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

Position paper of the financial sector

on the implementation of DORA's 'Encryption in Use' requirement

Contact:

German Banking Industry Committee (GBIC)
Coordinator 2025:
Bundesverband deutscher Banken e.V.
Diana Campar
Associate Director
Telephone: +49 30 1663-1546
E-Mail: diana.campar@bdb.de

German Insurance Association (GDV)
Gabriele Sieck
Information Security Officer
Telephone: +49 30 2020-5454
E-Mail: g.sieck@gdv.de

Berlin, 29 July 2025

Introduction and objectives

Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience (Digital Operational Resilience Act, DORA) creates a comprehensive regulatory framework for cybersecurity, ICT risk management and digital operational resilience across the entire financial sector. One of the new requirements relates to protecting data while it is being processed – known as 'Encryption in Use'. This requirement represents a major shift as it goes far beyond the current protection aims of encrypting data at rest and data in transit. This position paper describes the current status of the technology, assesses the relevance of possible threat scenarios, categorises established protective measures and formulates criteria for realistic and effective implementation in line with regulatory objectives.

Regulatory framework and implementation prospects

The requirement to encrypt data during its use is set out in Article 9(2) of DORA and in supplementing regulatory technical standards on ICT risk management. This specific constellation is a new regulatory requirement, which has not yet been explicitly required at either European or national level.

Against this background, the financial sector believes that an appropriate transition and implementation phase is necessary. This period could then be used to establish technical requirements and also to make organisational and strategic adjustments. It must be ensured here that functionally equivalent, risk-adequate protection measures are recognised as permissible alternatives to the technical implementation of Encryption in Use.

Threat scenarios and practical relevance

The threat scenario that Encryption in Use is designed to mitigate includes unauthorised access to data during processing, such as through memory attacks or by manipulating ongoing processes. These attack scenarios are technically highly complex to implement, require specialist technical knowledge and presuppose that several existing security mechanisms have already been circumvented. Although the success of such attacks in practice cannot be completely ruled out, they are not very realistic as they are mitigated by extensive security mechanisms.

Nevertheless, it is argued that with the advent of generative AI systems, the risk perspective is changing. While classic memory attacks are rare, the increasingly productive use of generative AI (GenAI) is creating a new, practical attack vector – for example through automated memory analyses in which AI specifically searches for sensitive data in the working memory. Even against the background of possible GenAI-based developments, the security requirements of confidentiality, integrity and availability during the processing of the data can be secured through established protective measures.

In the opinion of the financial sector, a differentiated, risk-based assessment is therefore required that individually determines the need for protection depending on the data category, processing context and attack model.

Technological status and development prospects

The encryption of data in use (i.e. data stored in the working memory of the computer) is still in its infancy. In terms of the technology, there are currently only a limited number of practicable solutions for genuine encryption during data processing. Homomorphic encryption procedures do allow computational operations to be carried out on encrypted data but are still at the research stage. So far, they are only suitable for very specialist use cases, involve enormous computing effort and cannot yet be used for practice-relevant usage scenarios, as the resource-intensive processing steps would remain with the encryption key owner and would not therefore be protected by homomorphic encryption. An adequate solution for the medium term might be to offer what is known as confidential computing. This is where data is processed in isolated, hardware-based execution environments. Initial versions already exist and are used by a number of cloud providers. However, this shifts the position of trust from the cloud provider to the hardware manufacturer – which creates new dependencies. Furthermore, the availability of this technology is still limited – both in terms of supported platforms and the services that can be based on them. In addition, there is a lack of practical experience, which would be a requirement for their widespread introduction.

There are also fundamental technical limitations in customer-oriented applications, such as mobile apps or web-based online banking. The implementation of Encryption in Use on mobile devices is neither established nor possible without further developments. In addition, it is not clear in regulatory terms, whether and to what extent the requirement is to be applied to customers' devices.

Encryption in Use is also not currently available for many AI processes, in particular for GenAI. The user's prompts and the context information (background information from a Retrieval Augmented Generation (RAG) system) are added to the models in the form of number vectors (embedding). Although the meaning of these number vectors is encoded through the embedding, this form of encoding is easily decoded. Training large language models (LLMs) to encrypt data during use would involve considerable effort and is not possible with the current state of the technology. According to the current state of knowledge, the encryption of data during use (Encryption in Use) is not yet technically feasible in the context of generative AI or large language models (LLMs). The requirement would therefore also have a negative impact on the use of AI by financial entities.

Established protective measures with high level of protection

Financial entities already have a variety of proven technical and organisational security measures in place, which ensure effective protection against the loss of sensitive data during processing. These include, in particular, Hardware Security Modules (HSMs) such as those used in payment systems to manage and utilise cryptographic keys. Such established solutions offer a physically isolated environment that protects against manipulation and, therefore, meets the objective of "separated and protected environments", as provided for in Article 9 of the DORA regulation as a permitted alternative to Encryption in Use.

Other established protective measures include the segmenting of sensitive data processing, strict access control, the use of secure runtime environments and comprehensive measures for analysing vulnerabilities and identifying attacks. These measures are technologically mature, have been tested in an operational environment and found to ensure a high level of protection for particularly confidential data. They already make a considerable contribution to guaranteeing confidentiality, integrity, authenticity and availability in critical business processes.

Even taking into account new technological developments, particularly in the field of generative AI, these protective measures remain relevant and can be transferred to corresponding use cases on a risk-based basis. Less stringent requirements apply to internal text generation, creating training materials or to processing internal guidelines containing no personal information, for example. In contrast, highly sensitive, financially relevant applications, such as customer interactions or AI-supported decision-making processes require more extensive protective measures based on context.

Regulatory recognition of measures of equivalent value

The financial sector is therefore explicitly in favour of having established and effective protective measures for Encryption in Use recognised as equivalent alternatives in regulatory terms. This complies with the DORA Regulation, which, if encryption during use is not technically feasible, also allows processing in protected environments or other equivalent measures. Appropriate consideration of this risk-based approach in supervisory practice enables practical implementation while maintaining high security standards. Financial entities should be given appropriate leeway in choosing compensatory measures with regard to protection needs.

Governance and risk-based implementation

Financial entities are very aware of their responsibility when it comes to sensitive data and regulatory requirements, and rely on established governance structures when implementing Encryption in Use. To ensure effective implementation, the responsibilities for the various encryption types – at rest, in transit and in use – are clearly defined within the financial entity. The relevant technology or alternative measures are employed on the basis of a robust data classification and risk analysis. Furthermore, ICT service providers would need to be contractually required to take adequate account of both future technological developments as well as regulatory requirements. Further technological developments would need to be reviewed regularly so that appropriate measures could be introduced gradually as they mature.

Conclusion

Encryption in use is a security objective, but its concrete implementation depends largely on medium- and long-term technological, economic, and operational conditions. Short-term, widespread implementation across all areas of application is neither realistic nor expedient and would not comply with the principle of proportionality as set out in the DORA Regulation.

The financial sector therefore recommends a phased, risk-based implementation approach that recognises existing protective measures, introduces new technologies with a sense of proportion and brings regulatory requirements into line with practical feasibility. The aim must be to effectively strengthen the digital resilience of financial entities without losing sight of technical and economic realities.