EPERI

Empower your Data.
Keep control.

eperi® sEcure — Maximale Sicherheit für sensible Daten in Microsoft 365

Warum eperi® sEcure?

Immer mehr Unternehmen setzen auf eine „Cloud-First"-Strategie und nutzen Anwendungen wie Microsoft 365. Gleichzeitig erfordern gesetzliche Vorgaben und Compliance-Richtlinien, dass nur die Dateneigentümer Zugriff auf persönliche und geschäftskritische Daten haben. **eperi® sEcure** schützt Ihre sensiblen Daten vor unbefugtem Zugriff — sowohl durch Cloud-Anbieter als auch durch Dritte — und sorgt für eine sichere, konforme Cloud-Nutzung. Unsere Lösung unterstützt beliebte Microsoft 365-Anwendungen wie SharePoint, OneDrive, Outlook, Teams, Planner und ToDo, während alle wichtigen Funktionen erhalten bleiben.

Gefahren ohne eperi® sEcure

Zugriff durch Dritte:

Wer Ihre Daten verschlüsselt, hat potenziell Zugriff darauf — auch Cloud-Anbieter bei BYOK- oder HYOK-Services.

Verantwortung:

Jedes Unternehmen trägt selbst die Verantwortung für den Schutz seiner Daten und die Einhaltung der gesetzlichen Anforderungen.

Compliance:

Microsoft 365 ist nur mit unabhängigen technischen und organisatorischen Maßnahmen (TOMs) DSGVO-konform.

Vorteile für Ihr Unternehmen

- **Datensicherheit:** Kritische Daten verlassen Ihr Unternehmen nur in verschlüsselter Form — Schutz vor Datenmissbrauch durch Dritte, auch bei Weitergabe an Behörden von Drittstaaten.
- **Volle Kontrolle:** Verschlüsselung und Schlüsselmanagement liegen ausschließlich in Ihrer Hand.
- **Einfache Verwaltung:** Die Verschlüsselung wird zentral über eine intuitive Oberfläche gesteuert.
- **Funktionalität erhalten:** Such- und Sortierfunktionen sowie andere wichtige M365-Funktionen bleiben uneingeschränkt nutzbar.
- **Modernste Technologie:** Verschlüsselung nach "Stand der Technik" VOR der Cloud
- **Nahtlose Integration:** Keine Anpassungen oder Installationen auf Client- oder Applikationsseite notwendig.
- **Höchste Sicherheitsstandards:** Nutzen Sie AES-256, RSA-4096 oder individuelle Algorithmen zur Verschlüsselung Ihrer Daten
- **Zukunftssicher:** Unterstützung von Crypto Agility durch auswechselbare Algorithmen und ready für Post-Quanten-Kryptografie
- **Unsichtbar für Nutzende:** Mitarbeitende haben keine Berührungspunkte mit **eperi® sEcure** und merken bei der Nutzung von M365 keinen Unterschied
- **Flexibel skalierbar:** Arbeitet mit bestehenden sowie neuen M365 Installationen (Background Encryption)

sales@eperi.com

+49 6157 95639 00

Gesetze und Vorschriften: Mit eperi® sEcure immer konform

Verschiedene nationale und internationale Gesetze und Regulatoriken fordern die Verschlüsselung von Daten, um deren Schutz zu gewährleisten und Datensouveränität herzustellen.

Datenschutz-Grundverordnung (DSGVO):
Artikel 32 fordert Pseudonymisierung und Verschlüsselung personenbezogener Daten. Verstöße können zu Bußgeldern von bis zu 20 Mio. Euro oder 4 % des Jahresumsatzes führen.

NIS2-Richtlinie:
Setzt neue Cybersicherheitsstandards und fordert Schutzmaßnahmen nach dem „Stand der Technik", wie Verschlüsselung. Die Geschäftsführung haftet bei Nichteinhaltung.

Digital Operational Resilience Act (DORA):
Verpflichtet Finanzinstitute zur Verschlüsselung, um Datenintegrität und Vertraulichkeit sicherzustellen. Maßnahmen müssen dem „Stand der Technik" entsprechen.

Geschäftsgeheimnis-Schutzgesetz (GeschGehG):
Schützt Geschäftsgeheimnisse nur, wenn „angemessene Maßnahmen" wie Verschlüsselung angewendet werden. Fehlender Schutz kann Schadensersatzansprüche gefährden.

§203 StGB:
Regelt den Schutz von Privatgeheimnissen für Berufsgeheimnisträger. Verschlüsselung ist essenziell, um Vertraulichkeit zu wahren und rechtliche Folgen zu vermeiden.

Bundesdatenschutzgesetz (§64 BDSG):
Die Verantwortlichen haben den Stand der Technik zu berücksichtigen. In Absatz 2 sind explizit Pseudo- und Anonymisierung als Maßnahmen genannt.

Welche Felder kann eperi® sEcure in Microsoft 365 schützen?

In den einzelnen M365 Anwendungen können Sie folgende Daten verschlüsseln oder tokenisieren:

- Outlook: Schutz für Betreff, Inhalte und Anhänge von E-Mails sowie von Kalendereinträgen.
- Teams (in Desktop-, Web- & Mobil-App): Schutz von Chatnachrichten, Kanälen, Gruppen und (mit eperi® sEcure M365 OneDrive & eperi® sEcure M365 Sharepoint) auch Anhängen, sowie Betreff, Beschreibung und Anhänge von Kalendereinträgen (empfohlen nur in Verbindung mit eperi® sEcure M365 Outlook).
- Planner & ToDo: Verschlüsselung von Aufgaben, Notizen und Anhängen in beiden Tools sowie Aufgabengruppen, Checklisten und Kommentaren in Planner und Aufgabenschritten in ToDo.
- SharePoint: Verschlüsselung von Dateiinhalten in Bibliotheken sowie Datei- und Feldinhalten in Listen.
- OneDrive: Absicherung von Dateien, einschließlich nativer Funktionen wie Explorer-Sync und Backup.

Cloud-Datensicherheit nach Stand der Technik

Durch die Verschlüsselung Ihrer sensiblen Daten VOR der Cloud bietet eperi® sEcure umfassenden Schutz — während der Übertragung, Speicherung und Nutzung — ohne Einschränkungen für Nutzer.