

DIGITAL OMNIBUS PACKAGE: WILL IT BOOST INNOVATION?



**JANUŠ
KIZENEVIČ**

Vice Minister – Ministry
of Finance of the
Republic of Lithuania

Digital Omnibus: unlocking innovation while safeguarding trust

For the past few years, words like simplification and proportionality, competition, protection have dominated the EU debate on regulation. On the one hand, the EU's regulatory framework – particularly in financial services – is often seen as excessively complex and difficult to navigate. On the other hand, this framework has ensured strong consumer protection and legal certainty for businesses. The key question is therefore where to draw the line between necessary protection and harmful overregulation, and how the EU can foster more competition while preserving trust in its financial system.

In this context, the Digital Omnibus Package is a crucial development. It represents an effort to streamline and rationalise the dense layer of digital rules shaping how banks, insurers or Fintech firms operate across the Single Market. In financial services, this is especially

relevant because firms currently face overlapping obligations stemming from frameworks such as GDPR, the AI Act, DORA and NIS2, which have created administrative burdens, legal uncertainty and high compliance costs – particularly for smaller Fintechs and cross-border services providers. By proposing simplified incident reporting, clearer rules on data use for innovation and greater regulatory coherence, the Omnibus aims to make it easier for financial firms to scale digital services EU-wide while still operating within a solid regulatory framework.

At the same time, this raises complex issues. Financial institutions are subject to extensive regulation because they protect and manage financial data, influence the allocation of financial resources, and underpin the stability and functioning of the financial system and the wider economy. Excessive deregulation could increase risks for consumers and the broader economy. Yet it is also true that EU financial regulation has become so complex over the last 15 years that it can hinder innovation and make cross-border expansion extremely difficult. Divergent national interpretations of EU rules further exacerbate this problem, creating de facto barriers within the Single Market and adding to companies' compliance costs.

The Omnibus is expected to reduce legal uncertainty and compliance friction that currently constrain digital innovation in financial services. Greater clarity around data use should enable wider deployment of AI-driven risk assessment, fraud detection and personalised services, while more consistent interaction with the AI framework provides firmer ground for automated decision-making in areas such as creditworthiness and compliance monitoring. Better alignment between horizontal digital rules and sector-specific regimes such as DORA and NIS2 should ease overlapping cybersecurity and incident-reporting obligations. Overall, the result should be a more coherent and predictable digital rulebook, strengthening both innovation capacity and trust in the EU financial sector.

The Package comes with its criticisms. Some say that financial services providers already hold massive power over the daily lives of our people, businesses and economies. They gather data, know patterns and decide who

gets financing – thus, it is no wonder that we should regulate them. Failure of these institutions would have significant impact on the whole economy. The rising powers of multinational tech companies and AI driven solutions should be controlled to protect the consumers. However, over the last 15 years the financial services regulation was made stricter than ever before making it more challenging to compete on global scale or even in several EU member states. Inconsistent national application of EU rules has created invisible barriers within the Single Market, compounding the administrative burden. Easing some of the regulations, simplifying the reporting requirements could help them do businesses, scale in the EU and globally without sacrificing the consumer and economy protection.

**The EU must pair strong
consumer protection
with rules that still allow
innovation to scale.**

In this respect, tools such as the Digital Fitness Check could play a constructive role by identifying where rules are genuinely problematic and where simplification is most needed. By involving both industry and consumer representatives, this process could help strike a better balance between competitiveness and protection.

In sum, EU financial regulation has been strict for good reasons, but it has also become overly complex and fragmented. This makes it harder for new firms to emerge, innovate and scale across the Union. The Digital Omnibus Package is a step in the right direction, but it must go beyond superficial adjustments if it is to truly strengthen the competitiveness of the EU financial sector. The EU must pair strong consumer protection with rules that still allow innovation to scale.



CHRISTOPHER P. BUTTIGIEG

Chief Officer Supervision –
Malta Financial Services
Authority (MFSA)

Beyond simplification: the EU's quest for digital autonomy

In November 2025, the European Commission published the Digital Omnibus proposal, which constitutes a legislative initiative aimed at refining the Union's digital architecture. The proposal mandates substantial revisions to foundational data protection, privacy, and cybersecurity frameworks and facilitates critical updates to the AI Act, reflecting an evolving regulatory stance toward automated systems. While the package purports to streamline existing mandates, it notably omits a dedicated framework for technological sovereignty. This omission is particularly significant given the current geopolitical shifts, where the EU's strategic autonomy and digital resilience are increasingly predicated on reducing systemic dependencies, a pressing concern that remains unaddressed by these specific legislative updates.

The prevailing European digital framework is a manifestation of successive regulatory waves designed to mitigate specific policy exigencies rather than an architecture derived from an integrated, ex ante design principle. Initial efforts centred on data governance and the preservation of fundamental

rights, a phase that culminated in the horizontally applicable GDPR. This was followed by a shift toward market liberalisation and competition, notably through PSD2 and associated open banking reforms. Subsequent activity pivoted toward systemic stability and cybersecurity, producing the NIS2 and the DORA, while more recent interventions have extended oversight to nascent technologies via the MiCA regulation and the AI Act.

Because each regulatory stratum pursued legitimate socio-economic objectives without consistently displacing previously established obligations, the Union has developed a cumulative ecosystem defined by overlapping jurisdictional scopes. Consequently, regulatory density arises not merely from the volume of rules, but from the absence of a unifying integrating principle. This has resulted in a landscape where for example operational resilience is governed simultaneously by horizontal cybersecurity mandates and sector-specific protocols.

Building upon this structural analysis, the 2024 publication of the Draghi Report served as a critical catalyst for reform, underscoring an exigent requirement to fortify the Union's global competitiveness. In response, the European Commission has articulated a renewed commitment to catalysing digital innovation, primarily through regulatory simplification and burden reduction. This strategic direction is formalised within the Political Guidelines for 2024–2029, which elevate "competitiveness" to a primary strategic priority and emphasise the imperative of securing a leadership position in the global artificial intelligence hierarchy. Central to this vision is a balanced and efficacious approach to data accessibility, predicated on the recognition of data as a foundational driver of innovation, particularly for the optimisation of financial services.

The emergent strategy endeavours to synthesise a more transparent, coherent, and market conducive data framework without compromising established privacy and security standards. Within this context, the Digital Omnibus proposal represents the inaugural phase of a broader effort to optimise the application of the European digital rulebook. By introducing a series of targeted technical amendments across an expansive corpus of digital legislation, the initiative seeks to provide immediate relief to commercial entities and public administrations alike. The primary objective is to reduce the "cost of compliance" while maintaining the integrity of original policy goals, thereby

transforming regulatory adherence from a fiscal drain into a distinct competitive advantage for compliant enterprises.

Nonetheless, while these efforts toward simplification are necessary, the current geopolitical volatility necessitates a more fundamental paradigm shift in the European approach. The European economy, particularly the financial sector remains profoundly reliant on extra-territorial digital infrastructures, characterised by a prevalent dependence on United States based cloud providers, software ecosystems, and AI platforms. This structural reliance precipitates significant concentration risks and strategic vulnerabilities that transcend conventional antitrust or competition concerns.

EU Digital Simplification and the Quest for Sovereignty.

Ultimately, simplification and burden reduction must, therefore, be coupled with a robust strategy for technological sovereignty. Without a concerted effort to foster domestic technological capacities and decouple from singular external providers, the Digital Omnibus risks being a procedural fix for a structural crisis. To achieve genuine resilience, the Union must ensure that its digital governance is not merely efficient and unburdened, but fundamentally autonomous in the face of shifting global power dynamics.



ANNA DUNN

EMEA CFO & UK CEO –
JPMorgan Chase & Co.

Regulation squared: sector and horizontal

The Digital Omnibus package is an explicit recognition from the European Commission that there is a need to simplify digital regulations. Yet the package does little to address the most unhelpfully bureaucratic aspect of the current EU digital acquis for financial services, namely the overlap and duplication between horizontal and sector-specific rules.

Financial regulators were ahead of the curve seven years ago with their focus on operational and technology risks. But the Commission has now published a raft of digital rules targeting the same risk as financial services regulations. The result? **The sector is having to manage the same risks in two different ways**, leading to significant additional complexity and expense that will hurt European bank competitiveness and obscure real risk amongst paperwork.

The Council has already recognised the risk of overlap between horizontal and sector-specific rules and urged the Commission in 2024 to avoid duplication and overlap.¹ However, unless finance ministries and regulators are now willing to make an intentional effort to solve this problem it will continue and the EU financial sector will be the worse for it.

So where should the Omnibus be focused to reduce duplication and thereby achieve meaningful simplification?

CRA

The most egregious duplication is the inclusion of the financial sector in the scope of the Cyber Resilience Act (CRA). The Digital Operational Resilience Act (DORA) only came into effect in January 2025 and already the sector is being subjected to a parallel set of requirements. DORA already regulates the ICT assets and systems of a financial entity, known as products with digital elements and remote data processing in the CRA's language. And mapping between the CRA and DORA shows nearly complete overlap in the security controls they require.

What does double regulation get us? Additional supervisors, additional documentation, additional incident reporting, additional compliance processes, additional governance. But no additional risk management.

The CRA has a built-in mechanism for just this situation in the form of an article allowing the Commission to exempt sectors subject to equivalent regulations. This has been used for several sectors already such as automotive and airplane manufacturing. However, the financial services sector to date has not been considered for exemption, despite the irrefutable overlaps in scope.

Not that DORA is perfect. It remains far too focused on documentation rather than risk. DORA requires an annual review of the entire ICT risk management framework; it requires incidents to be classified and reported under a dizzying array of criteria and thresholds such as geographic spread and duration that often do not correlate to an incident's severity. Inevitably in something so complicated, firms are over-reporting and authorities are receiving a level of reporting far in excess of what would provide meaningful supervisory information and signalling. Rather than wait four years to address these issues in the DORA statutory review, we should take advantage of any second digital omnibus package to tackle them now.

AI

Similar overlap between horizontal and sectoral regulation is being assessed explicitly for AI. The European Banking Authority's (EBA) work last year on mapping the interactions² between the EU AI Act and financial sector legislation is a welcome step in understanding where burden can be alleviated for financial institutions.

The EBA finds – perhaps unsurprisingly – that there are areas of overlap between banking and payments legislation and

the AI Act sufficient to warrant the consideration of derogation from certain obligations. I would echo the letter from EBA Chair Campa to DG FISMA³ and urge the Commission to seriously consider introducing derogations from certain obligations where appropriate.

The sector is having to manage the same risks in two different ways.

Conclusion

Financial authorities were early to prioritise operational and technological risks. But the digital acquis has now caught up. The sector increasingly faces overlapping and duplicative regulation covering the same risks. The simplification agenda must urgently address this unnecessary and unhelpful complexity, one that is driven primarily by a failure to coordinate and agree between sector-specific and horizontal rules. The prospects for “ever closer” European Union are bleak indeed if basic coordination cannot occur inside the Brussels Ring.

1. <https://data.consilium.europa.eu/doc/document/ST-10133-2024-INIT/en/pdf>
2. <https://www.eba.europa.eu/sites/default/files/2025-11/d8b999ce-afd9-4964-9606-971bbc2aaf89/AI%20Act%20implications%20for%20the%20EU%20banking%20sector.pdf>
3. <https://www.eba.europa.eu/sites/default/files/2025-11/2019d1b5-59f8-4149-ad3b-23cfd4388a1/EBA%20Chair%20letter%20to%20Mr%20Berrigan%20and%20Mr%20Viola%20on%20outcome%20of%20EBA%E2%80%99s%20AI%20Act%20mapping%20exercise.pdf>



NADIA FILALI

Chief Innovation Officer –
Groupe Caisse des Dépôts (CDC)

Digital Omnibus: digitalisation of finance and capital market integration

As a long-term public investor, Caisse des Dépôts views the Digital Omnibus Package not merely as a simplification exercise, but as a test of Europe's ability to reconcile regulatory ambition with market integration. Aligning the EU digital framework with competitiveness and strategic autonomy is essential; ensuring that it enables the scaling of AI and tokenisation of assets across borders is equally critical. In that sense, simplification becomes a strategic lever rather than a procedural adjustment, and a first step toward capital markets integration.

The Omnibus addresses structural frictions that have constrained digital transformation in finance.

Regulatory overlap and cumulative compliance burdens have generated legal uncertainty and operational complexity. The interaction between GDPR, the AI Act, DORA, NIS2, eIDAS and the Data Act has resulted in duplicative reporting and inconsistent supervisory expectations, particularly for cross-border institutions. The creation of a cybersecurity single reporting gateway via ENISA, deadline extensions and lighter documentation requirements for SMEs and Small Mid-Caps are pragmatic steps that reduce fragmentation. For financial

actors operating across Member States, such rationalisation is not marginal: it directly affects investment capacity and competitiveness.

Access to and use of data is another structural bottleneck for AI deployment. Clarifying anonymised data and enabling reliance on “legitimate interest” for model training can facilitate responsible AI applications in credit risk modelling, anti-money laundering and fraud detection. These use cases are not peripheral: they underpin pricing accuracy, risk management and ultimately capital allocation efficiency. However, legislative simplification must be accompanied by harmonised supervisory guidance and coordinated enforcement to avoid divergent national interpretations that would fragment the Single Market.

Distributed ledger technology and tokenised assets illustrate both the progress made and the limits of the current framework. Although the EU acted early with MiCA and the DLT Pilot Regime, restrictive thresholds and complex authorisation procedures have limited practical uptake. Outside the Pilot Regime, post-trade legislation still provides insufficient legal certainty for DLT-based issuance and settlement. Yet tokenisation has the potential to reduce issuance, custody and settlement costs while broadening investor access across borders – a direct lever for deeper and more efficient European capital markets. The Commission's “Market Integration Package” moves in the right direction by raising caps and reinforcing technological neutrality in settlement rules, while centralising supervision of crypto-asset service providers at ESMA level. Further operational clarity will nevertheless be required to ensure that tokenised instruments can scale under predictable and proportionate conditions that genuinely support integrated European markets.

certain stablecoins, even where their economic risk profile is comparable to traditional instruments. A more technology-neutral approach, grounded in underlying risk rather than legal form, would reduce distortions between tokenised and non-tokenised assets and support responsible innovation without compromising financial stability.

More broadly, simplification must translate into supervisory convergence. Divergent national interpretations risk reintroducing fragmentation despite EU-level streamlining. Coordination between ESMA, the other European Supervisory Authorities and national authorities is therefore essential to ensure a level playing field.

The forthcoming Digital Fitness Check offers an opportunity to strengthen systemic coherence. Aligning core definitions across GDPR, the AI Act, DORA and NIS2 and reinforcing proportionality would reduce interpretative risk and compliance uncertainty. Digital legislation should increasingly be assessed not only through the prism of protection and resilience, but also in terms of its contribution to cross-border capital formation and market depth.

Ultimately, simplification should be understood as strategic calibration rather than deregulation. If properly implemented, the Digital Omnibus can help transform digital regulation from a source of friction into an instrument of financial integration. Its full effectiveness will depend on sustained efforts to ensure that Europe's digital governance framework actively supports the ambition of a deeper, more integrated and innovation-driven Capital Markets Union.

Digital Omnibus turns regulation into a financial digitalisation and integration tool.

Yet regulatory simplification alone will not suffice if structural inconsistencies persist in adjacent financial frameworks. In this respect, prudential treatment remains a decisive issue. The current EU banking framework applies a transitional regime to crypto-assets and, in practice, imposes significantly higher capital and liquidity requirements on