SMART PAYMENT ASSOCIATION

# THE DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

## SPA's Position on Physical Payment Card Personalization

November 2024

## 1. INTRODUCTION

The Digital Operational Resilience Act[1] ("DORA") has been released to achieve a harmonized high level of cyber-resilience in the information and communication technology ("ICT") systems used by the European financial industry. DORA was adopted on December 14, 2022, and will come into effect on January 17, 2025. DORA is further supported by Regulatory Technical Standards, which outline additional requirements for different articles of the regulation.

DORA includes provisions for financial entities to monitor the ICT services they outsource to third parties. DORA also establishes criteria to identify the level of criticality of outsourced ICT services with a focus on contractual aspects for third Party ICT service providers to ensure the conformance with DORA.

Smart Payment Association (SPA) considers that physical payment card personalization doesn't fall under the remit of DORA.

This document describes why.

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector

# 2. KEY SPA MESSAGES ON PAYMENT CARD PERSONALIZATION IN RELATION TO DORA COMPLIANCE

1. **Card personalization is a manufacturing process, not an ICT service provided to banks**: the issuance of a physical payment card is **the outcome of an industrial process that concludes with the delivery of a physical payment card to the bank customer.**
2. **Card personalization is not part of the card payment system**: Card personalization centres operate independently and are not integrated in the bank's ICT systems nor in the card payment systems. Any disruption in card personalisation cannot impact these systems.
3. **Card personalization is an offline process**: The personalization of payment cards should be out-of-the scope of DORA since it is not an online, but an offline process. Therefore, card personalization services shouldn't be included in the specific risk management program to be elaborated by banks to comply with DORA.
4. **The resilience scope of DORA refers to networked ICT Systems**: A card personalization centre is neither a networked infrastructure nor an information system and therefore does not fall under the DORA remit.

# 3. WHY PERSONALIZATION CARD SERVICES DO NOT FALL UNDER THE DORA REMIT

## 3.1. Card personalization is a manufacturing process, not an ICT service provided to banks

According to article 3 (21) of DORA: "***ICT services*** *means* ***digital, and data services*** *provided through ICT systems to one or more internal or external users* ***on an ongoing basis****, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services*".

Card personalization is an industrial process where an individual set of cardholder data is stored into each card. Personalization is completely and exclusively executed in a manufacturing site called the card personalization centre, using customer data provided by banks. Card personalization centres are subject to stringent security audits and certifications against recognized international industrial standards, in particular to ensure adequate protection of the customer data received.

Card personalization is the final step of the production and issuance process of a physical payment card. After the card has been personalized, SPA members use postal services to mail the physical card to the customer, at the address designated by the bank. The physical delivery of cards by postal mail, final step in the card personalization and issuance process, cannot be considered as a DORA ICT service. Furthermore, none of the DORA categories is relevant to this context as set out in Annex III of the Commission Delegated Regulation 2024/1773[2].

The personalization and physical delivery of a physical payment card is not an ICT service, but **the outcome of an industrial process independent from the card payment service itself**.

## 3.2. Card personalization is not part of the card payment system

Card payment systems are networked infrastructures operated by a card payment scheme and other accredited actors. Moreover, their individual hardware and software components as well as processing networks are owned by different payment service providers and eventually outsourced to third parties. All of them need to be able to interact in real-time for the card payment service to be provided. Incidents in a card payment system may lead to the degradation or even the interruption of the payment service.

By contrast, card personalization centres do not connect with card payment systems at any time during the Personalization process. Therefore, any incident in a card personalization centre has no impact in the card payment system operation and thus on the provision of the card payment service.

In conclusion, card personalization centres are not information systems that financial entities use to provide financial services to end-users and should not be regulated under DORA.

## 3.3. Card Personalization is an offline process

Card personalization centres are not integrated with any banking ICT system. Banks only send to the personalization centre files containing customer data, which are used for the production of the card. These data are processed offline in order to be personalized into each individual card. The bank's ICT systems cannot be affected by the personalization process in particular because, once the card is personalized, the customer data is deleted and not fed back to the bank.

Moreover, the transmission by the bank of the files containing the customer data to the personalization centre takes place exclusively through a dedicated and protected end-to-end communication link independent from any payment processing circuit.

[2] Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers.

A card personalization centre is not networked, and the personalization process is asynchronous with any card payment system or bank ICT activity. This way to proceed has a very significant impact in terms of reinforcing the security of bank ICT systems.

Thus, any potential disruption of the card personalization process has no impact on the card payment service itself, nor on the bank's ICT systems. The cardholders can continue to pay and/or withdraw cash exactly in the same way. This absence of integration with the bank means that any incident during the card personalization process cannot propagate to the issuer bank, degrading other financial services or creating any systemic financial risk of any kind. At worst, it will result in a delay in the card issuance and shipment process, whereas DORA is about the resilience in the provision of payment services in case of cyber-incident. A very different challenge.

# 4. TO SUMMARIZE

The central concern of DORA is to prevent and counter those cyber-vulnerabilities that may lead to propagate a technical incident or cyber-attack, amplified because of interconnectivity reasons and threatening the availability of a financial service and, worse, creating a systemic risk for the financial system.

The digital operational resilience of financial services constitute the central purpose of DORA and the term resilience is the first definition mentioned in Article 3 (1) of DORA: "*Digital operational resilience' means the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to* ***address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services*** *and their quality, including throughout disruptions;*"

According to this definition in Article 3(1), digital operational resilience refers to networks and information systems required for the continued provision of the financial service, in our case the service of payment using a card.

A card personalization centre is neither a networked infrastructure nor an information system required by banks for card payments to end-users (consumers and merchants) and therefore does not fall under the DORA remit.