Brussels, 13 March 2026
FINAL

EACB Position Paper on the Digital Omnibus

The **European Association of Co-operative Banks** (EACB) is the voice of the cooperative banks in Europe. It represents, promotes and defends the common interests of its 29 member institutions and of cooperative banks in general. Cooperative banks form decentralised networks which are subject to banking as well as cooperative legislation. Democracy, transparency and proximity are the three key characteristics of the cooperative banks' business model. With 2,400 locally operating banks and 35,150 outlets cooperative banks are widely represented throughout the enlarged European Union, playing a major role in the financial and economic system. They have a long tradition in serving 228 million customers, mainly consumers, retailers and communities. The cooperative banks in Europe represent 91 million members and 747,000 employees and have a total average market share of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Table of contents

Introduction

Over the past years, we have seen a significant increase in digital and cyber-related legislation and policymaking. A large number of legislative initiatives have been introduced, many of which are interconnected. This is the case both formally – as the same definitions are often used across different pieces of legislation – and informally, as several regulations address similar topics or apply to the same organisations.

New legislation or legislative proposals have been published in areas such as data, data sharing, payments, digital money, artificial intelligence, cyber resilience and digital identity. It's a fact that the regulatory landscape has become increasingly complex and fragmented, while the penalties for non-compliance are often very significant.

This situation often leads to additional guidance being issued by supervisory authorities, which may not always coordinate with one another before publishing such guidance. In addition, case law from the Court of Justice of the European Union can also influence the interpretation of legislation, potentially leading to evolving interpretations over time.

We therefore believe it is important to ensure sufficient alignment between different legislative initiatives, while keeping the intended policy objectives in mind. Furthermore, we would like to stress the importance of

carefully drafted definitions and legislative provisions, which could reduce the need for further guidance from supervisory authorities or the European Commission.

Digital Omnibus – Data legislative acquis

Comments on the Commission's suggested changes to the data legislative acquis section

The proposed consolidation of existing EU data-sharing rules into a single legal framework is a welcome simplification. It represents a positive step towards improving clarity for stakeholders regarding the requirements for sharing and reusing both public and private data.

Safeguarding intellectual property, trade secrets and sensitive corporate data remains a fundamental requirement. Preventing the mandatory disclosure of such information is key to preserving the competitiveness and strategic autonomy of the cooperative banking sector. In this regard, Article 1(3) of the Digital Omnibus, which introduces additional grounds to refuse the sharing of sensitive data, is a positive development.

In addition, the Digital Omnibus envisages exemptions from certain data-sharing obligations for SMEs and small mid-cap companies. While administrative simplification for smaller actors is an important objective, it should not result in an uneven playing field. Moreover, the sensitivity and strategic importance of data are not necessarily correlated with the size of the entity processing it.

Digital Omnibus – Personal data

Comments on the Commission's suggested changes to the persona data section

GDPR

Generally speaking, we support a balanced approach that preserves the core objectives of the GDPR while improving its workability in practice, especially where overlaps with other digital regulatory frameworks create duplicative or disproportionate compliance efforts.

When it comes to the Digital Omnibus, we overall welcome the changes suggested by the Commission in simplifying the GDPR.

In particular, we welcome the following proposals:

- **Processing of special categories of personal data**: We welcome the amendments introduced by the Digital Omnibus to **Art. 9 of the GDPR** (Art. 3.3 Digital Omnibus), which aim to facilitate the processing of special categories of personal data **for innovation and AI development** purposes, including for training and operating AI systems as defined in the AI Act. These adjustments help strike a more appropriate balance between consumer protection and the economic needs of businesses, without amounting to deregulation and are conducive to strengthening both European competitiveness and sovereignty. We also view positively the proposed derogation allowing the **processing of biometric data** for identity verification purposes under the sole control of the data subject, as this could support

secure digital onboarding and authentication. Nevertheless, further clarification would be desirable regarding the scope of the definition of 'biometric data' under the GDPR and the AI Act, the distinction between 'verification' and 'unique identification' and the conditions under which biometric data can be considered to be 'under the sole control of the data subject'.
In addition, further adjustments to Art. 9 could be considered, such as allowing the processing of special categories of personal data where necessary for the performance or conclusion of a contract and clarifying situations of accidental or incidental processing (e.g., where payment transactions may inadvertently reveal sensitive information, such as donations to religious organisations).

- The proposed implementation of **Articles 12(5)** on conditions and possible fees for data subject requests, **13** on exceptions to information obligations, and **33** on personal data breach notification of the GDPR (corresponding to Articles 3(4), 3(5) and (6), and 3(8) of the Digital Omnibus) could have a significantly positive impact.

- **Automated decision-making (Art. 3(7) Digital Omnibus – Art. 22 GDPR)**: We are positive about the shift from a prohibition on automated decision-making to a framework that allows more room for automated decision-making. For clarity, the wording regarding the 'necessity' requirement and the notion that a decision can be taken 'regardless of whether the decision could be taken otherwise than by solely automated means' (Art. 22.1(a)) should be further illustrated. It should also be clear that controllers are not obliged to disclose internal algorithms, proprietary logic or commercially sensitive business knowledge when responding to data subject requests about automated processing.

With regard to the **use of legitimate interest for AI systems (Art. 3(15) Digital Omnibus – new Art. 88c GDPR)**, the Digital Omnibus proposes to amend the GDPR in order to explicitly allow reliance on legitimate interest as a legal basis for processing personal data in the context of AI-related projects. While the objective of facilitating data use is welcome, the GDPR already provides flexibility for data controllers, by allowing them to determine and justify the most appropriate legal basis over another, depending on the circumstances. In this context, it does not appear necessary or appropriate to specify in the GDPR a dedicated legal basis for the deployment or development of AI systems. **We recommend removing this provision from the Digital Omnibus**. The issue could instead be addressed in the forthcoming guidelines clarifying the interplay between the GDPR and the AI Act.

While the proposed changes represent a positive step, the implementation of the GDPR continues to raise a number of practical challenges for financial institutions that are not fully addressed by the Digital Omnibus. In particular, differences in interpretation and enforcement among national data protection authorities may lead to fragmented application of the rules, creating legal uncertainty for cross-border activities. At the same time, financial institutions must reconcile GDPR requirements with obligations stemming from sector-specific legislation, which may at times create overlapping or potentially conflicting expectations. In addition, supervisory authorities across different policy areas may take diverging views on how data protection requirements should be applied in practice. Addressing these challenges and ensuring greater consistency in the interpretation and interaction of the GDPR with sectoral frameworks would help provide legal certainty while maintaining a high level of data protection.

ePrivacy

We welcome the Commission's initiative under the Digital Omnibus to reduce consent fatigue, particularly regarding cookie banners and access to terminal equipment. Consolidating and harmonizing privacy rules in the digital environment under the GDPR will improve legal clarity and reduce compliance burdens for

businesses while ensuring individuals' rights are protected. At the same time, we consider that this initiative should focus on operational simplification and alignment with the GDPR, without triggering a broader revision of the ePrivacy Directive.

Further changes not addressed in the Digital Omnibus

Data retention and deletion rules

We see room for improvement in the area of data retention and deletion rules. In particular, greater legal certainty is needed regarding the retention of personal data for the purpose of defending legal claims.

While the GDPR establishes the principle of storage limitation under Art. 5(1)(e), companies must also be able to retain data where necessary to establish, exercise, or defend legal claims. In practice, however, strict interpretations of deletion obligations and certain national retention caps may create uncertainty, particularly where statutory limitation periods extend beyond commonly applied retention timelines (for example, seven years under certain national laws).

Deleting data before the expiry of applicable limitation periods may leave companies unable to effectively defend themselves in future proceedings due to the lack of access to relevant evidence. This creates an imbalance between data protection obligations and the right to effective legal protection.
We encourage the co-legislators to clarify, in the context of the revised GDPR, that retaining personal data for the duration of applicable national limitation periods is lawful where necessary for the establishment, exercise or defense of legal claims.

Fraud prevention in ePrivacy

In order to enhance security for users and bank customers, it would be appropriate to introduce an exception to the requirement to obtain consent for read or write operations on user terminals when such operations are carried out for fraud prevention purposes. Fraud continues to generate significant losses for the banking sector, its customers and public authorities. Exempting read or write operations performed for fraud prevention from the consent requirement would therefore strengthen the ability to prevent and detect fraudulent activities. In the same spirit, read or write operations on user terminals carried out for the purposes of combating money laundering and terrorist financing could also benefit from a similar exemption from the consent requirement.

Digital Omnibus – Incident reporting

Comments on the Commission's suggested changes to the incident reporting section

The Single Entry Point

While we understand that the creation of a Single Entry Point (SEP) for incident reporting, covering NIS2, DORA, eIDAS, GDPR, and CER, is intended to facilitate access for both authorities and businesses, with ENISA tasked with designing and developing the interface, further substantive simplification is needed to ensure it does not remain merely a technical solution. Although the SEP may reduce the number of portals that

companies must access, it does not alleviate the substantive compliance burden of navigating overlapping reporting obligations.

In addition, limited attention appears to have been given to the sensitive nature of incident reports and to the need to ensure that information submitted for one competent authority does not automatically become accessible to other authorities via the SEP, either directly or indirectly. Given the sensitivity of such reports, the sharing of information between authorities should only occur where a clear legal basis exists. Strong safeguards should therefore be put in place to ensure that the portal does not disseminate information beyond what is strictly required by law. At the same time, the SEP should be designed in a way that ensures it is easily accessible and user-friendly for reporting entities.

Incident reporting obligations in the financial sector remain particularly burdensome due to the lack of harmonisation between DORA, CRA, NIS2 and PSD2 (future PSR). Financial institutions currently face multiple, sometimes conflicting, reporting requirements across these regulations. Criteria such as incident duration, the definition of major incidents and the treatment of recurring incidents are not applied consistently, leading to confusion and inefficiency. The underlying legal requirements, timelines, content, thresholds and definitions, should be aligned across these frameworks.

Further changes not addressed in the Digital Omnibus

Digital Omnibus should provide a clear exemption from the CRA for financial entities subject to DORA

Given the overlap with DORA, the Digital Omnibus offered a timely opportunity for the Commission to introduce a sectoral exemption for financial services under the Cyber Resilience Act, which was not pursued. The co-legislators now have the opportunity to address this.

While the CRA introduces horizontal cybersecurity requirements for products with digital elements, DORA establishes a comprehensive and sector-specific resilience framework tailored to the financial sector that achieves the same objectives. It covers the full lifecycle of digital products and ICT systems, from development and deployment to maintenance and to decommissioning, and includes robust requirements on risk management, incident reporting, vulnerability management, third-party risk, testing and customer communication. The DORA Regulatory Technical Standards adopted by the ESAs' Joint Committee further specify these requirements and form the basis for Commission Delegated Regulations, ensuring a high and consistent level of cybersecurity protection.

Introducing additional obligations under the CRA would create unnecessary duplication, documentation burdens and compliance costs for entities already subject to DORA, which in many respects ensures an equivalent or higher level of protection. For example, a retail mobile banking application, as well as other digital products used in banking, is already fully subject to DORA's ICT risk management and operational resilience requirements.

We believe that products with digital elements forming part of the network and information systems or ICT assets falling within the scope of DORA meet the conditions for exemption under Art. 2(5) of the CRA. An explicit exclusion is necessary to avoid redundant and resource-intensive overlaps and to ensure legal certainty for financial entities, for example by clarifying that:

'Regulation (EU) 2024/2847 shall not apply to products with digital elements that form part of the network and information system or ICT assets falling within the scope of Regulation (EU) 2022/2554 (DORA)'.

Other point for consideration

Call for clear recognition of DORA as *Lex Specialis*

In the broader discussion on simplification, we want to once again stress the importance of **better coordination between national authorities responsible for NIS2 and DORA**. We are concerned that in some Member States this coordination remains insufficient, resulting in duplicate incident reporting obligations for financial institutions. This creates unnecessary operational burdens and legal uncertainty, despite DORA being recognised as *lex specialis* over NIS2.

To address this, we encourage the Commission, particularly DG CNECT, in collaboration with DG FISMA and the ESAs, to provide clear guidance to national authorities to ensure consistent recognition of DORA as *lex specialis*.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Financial Markets, Payments, Digitalisation (marieke.vanberkel@eacb.coop)
- Ms Chiara Dell'Oro, Director for Digitalisation (chiara.delloro@eacb.coop)