

Compliance mit PaperOffice AI: Workspaces, Audit-Center, Nachweise

Wer hat wann welches Dokument gesehen, geändert, geteilt oder gelöscht? Im Nachhinein lässt sich das nicht bauen. PaperOffice protokolliert unveränderlich, schwärzt personenbezogene Daten und hält Fristen je Dokumenttyp.

Drei Sicherheitsstufen je Workspace

Standard

Für den laufenden Betrieb

- AES-256-Verschlüsselung jeder Datei in Chunks und RAM-Disk-Verarbeitung
- Whitelist-Zugriffslisten und Rollen
- Versionen mit Audit-Trail, endgültiges Löschen

Für Teams, Projekte und den Alltag

Business

Für sensible Bestände

- Alles aus Standard
- Papierkorb, WORM-Schreibschutz und Workspace-Passwort
- Zugriffsschutz, externe Freigabe, SMS- oder Zwei-Personen-Freigabe

Für Buchhaltung, Personal und Verträge

Compliance

Für Hochsicherheit

- Alles aus Business
- Hardware-Verschlüsselung
- IP-Whitelist, 2FA-Pflicht, Wasserzeichen und geschützte PDF-Auslieferung

Für regulierte Branchen und Prüfungen

So entsteht ein Compliance-Workspace

1 Anlegen

Name, Zweck und Typ wählen: Standard, Business oder Compliance. Dazu Verarbeitungstiefe von Archiv bis Ultra, Speicherort EU-Cloud oder eigener Storage Mount, Aufbewahrungsfrist und Sprache.

2 Absichern

Je Workspace Passwort, Zwei-Personen- oder SMS-Freigabe, Papierkorb, WORM-Schutz, externe Freigaben mit Ablauf, in Compliance zusätzlich IP-Whitelist, 2FA-Pflicht, Wasserzeichen und Hardware-Verschlüsselung.

3 Arbeiten

Nutzer und Gruppen erhalten Rechte je Workspace, Agenten und MCP halten sich daran. Ein Upgrade der Stufe ist jederzeit möglich, ein Downgrade aus Compliance-Gründen nicht.

Audit-Center

Das Audit-Center hält fest, wer wann was mit welchem Dokument getan hat, und stuft Findings nach Schweregrad ein.

1 Erfassen

Jede Aktion an einem Dokument wird mit Zeit, Nutzer, Kontext und Integritäts-Hash festgehalten: ansehen, ändern, exportieren, freigeben, löschen. Nachträglich nicht veränderbar.

2 Bewerten

Die KI vergleicht Dokumente und Aktionen mit Mustern und Stammdaten: abweichende Bankverbindung, Rechenfehler, ungewöhnliche Zugriffe. Jedes Finding erhält einen Schweregrad von niedrig bis kritisch.

3 Prüfen

Kritische Findings lösen Benachrichtigungen aus und landen als Aufgabe bei einem Prüfer: genehmigen, ablehnen oder eskalieren, mit Kommentar im Trail. Berichte für Auditoren als PDF, CSV oder JSON.

Vollständiger Trail

Jede Aktion mit Zeit, Nutzer, Dokument und Kontext, feldgenau bei Änderungen: alter Wert, neuer Wert.

Unveränderlich

Einträge mit Integritäts-Hash, nachträglich nicht editierbar oder löscherbar.

Export und Berichte

Audit-Bericht je Dokument als PDF, Trail als CSV oder JSON, mit wählbarem Umfang.

Aufbewahrung

WORM-Schutz und Fristen je Dokumenttyp, Löschungen selbst sind Teil des Trails.

Fristen, Schwärzung, Integrität

Fristen je Dokumenttyp

Aufbewahrungsfrist in Jahren je Workspace, mit WORM-Schutz, der nach dem Aktivieren bestehen bleibt.

Freigabe als Prozess

Zwei-Personen-Freigabe, Aufgaben mit Frist und Eskalation, jeder Schritt landet im Protokoll.

Drei Sicherheitsstufen

Standard, Business und Compliance mit Papierkorb, WORM, Passwort, IP-Liste und Hardware-Verschlüsselung.

Trust Agent

Der Trust Agent prüft PDFs auf versteckte Inhalte, Überdeckungen, eingebettete Dateien und Manipulation.

PII automatisch gefunden

Namen, Adressen, IBANs, Geburtsdaten, E-Mail und Telefon je Kategorie wählbar, dazu eigene Begriffe und Whitelist.

Integrität geprüft

Versteckter Text, überdeckte Stellen, eingebettete Dateien und mehrere Speicherstände werden sichtbar gemacht.

Redact Agent

Der Redact Agent erkennt Namen, Adressen, IBANs und andere PII in Dokumenten und Bildern und schwärzt sie.

Audit-sicherer E-Mail-Versand

Bis zu zehn Dokumente aus dem DMS per E-Mail versenden, mit PDF-Passwort, sicherem Link und Protokoll jedes Schritts.

Nachweise und Dokumente

AVV-Generator · Art. 28 DSGVO

Der Auftragsverarbeitungsvertrag entsteht in der App — vorausgefüllt mit den Unternehmensdaten, als PDF mit PaperOffice-Briefkopf.

TOM-Generator · Art. 32 DSGVO

Technische und organisatorische Maßnahmen für genau die Services, die im Konto genutzt werden.

Security Center

Alle Geräte und Sitzungen des Kontos im Blick — wer greift wann und von wo zu.

DSGVO

PaperOffice erfüllt die DSGVO-Anforderungen an Auftragsverarbeiter — AVV (Art. 28) und TOM (Art. 32) aus dem Generator, Verarbeitung in der EU.

ISO/IEC 27001 (zertifiziert)

Internationaler Standard für Informationssicherheits-Management. ISO/IEC 27001 zertifiziert (Zertifikat unter NDA verfügbar); SOC 2 Type II in Vorbereitung.

SOC 2 Typ II (in Vorbereitung)

AICPA Service Organization Control für Trust Services Criteria

Betrieb und Verschlüsselung

Rechenzentrum

Dokumente rein. Ergebnisse raus. Keine externen KI-Anbieter, keine AI-Subprozessoren und kein Training mit Ihren Daten. Eigenes Rechenzentrum in der EU (Navarra, Spanien).

Verschlüsselung

AES-256 im Speicher, jede Datei in Chunks einzeln verschlüsselt, TLS 1.3 in der Übertragung, Compliance-Workspaces zusätzlich mit Hardware-Verschlüsselung.

Schlüsselverwaltung

Schlüssel außerhalb der Datenbank — nur für berechtigte Dienste lesbar

Zugriffskontrolle

Entschlüsselung nur für autorisierte Verarbeitung — mit Audit-Trail

Hinweis. Ob ein Verfahren regulatorischen Anforderungen genügt, hängt von der Umsetzung im Unternehmen ab (Rollen, Verfahrensdokumentation, Kontrollen). PaperOffice AI stellt die technischen Bausteine bereit; dieses Datenblatt ersetzt keine rechtliche Beratung. Nachweise: ISO/IEC 27001 zertifiziert (Zertifikat unter NDA verfügbar); SOC 2 Type II in Vorbereitung.