European Financial Services Round Table

November 2025

EFR PAPER ON SIMPLIFICATION PROPOSALS FOR THE NEXT DIGITAL PACKAGE

Executive summary

- The EFR supports the aim to simplify the European Digital Regulatory Framework, addressing the fact that there is too much complexity, and that red tape has to be cut. Furthermore, it is essential for the digital legislations to be reviewed in light of the global geopolitical challenges and the unprecedented technological evolution, which have significantly changed and profoundly transformed our societies since the adoption of these texts.
- Requirements in the various digital legislations and regulations should be straightforward, consistent, coherent, aligned and not overlapping or diverging in order to ensure European businesses' competitiveness and legal certainty. There must also be clear and consistent guidance for regulators across different jurisdictions.
- Concerning AI, it should be taken into account that the financial and insurance sectors are highly regulated and early adopters of AI. In this regard, the financial services industry has been vocal in requesting an extension of one year to implement the obligations related to high-risk AI systems. Clearer guidance and greater predictability on the implementation of the AI Act will help businesses navigate the implementation of that legislation.
- Regulation should support cloud uptake by providing legal certainty, harmonised standards, and security requirements that build trust in cross-border services.

Introduction

By the end of the year, the European Commission will launch a Digital Omnibus package to review, among other topics, cybersecurity legislation, data sharing rules, as well as matters related to cloud and AI. We support plans to simplify its Digital Regulatory Framework for the purpose of aligning European values, such as inclusion, and foster responsible innovation.

To avoid additional or overlapping digital requirements under other legislation or supervisory expectations, the simplification process should ensure the alignment of regulatory / supervisory requirements.

Ensure consistency and legal coherence across EU regulations

Over the past decade, the EU has adopted numerous digital regulations, both horizontal (e.g. Data Act, Artificial Intelligence (AI) Act, Cyber Resilience Act (CRA), General Data Protection Regulation (GDPR), Cybersecurity Act (CSA), Digital Markets Act (DMA) and sectoral (e.g. Digital Operational Resilience Act (DORA)), which interact with and sometimes overlap existing standards. Under the GDPR, for instance, companies already complete Data Protection Impact Assessments (DPIAs). The AI Act introduces "fundamental rights impact assessments" (FRIAs), involving a new process with a separate template and trigger. Equally, although the concept of "high-risk" already exists within the GDPR, it is unclear how this definition maps to the definition provided in the AI Act – for instance, where automated processing under the GDPR is high-risk, it is not clear if using AI to inform one part of a decision would be high-risk under the AI Act.

EFR Recommendation:

- Take stock of existing rules and ensure their consistency and coherence, harmonising them where possible.
- Encourage joint guidelines by different EU authorities on converging legislation, e.g. joint guidelines from the EDPB and AI Office on the interaction between Article 22 of the GDPR and the AI Act.

Adopt risk-based, proportionate and innovation-friendly implementation of the AI Act

Clearer guidance and greater predictability on implementation of the AI Act will help businesses navigate implementation of the AI Act and allocate resources more effectively.

The financial and insurance sectors are mature, highly regulated and early adopters of AI. To fully unlock its potential while ensuring its responsible use, there are areas, such as the definition of AI, where we feel it is important to have clarity.

EFR Recommendations:

- **Clear definition and scope of AI.** The definition of an AI system under the AIA is centred on the system operating autonomously and the ability of a system to work out how to generate outputs such as predictions that can influence environments. Our sectors use numerous low-autonomy models based mostly on traditional statistical methods, e.g. general linear models such as linear and logistic regression, which lack these abilities. The AI Act should provide clear distinctions between high-risk autonomous systems and traditional models to ensure proportional regulation. Although current guidelines have already addressed this issue, EFR supports clear validation of this view by financial regulators.
- **Supervisory architecture -** to ensure clear, consistent and effective oversight of AI, financial authorities should be promptly confirmed as AI market supervisors. Additionally, the AI Office should include financial and insurance supervisors when coordinating the development of secondary legislation and guidelines by financial regulators in order to prevent fragmented supervision and conflicting interpretations.
- **Adequate timing for implementation to** allow flexibility and take account of the delay in publishing guidelines and standards related to high-risk AI systems.

For upcoming efforts concerning Digital simplification, EFR identifies the following key areas:

Streamline DORA reporting requirements

The next Digital Omnibus should be based on a thorough analysis of requirements to identify areas where it is possible to reduce the administrative burden of the cyber incident reporting under DORA. For example, this can be achieved by creating a common European (cyber) incident report template that can be used within all reporting regimes (e.g. DORA, GDPR) irrespective of whether the reporting entity is subject to all reporting regimes. Such a common report template should replace - as a single joint report template - the other current templates and not be an additional template over and above those currently in existence. More broadly, it is also an opportunity to take stock of DORA's overall reporting burden. This should include reviewing the volume of information sent to authorities, how this data is used and opportunities to streamline this, particularly by prioritising and significantly reducing the number of data points required from firms under DORA so that they remain focused on the key risks.

Overlap and duplication of reporting, e.g. CRA/ DORA/ Cyber Security / NIS II

Financial institutions already comply with DORA's strict cybersecurity and resilience rules. The Cyber Resilience Act (CRA) introduces requirements such as vulnerability management and incident reporting, applying to products with digital elements, and any remote data processing needed for functionality. The depth of data processing required to support financial sector applications (e.g. retail banking platforms, investment tools) means the CRA effectively applies to a large portion of back-end IT infrastructure, which is already governed by DORA. This adds complexity and legal uncertainty for FIs, without improving security.

In addition, under NIS2, financial institutions can be asked to register with national cyber authorities, which could result in overlapping reporting obligations. Given that DORA acts as a *lex specialis* to NIS2, areas specifically regulated by DORA should not come under the jurisdiction of NIS2.

EFR Recommendations:

The Commission should use its powers under Article 2(5) of the Cyber Resilience Act to adopt a delegated act that excludes financial sector products already covered by DORA. DORA provides cybersecurity and resilience standards that are equal to or higher than those in the CRA. This exclusion would:

- Prevent overlapping regulation of back-end IT infrastructure used in financial services.
- Simplify compliance for financial institutions.
- Align with the EU's broader objective of streamlining cybersecurity rules without compromising resilience.

When engaging with Member States on the transposition of NIS2, the Commission should encourage national authorities to account fully for DORA's role as lex specialis to NIS2 and urge them to avoid overlapping obligations, such as duplicative registration requirements for financial institutions. This approach will help financial institutions to comply more efficiently and avoid unnecessary administrative burdens.

Targeted adjustments concerning the General Data Protection Regulation

While we note that the Digital Omnibus does not mention the GDPR, it is important that, in the context of the simplification of the digital acquis, GDPR is considered for the reasons outlined below.

The GDPR marked a new era for data privacy in 2018, driving major changes and investment across businesses in the management and protection of personal data. Since its adoption, a key criticism has been the significant administrative burden it places on companies, demanding substantial resources to ensure compliance. In addition, given the rapid evolution of the digital world to be addressed, simplification efforts by the European Commission are timely and appropriate.

EFR Recommendations:

- **Recognition of group concept in the GDPR.** The GDPR does not specifically recognise the concept of a corporate group (usually including a parent company and numerous subsidiaries worldwide), forcing firms to rely only on Binding Corporate Rules for streamlined privacy. To allow for simplification and competitiveness, the GDPR should provide clearer guidance for global and multinational companies, which adhere to the same strict principles group-wide.
- **More coordination between the different authorities addressing fragmented implementation and enforcement of the GDPR**

  Although the GDPR is directly applicable, it allows Member States to rule on several topics, causing fragmentation and legal uncertainty. Each Member State also has at least one Data Protection Authority, which can interpret the regulation differently, and existing coordination mechanisms often fail. The EDPB should play a stronger harmonisation role, with national authorities handling local matters. Alignment between data protection and AI Act authorities is also crucial.
- **Current and future regulation does not hinder innovation**

  The European Data Protection Board (EDBP) as set out by the GDPR should take current technological and economic challenges into consideration: this means requesting greater consideration of business feedback when preparing consultation processes for EDPB Guidelines, ensuring that the private sector is better represented and opening EDPB bodies to private actors. This would allow guidelines that are more adapted to business processes and technological developments.

  Furthermore, the EDPB should demonstrate clarity and conciseness in its publications. By focusing solely on data protection, it will be a hindrance to encompassing economic data, as well as technological and technical developments.

  Certain practices to confirm identity as part of the AML process are understood to be inhibited due to GDPR concerns. The GDPR is a barrier to the development of permissionless blockchains, which are emerging as a key technology for digital assets. At the minimum, guidance on the application of the GDPR to emerging technologies should seek to enable their responsible use rather than limit their uptake. A more fundamental review of the GDPR may also be required.
- **Clarify the GDPR minimisation principle in relation to other legislative frameworks**

  The GDPR data minimisation principle (collect only data that is strictly necessary for the purpose at hand) creates problems for financial institutions when trade-offs need to be made between this principle and other frameworks requiring the collection and sharing of data. This includes (but is not limited to) PSD2 (sharing of data by ASPSPs to AISPs) and IPR (Verification of Payee requires the presentation of the payee's full name, which in some cases sits uncomfortably with data minimisation). The supervisors involved often have diverging views, based on the framework they are enforcing. This results in a lack of legal clarity or outright conflicting requirements.

Cloud

Cloud services are increasingly becoming the backbone of Europe's digital economy, enabling businesses, public authorities and citizens to access scalable computing power, secure data storage, and advanced applications that drive innovation and competitiveness. For the EU to meet its long-term competitiveness objectives, cloud adoption must be encouraged actively through smart regulation. As Mario Draghi[1] cautioned, the EU cannot achieve true digital sovereignty in isolation. Constructive cooperation on transatlantic data flows, certification schemes and security frameworks ensures that European businesses can access and build on world-leading infrastructure without compromising on fundamental rights and strategic autonomy. A stable, long-term and trusted mechanism to overcome the recurring legal uncertainty around data transfers (as seen in Safe Harbor, Privacy Shield, and Schrems rulings) is particularly critical.

[1] The Future of European Competitiveness – A competitiveness strategy for Europe - 9 September 2024.

EFR Recommendation:

- Regulation should therefore support cloud uptake by providing legal certainty, harmonised standards, and security requirements that build trust in cross-border services. Without this, fragmentation in national rules and diverging security standards risk undermining the Single Market.

Cookie rules (ePrivacy)

It is crucial that the envisaged review of the 2002 Directive does not lead to a stronger need for consent collection, particularly in view of the currently widespread "consent fatigue", which risks further reducing the already very low rate of consent. Harmonisation of practices would be key in that perspective, together with the extension of the concept of legitimate interest, in order to limit the need for consent to subjects where the protection of personal data is genuinely necessary.

EFR Recommendation:

- Clarify and standardise the purposes and categories of tracers in order to standardise the information indications in order to enlighten users more effectively and reduce their fatigue.
- Extend the categories of tracers not subject to consent to include tracers whose purpose is to help the person seeking an interaction on the site, or to protect customers.

Electronic identification and implementation of the digital wallet (eIDAS)

The roll-out of digital identity should enable the modernisation and streamlining of remote and branch banking and financial processes, and even the security of certain transactions. To ensure that, although technical discussions are already underway, clarifications are required regarding certain aspects of the eIDAS revision, together with a more realistic timetable for its implementation.

EFR Recommendation:

- Clarify the respective responsibilities between digital identity providers, banks and customers in the event of a proven malfunction of the Digital Identity Wallet.
- Clarify the definitions of 'online' and 'identification' by using the definitions from European Directive (EU) 2015/1535.
- Align application schedules between eIDAS v2 and PSR/PSD3.
- Maintain a consistent reading of authentication requirements (SCA& SUA) for payment service providers (PSPs).

The European Financial Services Round Table (EFR) was formed in 2001. The Members of EFR are Chairs and Chief Executive Officers of international banks or insurers with headquarters in Europe. EFR Members believe that a fully integrated EU financial market, a Single Market with consistent rules and requirements, combined with a strong, stable and competitive European financial services industry will lead to increased choice and better value for all users of financial services across the Member States of the European Union. An open and integrated market reflecting the diversity of banking and insurance business models will support investment and growth, expanding the overall soundness and competitiveness of the European economy.