FESE response to the Commission Consultation on the Digital Fitness Check

10th March 2026

Introductory questions

Q1: Do you give the European Commission's services permission to contact you for follow-up discussions or events related to the topics covered in your submission?

☒ Yes

☐ No

Opportunities supported by the Digital Rulebook

Digital rules have been instrumental in framing a fair business environment in the EU. They established a true single market for digital services instead of a fragmented business environment across Member States, promoting the competitiveness of businesses across the EU. Europe has pioneered digital regulation, and has set the gold standard for the highest level of protections for fundamental rights, consumer safety and the protection of our values. Hereafter, the 'digital rulebook' or 'digital rules' are understood broadly as the body of EU legislation with a significant digital angle and its implementation. Examples include, but are not limited to, rules on data, artificial intelligence, telecommunications services, regulations on online platforms and digital services, media services, cybersecurity or privacy of communications.

For businesses and organisations:

Q2: How has the EU's digital rulebook created opportunities or otherwise positively impacted your business?

Q3: Identify the 3 pieces of EU regulation holding a digital angle that have had the largest impact on your organisation. This will inform the European Commission's scoping and prioritisation of the legal framework to be analysed more in-depth in the Digital Fitness Check. If you are not familiar with the names of specific legislative acts, you may refer instead to policy areas or domains.

The three EU regulatory initiatives with a digital angle that have had the largest impact on our membership include:

- **The Digital Operational Resilience Act (DORA),** which focuses on cybersecurity, ICT risk management, and incident reporting frameworks in the finance sector. DORA has required substantial internal organisational and operational changes.
- **EU regulatory initiatives governing distributed ledger technologies and crypto-assets,** including sector specific DLT-related amendments to existing financial services

frameworks such as MiFID II/R and CSDR, the experimental sandboxes such as the DLT Pilot Regime, and the Markets in Crypto-Assets Regulation (MiCA).
- **Horizontal legislation governing AI, such as the AI Act,** which sets requirements for the use and governance of artificial intelligence systems, AI risk classification, etc.

For all respondents:

Q4: What do you consider to be the most important achievements of the EU-wide digital rulebook? Please explain.

Q5: What are the benefits for cross-border trade within the EU supported by the application of digital legislation?

☐ Increased market access

☒ Regulatory consistency

☒ Legal certainty

☒ Access to EU digital infrastructures

☐ Competitive pricing

☒ Rights protection

☒ Enhances safety and quality

☐ Increased innovation

☐ Other

Please explain your experience related to the previous question and/or elaborate on 'Other'.

What are the benefits for cross-border trade with non-EU countries supported by the application of digital legislation?

Digital regulation creates a secure and predictable environment for services to be exchanged between EU and non-EU entities by providing clear legal guidelines.

Challenges and areas where further analysis and optimisation of the rules are needed

The Draghi and Letta reports highlight that the accumulation of rules has sometimes had an adverse effect on competitiveness. Fast and visible improvements are needed for people and businesses, through a more cost-effective and innovation-friendly implementation of our rules – all the while maintaining high standards and core objectives of the rules.

The first step is a 'stress-test' of the rules, to see their real-world impact, not just in isolation, but in the way they are applied together by businesses, administrations and other organisations, and how they achieve their goals.

Based on the preliminary views received from stakeholders on the margins of the consultations for the Digital Omnibus, there is a need for a wider analysis on the interplay between laws for example as regards the data acquis of the EU, or more recent rules applicable to cybersecurity or to online services and sector-specific rules.

Q6: What are, in your opinion and experience, areas of digital law where there is scope for making key improvements? Be as precise as you can. Please highlight, where possible, the aspects specifically relevant to SMEs.

1) **Digital Omnibus**

While further simplification would have been beneficial, we welcome the introduction of a Single Entry Point for incident reporting across multiple legislative frameworks, including DORA, the NIS 2 Directive, eIDAS, CER, and the GDPR, as a positive step towards streamlining reporting obligations.

2) **Cybersecurity Package**

While acknowledging ENISA's important role in strengthening the EU's cybersecurity landscape, we caution that an excessive reinforcement of its powers could create concentration risks and may affect the EU's attractiveness for non-European service providers, including global cloud service providers. We therefore underscore the importance of ensuring that governance arrangements strike an appropriate balance between effective oversight and the preservation of an open, competitive and non-discriminatory internal market.

Q7: To what extent do you perceive overlaps, conflicts, or redundancies between the EU digital legislation and sector-specific EU regulations in your area of activity? Please provide examples and elaborate on aspects you find problematic.

From the FESE perspective, we observe several overlaps between sector-specific legislation such as DORA and horizontal regulation such as the NIS 2 Directive and the Cyber Resilience Act. Our longstanding position is to support the use of DORA as the reference framework for ICT security in the financial sector, and we therefore welcome recital 16, which recognises that DORA constitutes *lex specialis* to the NIS Directive. However, we would recommend ensuring consistency when streamlining all horizontal legislation. With regard to overlaps, we observe the following aspects:

1) **DORA and CRA**

The Cyber Resilience Act (CRA) and DORA both aim to increase the cybersecurity and resilience of the EU economy, one through the lens of products with digital elements (PDEs) and the other via the ICT systems of financial entities. CRA provides requirements for economic operators of PDEs such as manufacturers and distributors, while DORA focuses on financial entities receiving ICT services. Overlap may arise in specific scenarios, for instance when a product (e.g. software or hardware) constitutes the performance object of an ICT service provided by one financial entity to another, and simultaneously qualifies as a PDE under CRA. In such cases, the scope of both regulations may overlap, potentially resulting in duplicative compliance obligations.

Proposal: Propose a targeted exemption in the CRA for PDEs that are designed and provided by a DORA financial entity to another financial entity as part of the provision of an ICT service within the meaning of DORA.

2) **DORA and NIS2**

DORA and NIS2 have introduced cybersecurity frameworks that led to extensive reporting and auditing obligations, with a particular emphasis on third party risk management. However, misalignment between the two frameworks has led to fragmented oversight, and increased compliance burdens. A small number of major ICT providers dominate the market, creating systemic risk and forcing tens of thousands of regulated entities (20.000

DORA regulated entities and 100.000 NIS2 regulated entities) into repetitive negotiations over similar contractual terms. Furthermore, financial institutions and ICT service providers are frequently subject to inconsistent reporting requirements from different national competent authorities (NCAs). Greater alignment between the DORA and NIS2 frameworks would be essential to streamline oversight and reduce duplication.

Proposal: Uniform contractual terms on operational resilience would remove the need for thousands of financial institutions to negotiate separately with a small number of ICT providers, and a standardised template would streamline agreements.

Better alignment between DORA and NIS2 could be achieved through joint auditing standards and mutual recognition of certifications. To address provider concentration risk, oversight should be harmonised through accredited audit regimes based on common standards. Unlike pooled audits under DORA, accredited audits would allow providers to undergo one annual audit and share the results with all regulated clients, avoiding the inefficiency of thousands of parallel audits.

While DORA already foresees the possibility of pooled audits, accredited audit regimes would allow service providers to mandate an annual audit by an accredited audit firm and to provide the results to its respective regulated service receivers. This would be a significant improvement in comparison to thousands of entities trying to execute the same audits on the same dozen providers.

3) EBA Guidelines on non-ICT risk of third-party service providers (TPSPs)

The proposed EBA Guidelines would significantly expand the scope of services subject to regulatory requirements. Almost all non-ICT third-party arrangements, including intragroup third-party service providers, would fall within the scope.

The Guidelines would not only cover material non-ICT services but also extend to the procurement of other third-party services which do not have a material impact on financial entities' risk exposures or their operational resilience (e.g., "Advertising & Marketing", "Document Management & Archiving", "Postal services & Mailing" "Talent acquisition & hiring", as well as advisory services).

Significant expansion in scope would not only result in high costs for the regulated entities, which would need to perform the required risk assessment, negotiate contractual terms and perform the monitoring for these providers, it could also lead to many suppliers not being able to provide services to financial entities anymore. For example, a small marketing agency may not have the resources to comply with numerous and stringent regulatory requirements.

Such expansion runs counter to the Commission's simplification agenda, placing disproportionate burden on financial entities and their supplies (especially SMEs), without delivering commensurate resilience benefits.

Proposal: To avoid a significant increase of the regulatory burden, the Guidelines should explicitly exclude functions that are either legally required to be performed by a third-party service provider or are typically performed by a supervised enterprise and are not regularly carried out by the financial entities themselves. Examples include, but are not limited to, the use of central bank functions, liquidity lines, or publicly accessible (also fee-based) data from market information providers (e.g., rating agencies).

Likewise, services provided by financial institutions for another financial institution should also be out of the scope, as those services are regulated by extensive sectoral frameworks.

Moreover, to ensure consistency of non-ICT services with the interpretation of ICT services under DORA, the Guidelines should confirm that regulated financial services, including ancillary services provided by licensed financial entities to other financial entities, are

not in scope. These services are already subject to robust sectoral regulation, guaranteeing a high level of operational resilience and management of the risks associated with the provision of the respective financial services.

As the scope of covered non-ICT services is broad in nature and thus contractual requirements may diverge largely, it is even more important that financial entities are in a position to adapt contract requirements on a risk-based basis rather than to implement mandatory contractual requirements which may not suit the individual requirements.

Lastly, it would be highly cost-inefficient if each financial entity were required to conduct its own supplier audits. Instead, third-party audits should be leveraged in a standardized and widely recognized format – preferably aligned with the established frameworks such as ISO certification. This would reduce unnecessary costs to the industry without jeopardizing industry-wide resilience.

However, we caution against introducing eligibility criteria that could limit the pool of eligible providers to only those who are certified to provide services to the financial sector; or that could lead to unjustified cost premiums charged by financial industry-certified service providers.

Q8: To what extent do you perceive overlaps, conflicts, or redundancies between the EU's digital rules and legislation issued by Member States? Please provide examples.

Q9: Are there EU rules or provisions in the digital area that you believe are no longer up to date, or that are obsolete?

Q10: Regarding cross-border trade within the EU, what negative effects do you experience (if organisation, within your sector) from the application of digital EU legislation?

☒ Increased compliance costs

☒ Regulatory fragmentation

☐ Reduced innovation capacity

☒ Market concentration

☐ Slower market entry

☐ Limited consumer choice

☐ Other

Please specify your answer to the previous question.

We would support a 28th Regime for (digital) issuance going forward. Please see our summary of the proposal.

The proposed 28th Regime for digital issuance would:

- address what the current fragmented legal landscape cannot provide: legal certainty as to the issuance requirements applicable to dematerialised debt securities in a cross-border market environment.
- be available for issuances across all Member States of the EU, regardless of the law chosen to govern the rights attached to the relevant securities and regardless of where the issuer has its seat or is operating within the EU.

- be also available in jurisdictions that do not (yet) provide for a legal framework applicable to dematerialised debt securities and that may not (yet) permit the issuance of dematerialised debt securities.
- state that each EU Member State will have to ensure that it provides for a legal framework applicable to dematerialised debt securities and permits the issuance of debt securities in a dematerialised manner.
- pave the way for digital asset issuance legal certainty and growth.

Q11: What are possible negative consequences of the application of digital EU legislation for cross-border trade with non-EU countries?

Based on the preliminary views received on the margins of the consultations for the Digital Omnibus, stakeholders pointed to the need for a more in-depth analysis of elements such as:

- The coherence between specific legal notions, such as definitions, or questions of clarity of obligations and coherence of scope;
- The cumulative impact of rules and potential for further streamlining, in particular where there are duplications of obligations;
- The good practices and challenges in the interplay between the different governance systems of the rules, including cooperation and consultation mechanisms between authorities and EU-level cooperation through Boards and other fora;
- Mechanisms, tools, guidance or experimental practices that bring legal clarity, burden relief or assist in the application of rules in novel areas, supporting innovative practices.

Q12: What areas, if any, do you perceive as incoherent and unclear in terms of concepts used across different laws, definitions, or scope of the rules?

Q13: In what areas, if any, do you consider that changes could be made to optimise the cumulative impact of the rules? In particular, where do you identify, in practice, that obligations in different rules lead to duplications of costs or processes?

Please see our response to Q7.

You can find as an Annex to the Staff Working Document supporting the Digital Omnibus proposal a detailed list of **reporting obligations** identified across major digital EU legislation, including one-off obligations, as well as recurrent reporting requirements.

The Commission has already made proposals for streamlining reporting obligations, for example through the **Digital Omnibus** proposal for cybersecurity and related incident reporting, and for online platforms, with the repeal of the Platform-to-Business Regulation.

In addition to these immediate changes, stakeholders have flagged **other areas** where further streamlining across different horizontal and sector-specific requirements could

facilitate their business operations, for example as regards reports on content moderation decision or risk assessments.

Q14: Are there areas of digital law where you currently identify a disproportionate administrative burden stemming from reporting obligations?

As FESE, we mainly observe several instances of a disproportionate administrative burden in the DORA framework. Please find below several examples:

1) **Simplifying DORA Register of Information**

DORA Register of Information (ROI) was intended to identify and oversee the critical ICT providers on the EU level, by collecting data and publishing a list of providers based on submitted registers. However, the current ROI template prescribes 95 data fields for each supplier contract and depending on the number of contracts and sub-contracts, submissions can amount to hundreds of thousands of rows.

For instance, a Central Securities Depository (CSD) must list sub-services as stand-alone licensed activities, multiplying function identifiers and entries. The implementation costs alone have been reported at seven digits, with ongoing maintenance and reporting adding further expense to the industry.

Proposal: By introducing a materiality threshold (e.g., based on contract value) to exclude low-impact contracts from the ROI reporting, or simplifying function identifiers, such as consolidating CSD sub-services under a single category, unnecessary reporting costs would be significantly reduced without compromising oversight. In a further step, in line with the Commission's simplification and burden reduction agenda, regulators could clarify the "ad-hoc basis" for reporting requests to avoid unrealistic timelines that increase complexity and consider annual reporting of a high-level supplier list rather than thousands of rows of granular contractual details.

In addition, whilst cross-border groups of financial entities belonging to the same category (e.g. credit institutions) could benefit from simplified reporting requirements (e.g. consolidation of register of information) this is not the case for market infrastructures belonging to the same group since there is no single supervision and consolidation of reporting requirements is not allowed by NCA.

Proposal: To simplify the reporting obligation for groups of market infrastructures. The Commission could propose the adoption of specific provisions allowing such consolidation that would avoid the duplication of reporting requirements.

2) **DORA ITS on major incident reporting**

Financial entities located in different member states are not allowed to aggregate incident reports even if they belong to the same group and share the same ICT infrastructures. Amending this framework by allowing trading venues to submit aggregated notifications of incidents would reduce the regulatory burden on entities that operate in several member states and allow for a clearer, more consistent response across all impacted markets. It would also reduce the likelihood of fragmented or inconsistent data being communicated to regulators, which would be provided with a clearer, holistic view of the incident's impact, enabling better detection of systemic risks and faster, more coordinated responses.

Proposal: To simplify the reporting obligation for groups of market infrastructures, allowing the possibility to aggregate information for DORA reporting obligations. However, it should be considered as a possibility rather than a requirement or obligation. The Commission could propose the adoption of specific measures to enable such consolidation,

avoiding duplication of reporting requirements. In particular, it is proposed to delete letter d) of Article 7(1), and to delete Article 7(2) of DORA ITS on the reporting of major ICT-related incidents.

Article 5(5) of the ITS specifying time limits for the initial notification, and for the intermediate and final reports should also benefit from the principle of proportionality. The reporting deadline during the weekend represents a disproportionate burden, especially in countries with only one stock exchange, where those trading venues are typically small firms with few employees. Therefore, the reporting deadline during the weekend should only apply to companies above a certain size.

Proposal: As this is an EU-level regulation, the reporting obligation during the weekend for the initial report for trading venues should be classified on the basis of market share in terms of turnover at Union level (see also RTS on thread led-penetration testing (TLPT) Article 2 (2) (f) (ii)) Regulation 2025/1190 and not at national level).

3) DORA RTS on Subcontracting

This technical standard has already been challenged by the Commission (here) and could include further simplification of the requirements on subcontracting. For example, the Commission deleted Article 5 on Conditions for subcontracting which is a welcome development. However, the provisions concerning the entire ICT subcontracting chain remain extremely onerous and risk undermining the EU's competitiveness. The delivery of ICT services relies on a complex network of third-party providers, each of which may depend on additional third-party ICT services. Unlike outsourcing as defined in frameworks like the EBA Guidelines, DORA subcontracting rules apply to any ICT service supporting critical or important functions — even if not formally outsourced. This broader scope, combined with new sub-outsourcing rules, makes third-party management significantly more challenging and may ultimately prompt ICT providers to withdraw from serving the EU financial sector.

Proposal: It could be proposed to limit the layers of ICT- subcontractors for which requirements must be fulfilled (e.g. information-, access- and audit rights, due diligence, register of information, etc.) to certain levels of subcontracting (e.g. 3 layers) instead of focusing on the whole value-chain, and primarily concentrate on ICT subcontractors whose failure could have a material impact on the ICT services received by the financial entity.

Q15: If you are the recipient of reports from businesses or other entities, what are the possibilities for rendering more efficient the forms and ways in which you receive the reports?

Governance models

Q16: What are the good practices you have identified in the governance structure applicable to digital rules? Do you see particularly notable success stories for example when it comes to the cooperation across authorities, coordination in enforcement actions, clarifications and support actions for assisting businesses, organisations and consumers in the application of the rules?

Q17: What challenges do you identify in the governance structures of the digital rules?

Beyond the letter of the law: models that support the application of the rules

Q18: What are good examples of supporting actions and experimental practices that can help in giving legal clarity, cutting compliance costs, or supporting innovative practices and the take-up of new technologies, in particular for SMEs?

Supporting actions do not come only from authorities, but private entities also provide new mechanisms of assistance. In the Communication on a Data Union Strategy, the Commission explored in particular the concept of 'one-click compliance', where regulated entities can delegate compliance tasks, where this is permissible, to certified third-party providers. Such models can bring considerable optimisations, ensuring at the same time that the objectives of the rules are fully achieved.

Not all legal obligations can be prone to such mechanisms, and the important legal questions on liability and oversight arise. Determining who is accountable in case of errors, misuse, or system failures - whether the company, the certifier, or the regulator - will be essential to ensure trust and legal certainty.

Q19: What are sectors where such a 'one-click compliance' mechanism can bring particularly important opportunities? Please explain.

Q20: How could such mechanisms in conjunction with solutions like the European Business Wallets or the Digital Product Passport aid in enhancing trust, creating opportunities and simplify compliance?

Q21: What would you need to trust such solutions (e.g. certification, legal clarity, public oversight)?

Q22: What risks or concerns would you see in using automated compliance tools?

Q23: How could the EU best support their safe and effective use (e.g. standards, guidance, funding, pilots)?

Closing section

Q24: Please share any other remarks that you find important for the Commission to take into account in conducting the Digital Fitness Check. Please share any evidence, data, practical examples and analysis.

A centralised (Pan-European) public model for transmission of information related to shareholder's rights

We firmly believe that assigning a 'golden operational record' on shareholder-related information to a public European entity such as the European Single Access Point (ESAP), as proposed in the EU Commission's 'Study on the Application of the Shareholder Rights Directives', is not an appropriate path forward.

While the study notes that using ESAP has the potential to increase legal certainty, it also wisely cautions that such a mandate may impose significant costs on issuers. This cost concern, combined with more fundamental challenges, makes ESAP unsuitable for this role. ESAP is designed as a transparency and accessibility tool for publicly disclosed information, not as a legally and operationally embedded participant in the custody chain. It lacks the infrastructure and legal mandate to manage the operational complexities and liabilities of corporate events.

Additionally, corporate actions and securities registration are governed by diverse and complex national laws. The GOR function must be executed by an entity that understands and can apply national law. Any other issues that arise stemming from this legal fragmentation in national regimes will not be solved by placing data under a public European registrar. Lastly, a central body would assume immense liability for data accuracy. It would have no direct relationship with the data originators (issuers) to enforce the quality standards that are critical for the entire custody chain.