Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

GDV Gesamtverband der Versicherer

Positionspapier der Finanzwirtschaft

zur Umsetzung der DORA-Anforderung „Encryption in Use"

Kontakt:

Deutsche Kreditwirtschaft (DK)
Federführer 2025:
Bundesverband deutscher Banken e.V.
Diana Campar
Associate Director
Telefon: +49 30 1663-1546
E-Mail: diana.campar@bdb.de

Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV)
Gabriele Sieck
Referentin Informationssicherheit
Telefon: +49 30 2020-5454
E-Mail: g.sieck@gdv.de

Berlin, 29. Juli 2025

Einführung und Zielsetzung

Mit der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates über die digitale operationale Resilienz (Digital Operational Resilience Act – DORA) hat die Europäische Union einen umfassenden regulatorischen Rahmen für die Cybersicherheit, das Management von IKT-Risiken sowie die digitale operationale Resilienz im gesamten Finanzsektor geschaffen. Eine der neuen Anforderungen betrifft den Schutz von Daten während ihrer Verarbeitung – die sogenannte „Encryption in Use". Diese Anforderung stellt einen Paradigmenwechsel dar, da sie über die bisherigen Schutzziele der Verschlüsselung ruhender Daten („at Rest") und Daten in der Übertragung („in Transit") hinausgeht. Das vorliegende Positionspapier beschreibt den aktuellen Stand der Technik, bewertet die Relevanz möglicher Bedrohungsszenarien, ordnet etablierte Schutzmaßnahmen ein und formuliert Kriterien für eine realistische und wirksame Umsetzung im Einklang mit den regulatorischen Zielsetzungen.

Regulatorischer Rahmen und Umsetzungsperspektive

Die Verpflichtung zur Verschlüsselung von Daten während ihrer Nutzung ergibt sich aus Artikel 9 Absatz 2 der DORA-Verordnung sowie den ergänzenden technischen Regulierungsstandards zum IKT-Risikomanagement. In dieser konkreten Ausgestaltung handelt es sich um eine neue regulatorische Anforderung, die bislang weder auf europäischer noch auf nationaler Ebene ausdrücklich gefordert war.

Vor diesem Hintergrund erscheint es aus Sicht der Finanzwirtschaft erforderlich, eine angemessene Übergangs- und Umsetzungsphase vorzusehen, in der sowohl technische Voraussetzungen geschaffen als auch organisatorische und strategische Anpassungen vorgenommen werden können. Dabei ist sicherzustellen, dass funktional gleichwertige, risikoadäquat ausgestaltete Schutzmaßnahmen als zulässige Alternativen zur technischen Umsetzung von „Encryption in Use" anerkannt werden.

Bedrohungsszenarien und praktische Relevanz

Die Bedrohungslage, auf die sich „Encryption in Use" bezieht, umfasst insbesondere unbefugte Zugriffe auf Daten während der Verarbeitung, etwa durch Speicheranalysen („Memory Attacks") oder Manipulation laufender Prozesse. Diese Angriffsszenarien sind in ihrer Umsetzung technisch hochkomplex, erfordern spezielles Fachwissen und setzen das Überwinden mehrerer, bereits vorhandener Sicherheitsmechanismen voraus. Der Erfolg solcher Angriffe in der Praxis ist zwar nicht gänzlich auszuschließen, jedoch nicht sehr realistisch, da diese durch umfangreiche Sicherheitsmechanismen mitigiert werden.

Mit dem Aufkommen generativer KI-Systeme, wird argumentiert, verändere sich jedoch die Risikoperspektive: Während klassische Memory-Angriffe selten blieben, entstehe durch die zunehmend produktive Nutzung von generativer KI (GenAI) ein neuer, praxisnaher Angriffsvektor – etwa durch automatisierte Speicheranalysen, bei denen KI gezielt nach sensiblen Daten im Arbeitsspeicher sucht.

Auch vor dem Hintergrund möglicher GenAI-basierter Entwicklungen können die Sicherheitsanforderungen von Vertraulichkeit, Integrität und Verfügbarkeit während der Verarbeitung der Daten durch etablierte Schutzmaßnahmen sichergestellt werden.

Aus Sicht der Finanzwirtschaft ist daher eine differenzierte, risikobasierte Bewertung erforderlich, die den Schutzbedarf je nach Datenkategorie, Verarbeitungskontext und Angriffsmodell individuell bestimmt.

Technologischer Stand und Entwicklungsperspektiven

Grundsätzlich steckt die Verschlüsselung von „Data in Use“ (also Daten im Arbeitsspeicher des Rechners) noch in den Kinderschuhen. Technologisch existieren derzeit nur eingeschränkt praxistaugliche Lösungen für eine echte Verschlüsselung während der Datenverarbeitung. Verfahren der homomorphen Verschlüsselung erlauben rechnerische Operationen auf verschlüsselten Daten, befinden sich aber noch im Forschungsstadium. Sie sind bislang nur für sehr spezialisierte Anwendungsfälle geeignet, mit enormen Rechenaufwänden verbunden und können noch nicht für praxis-relevante Nutzungsszenarien angewandt werden, da die ressourcenintensiven Verarbeitungsschritte beim Schlüsselinhaber verbleiben würden und somit nicht durch die homomorphe Verschlüsselung geschützt wären. Eine mittelfristig adäquate Lösung könnte das sogenannte Confidential Computing bieten. Dabei werden Daten in abgeschotteten, hardwarebasierten Ausführungsumgebungen verarbeitet. Erste Implementierungen existieren bereits bei verschiedenen Cloud-Anbietern. Dabei verlagert sich die Vertrauensstellung vom Cloud-Anbieter auf den Hardware-Hersteller – was neue Abhängigkeiten schafft. Ferner ist die Verfügbarkeit dieser Technologien bislang noch begrenzt – sowohl im Hinblick auf die unterstützten Plattformen als auch auf die darauf aufsetzbaren Dienste. Zudem fehlen Praxiserfahrungen, die eine Voraussetzung für eine flächendeckende Einführung darstellen.

In kundenorientierten Anwendungen wie mobilen Apps oder webbasiertem Online-Banking bestehen darüber hinaus grundlegende technische Einschränkungen. Der Einsatz von „Encryption in Use“ auf mobilen Endgeräten ist bislang weder etabliert noch ohne weiteres umsetzbar. Zudem ist regulatorisch nicht eindeutig, ob und inwieweit die Anforderung auf Kundengeräte angewendet werden soll.

Auch für viele KI-Verfahren insbesondere für GenAI ist „Encryption in Use“ aktuell nicht möglich. Die „Prompts“ der Nutzer und die Kontextinformation (Hintergrundinformationen aus einem Retrieval-Augmented Generation System) werden in Form von Zahlenvektoren in die Modelle gegeben (embedding). Die Bedeutung dieser Zahlenvektoren ist zwar durch das embedding encodiert, dieses Encoding kann jedoch leicht decodiert werden. Das Training großer Sprachmodelle (LLMs) auf eine Verschlüsselung von Daten während der Nutzung wäre mit erheblichem Aufwand verbunden und ist nach aktuellem Stand der Technik nicht vorgesehen. Nach aktuellem Kenntnisstand ist eine Verschlüsselung von Daten während der Nutzung (Encryption in Use) im Kontext generativer KI bzw. großer Sprachmodelle (LLMs) technisch noch nicht umsetzbar. Die Anforderung würde sich daher auch negativ auf den KI-Einsatz bei den Finanzunternehmen auswirken.

Etablierte Schutzmaßnahmen mit hohem Schutzniveau

Finanzunternehmen verfügen bereits heute über eine Vielzahl bewährter technischer und organisatorischer Sicherheitsmaßnahmen, die einen effektiven Schutz sensibler Daten während der Verarbeitung gewährleisten. Hierzu zählen insbesondere Hardware Security Modules (HSMs), wie sie etwa im Zahlungsverkehr zur Verwaltung und Nutzung kryptografischer Schlüssel eingesetzt werden. Solche etablierten Lösungen bieten eine physisch abgeschottete, manipulationssichere Umgebung und erfüllen damit das Ziel der „separated and protected environments", wie sie in Artikel 9 der DORA-Verordnung als zulässige Alternative zur „Encryption in Use" vorgesehen sind.

Weitere etablierte Schutzmaßnahmen umfassen unter anderem die Segmentierung sensibler Datenverarbeitung, die strikte Zugangskontrolle, den Einsatz sicherer Laufzeitumgebungen sowie umfassende Maßnahmen zur Schwachstellenanalyse und Angriffserkennung. Diese Maßnahmen sind technologisch ausgereift, operativ erprobt und gewährleisten ein hohes Schutzniveau für besonders vertrauliche Daten. Sie leisten bereits heute einen wesentlichen Beitrag zur Sicherstellung von Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit in kritischen Geschäftsprozessen.

Auch unter Berücksichtigung neuer technologischer Entwicklungen, insbesondere im Bereich generativer KI, behalten diese Schutzmaßnahmen ihre Relevanz und lassen sich risikobasiert auf entsprechende Anwendungsfälle übertragen. So gelten etwa für die interne Textgenerierung, die Erstellung von Schulungsmaterial oder die nicht-personenbezogene Verarbeitung interner Richtlinien geringere Anforderungen. Demgegenüber erfordern hochsensible, finanzrelevante Anwendungen wie die Kundeninteraktion oder KI-gestützte Entscheidungsprozesse weitergehende, kontextgerechte Schutzmaßnahmen.

Regulatorische Anerkennung gleichwertiger Maßnahmen

Die Finanzwirtschaft spricht sich deshalb ausdrücklich dafür aus, dass etablierte und effektive Schutzmaßnahmen regulatorisch als gleichwertige Alternativen zu einer technischen „Encryption in Use" anerkannt werden. Dies entspricht der Systematik der DORA-Verordnung, die, sofern eine Verschlüsselung während der Nutzung technisch nicht umsetzbar ist, auch das Verarbeiten in geschützten Umgebungen oder andere gleichwertige Maßnahmen zulässt. Eine angemessene Berücksichtigung dieses risikobasierten Ansatzes in der Aufsichtspraxis ermöglicht eine praxisnahe Umsetzung unter Wahrung hohen Sicherheitsstandards. Dabei sollte den Finanzunternehmen ein angemessener Spielraum bei der Wahl der kompensierenden Maßnahmen mit Blick auf den Schutzbedarf eingeräumt werden.

Governance und risikobasierte Umsetzung

Finanzunternehmen sind sich ihrer Verantwortung im Umgang mit sensiblen Daten und regulatorischen Anforderungen bewusst und stützen sich bei der Umsetzung von „Encryption in Use" auf etablierte Governance-Strukturen. Zur Sicherstellung einer wirksamen Umsetzung sind die Verantwortlichkeiten für die verschiedenen Verschlüsselungsarten – „at Rest", „in

Transit“ und „in Use“ – innerhalb des Finanzunternehmens klar definiert. Der Einsatz entsprechender Technologien oder alternativer Maßnahmen erfolgt auf Grundlage einer fundierten Datenklassifikation und Risikoanalyse. Darüber hinaus sind IKT-Dienstleister vertraglich so einzubinden, dass sowohl zukünftige technologische Entwicklungen als auch regulatorische Anforderungen adäquat berücksichtigt werden. Technologische Weiterentwicklungen sind regelmäßig zu überprüfen, um mit fortschreitender Reife geeignete Maßnahmen schrittweise einführen zu können.

Fazit

„Encryption in Use“ ist ein sicherheitstechnisches Ziel, dessen konkrete Umsetzung jedoch maßgeblich von mittel- und langfristigen technologischen, wirtschaftlichen und betrieblichen Rahmenbedingungen abhängt. Eine kurzfristige, flächendeckende Umsetzung über alle Anwendungsbereiche hinweg ist weder realistisch noch zielführend und würde dem Grundsatz der Verhältnismäßigkeit, wie er in der DORA-Verordnung angelegt ist, nicht gerecht.

Die Finanzwirtschaft empfiehlt daher einen phasenweisen, risikobasierten Umsetzungsansatz, der bestehende Schutzmaßnahmen anerkennt, neue Technologien mit Augenmaß einführt und regulatorische Anforderungen im Einklang mit der praktischen Umsetzbarkeit bringt. Ziel muss es sein, die digitale Resilienz der Finanzunternehmen wirksam zu stärken, ohne dabei die technischen und wirtschaftlichen Realitäten aus dem Blick zu verlieren.