Datensouveränität im Praxistest

Gewährleistet unser Cloud-Dienst echte Datensouveränität?

tresorit | Swiss Post Digital

Datenstandort und rechtlicher Zugriff	Yes	No
Wo werden unsere Daten gespeichert – und ist das vertraglich klar geregelt?	☐	☐
Können Sie selbst entscheiden oder beeinflussen, wo Ihre Daten gespeichert werden?	☐	☐
Unterliegt der Anbieter rechtlichen Pflichten außerhalb der EU, die einen Zugriff auf unsere Daten ermöglichen könnten?	☐	☐
Verschlüsselung und Schlüsselkontrolle		
Sind unsere Daten bei Übertragung, Speicherung und Freigabe durchgängig verschlüsselt?	☐	☐
Werden die Daten auf unseren Geräten (clientseitig) verschlüsselt – bevor sie die Cloud erreichen?	☐	☐
Haben wir die Kontrolle über die Verschlüsselungsschlüssel – und nicht der Anbieter?	☐	☐
Handelt es sich um echte Ende-zu-Ende-Verschlüsselung bzw. Zero-Knowledge-Schutz, sodass der Anbieter keinen Zugriff Schlüssel und damit auf Klartextdaten hat?	☐	☐
Wenn ein Zugriff (rechtlich oder betrieblich) angefordert wird, wäre dies technisch möglich?	☐	☐
Rechte- und Zugriffskontrolle		
Können wir granular festlegen, wer Dateien sehen, bearbeiten, herunterladen oder weitergeben darf – und für wie lange?	☐	☐
Können wir klare Rollen und Berechtigungen für interne Teams sowie externe Beteiligte vergeben?	☐	☐
Können wir eine sichere Freigabe durch Passwortschutz, E-Mail-Bestätigung, Wasserzeichen, Download-Beschränkungen und weitere Funktionen gewährleisten?	☐	☐
Können wir Zugriffe bei Bedarf sofort widerrufen?	☐	☐
Können wir Richtlinien zentral festlegen und für alle Nutzer und Teams durchsetzen?	☐	☐
Nachvollziehbarkeit, Versionierung und Audits		
Wird automatisch protokolliert, wer wann auf welche Daten zugegriffen oder sie verändert hat?	☐	☐
Sind Protokolle detailliert, zuverlässig und exportierbar, so dass sie interne Überprüfungen und externe Audits unterstützen?	☐	☐
Können wie veraltete oder unnötige Zugriffsrechte leicht identifizieren und entfernen?	☐	☐
Können wir frühere Versionen von Dateien nachverfolgen und wiederherstellen?	☐	☐