KOMMENTAR

DORA Oversight Guide: Was Finanzunternehmen jetzt über Verschlüsselung und Schlüsselhoheit wissen müssen

Ein Kommentar von Andreas Steffen, CEO von eperi

Am 15. Juli 2025 veröffentlichten die europäischen Aufsichtsbehörden (ESA) den ersten DORA Oversight Guide, ein entscheidendes Dokument, das die künftige Überwachung kritischer IKT-Drittdienstleister konkretisiert. Im Zentrum steht der Aufbau sogenannter Joint Examination Teams (JETs) zur europaweiten Kontrolle von Cloud-Anbietern, Softwarelieferanten und anderen wichtigen Drittparteien.

Doch der Guide enthält weit mehr als nur organisatorische Hinweise. Insbesondere Artikel 5.4.1 des Leitfadens stellt klar, dass Aufsichtsbehörden künftig Empfehlungen zu Subcontracting und Verschlüsselungstechnologien aussprechen dürfen – mit gravierenden Folgen für alle Finanzunternehmen, die Hyperscaler wie Microsoft, Amazon oder Google nutzen.

Warum das jetzt relevant ist? Weil sich mit Inkrafttreten von DORA im Januar 2025 alle betroffenen Organisationen auf ein neues Kontrollniveau vorbereiten mussten und die Zeit drängt, falls es noch nicht bereits geschehen ist.

Was steht im DORA Oversight Guide?

Der 74-seitige Leitfaden beschreibt detailliert, wie die ESA (EBA, ESMA und EIOPA) ihre Aufsichtsbefugnisse gegenüber kritischen IKT-Dienstleistern künftig ausüben. Ein zentraler Mechanismus sind die Joint Examination Teams (JETs), die grenzüberschreitend Audits, technische Inspektionen und Vor-Ort-Besuche durchführen.

Ziel ist es, einheitliche Standards durchzusetzen und sicherzustellen, dass Anbieter kritischer Infrastrukturen das Risiko- und Resilienzprofil des Finanzsektors nicht gefährden.
Besonders relevant: Die ESA kann Empfehlungen zu kritischen Sicherheitsmaßnahmen aussprechen, darunter:

- Sicherheitsvorgaben für Subunternehmer (Subcontracting),
- Verwendung starker Verschlüsselung,
- Nachweis der Schlüsselhoheit durch das Finanzunternehmen selbst.

Artikel 5.4.1 – Der Schlüssel zur Schlüsselkontrolle

Artikel 5.4.1 des Oversight Guides ist besonders bedeutsam. Dort heißt es sinngemäß, dass Aufsichtsbehörden Empfehlungen abgeben dürfen, die auch kryptografische Schutzmaßnahmen betreffen, insbesondere im Hinblick auf Subdienstleister und ausgelagerte IT-Umgebungen.
Das bedeutet konkret: Wenn ein Finanzunternehmen Cloud-Dienste von Microsoft, AWS oder Google nutzt, muss es in der Lage sein, jederzeit die Hoheit über die verwendeten Verschlüsselungsschlüssel nachzuweisen – auch bei redundanten oder ausgelagerten Systemen. Damit rückt ein bislang oft vernachlässigter Punkt in den Fokus. Wer kontrolliert die Daten und wer hält die Schlüssel in der Hand?

Warum klassische Cloud-Verschlüsselung nicht mehr ausreicht

Viele Finanzunternehmen setzen bereits auf Verschlüsselung. Doch oft werden Schlüssel in der Cloud selbst gespeichert oder durch den Anbieter verwaltet. Das Problem:

- Die Datenhoheit ist nicht vollständig gewährleistet.
- Im Fall von Subcontracting (z. B. bei global verteilten Rechenzentren) fehlt der Überblick.
- Die Aufsichtsbehörden könnten dies als Mangel werten, inkl. Compliance-Risiken.

Die Anforderungen aus dem DORA Oversight Guide verlangen ein neues Niveau an Transparenz und Kontrolle.

Schlüsselhoheit behalten

Eine Verschlüsselungslösung, die perfekt auf die Anforderungen aus DORA zugeschnitten ist, verschlüsselt Daten, bevor sie die Cloud erreichen – Client-seitig und formaterhaltend, damit sie im Hintergrund weiterverarbeitet werden können. Eine Verschlüsselungsarchitektur sollte vier wichtige Aspekte sicherstellen:

- Die Schlüsselkontrolle bleibt vollständig beim Unternehmen. Weder Cloud-Anbieter noch Dritte haben Zugriff.
- Sie ist kompatibel mit Microsoft 365, Salesforce und anderen Web-Applikationen.
- Sie erfüllt strengste regulatorische Vorgaben – inklusive DORA, NIS2, DSGVO.
- Es ergeben sich keine Funktionseinbußen – Suchfunktionen, Sortierung und Kollaboration

Mit dieser Architektur können Unternehmen gegenüber Aufsichtsbehörden nachweisen, dass die kryptografischen Schutzmaßnahmen vollständig unter Ihrer Kontrolle stehen – genau das, was Artikel 5.4.1 fordert.

Fazit: Wer seine Schlüssel aus der Hand gibt, gibt auch die Kontrolle ab

Der neue DORA Oversight Guide zeigt unmissverständlich, dass Aufsichtsbehörden die ITK-Drittdienstleister künftig genau unter die Lupe nehmen. Für Finanzunternehmen bedeutet das, dass nur wer Datenhoheit und Schlüsselkontrolle nachweisen kann, die Anforderungen erfüllt. Mit eperi sEcure behalten Finanzunternehmen die volle Kontrolle, sowohl technisch, rechtlich und organisatorisch. Damit sind die Voraussetzungen für eine zukunftssichere, resiliente IT-Strategie im Finanzumfeld geschaffen.

Über die Eperi GmbH:

Wir bei eperi® sind der festen Überzeugung, dass Datenschutz ein grundlegendes Menschenrecht ist. Unser Ziel ist es, dass Menschen und Unternehmen zu jeder Zeit die Kontrolle über ihre Daten behalten. Ohne Kompromisse und mit der besten Technologie. Mit dem Fokus auf die Sicherheit unserer Kunden haben wir eine Lösung geschaffen, die für den Benutzer unsichtbar ist und gleichzeitig die höchsten Sicherheitsstandards erfüllt.
Mit der eperi® Lösung profitieren unsere Kunden von allen Vorteilen der Cloud-Nutzung, wie beispielsweise einer effizienten unternehmensweiten Kollaboration, und bleiben dabei rechtssicher gemäß weltweiten Datenschutzgesetzen. Wir besitzen mehrere internationale Patente für unsere innovative Multi-Cloud-Technologie, die einen konkurrenzlosen Datenschutz für SaaS Anwendungen, individuelle Applikationen und Dateien bietet. Unsere Kunden behalten die alleinige Kontrolle über alle sensiblen Daten, da keine unverschlüsselten Daten in die Cloud gesendet werden.
Wir ermöglichen die Cloud – einfach, sicher, individuell, DSGVO-konform.

Pressekontakt eperi

Eperi GmbH
Sabine Jost
Werner-von-Siemens-Str. 2
64319 Pfungstadt
Tel: +49 (0)6157 95639 16
E-Mail: sabine.jost@eperi.com
Web: www.eperi.com

Pressekontakt Agentur

TC Communications
Thilo Christ
Tel: +49 171 6220610
Alexandra Schmidt
Tel: +49 170 3871064
E-Mail: eperi@tc-communications.de