

Drei Betriebsmodelle

Derselbe Code, dieselbe Trennung – nur der Ort ist verschieden.

- **Gemeinsame Plattform.** Betrieb durch uns auf Microsoft Azure in Schweden-Mitte, Trennung auf Datenbankebene wie oben beschrieben. Der Regelfall.
- **Dedizierte Instanz.** Eine eigene Umgebung nur für Sie – auf Wunsch in Ihrem eigenen Azure-Mandanten. Die Infrastruktur ist als Code beschrieben und lässt sich je Umgebung aufbauen.
- **On-Premises.** Betrieb in Ihrer eigenen Infrastruktur. Die Plattform ist als Container-Anwendung mit PostgreSQL, Nachrichtenwarteschlange, Cache und Objektspeicher gebaut; Telemetrie kann an Ihre eigenen Systeme gehen. Umfang von Betrieb, Updates und Support legen wir je Vertrag fest.

OpexGuard GbR · Pommernstr. 12, 67454 Haßloch · info@opexguard.de · www.opexguard.de/sicherheit