Digital Finance, Simplified

Enabling Digital Innovation in EU Capital Markets

Introduction

Digitalisation is rapidly transforming capital markets, reshaping how capital is raised, traded, and allocated - a process which will continue and accelerate in the coming years.

In recent years, an extensive effort from EU policymakers has been under way to rethink the regulatory framework for digital technologies. Important legislative milestones have been achieved over the past legislative cycle, crafting a comprehensive framework to govern emerging technologies, data flows, and financial innovation and build resilience. In some cases, the result has been a complex and fragmented landscape that increasingly challenges businesses and hinders the EU's competitiveness.

Enabling digital innovation in European capital markets – and the broader financial sector – requires a simplification of digital finance related rules, to reduce unnecessary or duplicative administrative burdens and foster a more agile and innovation-friendly regulatory environment.

Simplification must become a central pillar of EU digital finance policy. This includes:

- **Eliminate duplication**, especially where horizontal regulations overlap with sector-specific rules.
- **Ensure effectiveness** by aligning regulatory requirements with their intended outcomes.
- Maintain a proportionate **cost-benefit balance**, which acknowledges compliance burdens.
- Provide **clarity** to reduce uncertainty and support innovation.
- Promote **international** standards to facilitate global competitiveness.

The planned digital simplification package, announced by the European Commission for Q4 2025 provides a crucial opportunity to achieve this objective.

This paper sets out concrete proposals to reduce administrative burdens and foster a more agile and innovation-friendly regulatory environment.

Operational Resilience and Incident Reporting

The Digital Operational Resilience Act (DORA) underscores the importance of digital operational resilience in today's increasingly interconnected and digitised landscape. Compliance with DORA is a top priority given financial entities' increasing use of ICT and dependence on third-party ICT service providers, as well as the heightened focus on ICT and cyber-related risks impacting these third parties.

With DORA being part of a broader regulatory framework which at times interacts and overlaps with horizontal or product specific rules, it is important to ensure a coherent regulatory environment, particularly for a heavily regulated sector like financial services.

An important example of challenging overlap is the interaction between the Cyber Resilience Act (CRA) and DORA (both of which arguably also have overlapping obligations with the EU AI Act), which presents serious implementation challenges for the financial sector. The lack of coordination between these frameworks risks creating superfluous obligations for financial institutions, leading to a misallocation of resources and, at the same time, contradicting the Commission's goal of regulatory coherence and competitiveness. Financial services offered through digital channels— such as mobile banking apps, insurance apps, payment cards, ATMs, and point-of-sale terminals — are already subject to DORA, which imposes stringent and comprehensive requirements on financial entities' ICT systems and services. These systems are indeed covered by DORA, which provides safeguards throughout the entire lifecycle of these systems, from development to decommissioning, and includes risk-based

management, incident handling, vulnerability management, and customer communication strategies. Therefore they should be excluded from the scope of the CRA, either at the entity level or through Article 2(5) which empowers the Commission to adopt delegated acts to exclude products already governed by equivalent Union rules. An exemption would be significantly more effective than any proposal for an EU wide incident reporting hub, given that DORA and CRA reporting are divergent in terms of thresholds and templates. There is limited, if any, value to firms from a hub which serves simply as a reservoir for multiple, divergent submissions. The benefit would be in the aggregation of reports which market participants must submit, based on a harmonised set of definitions and thresholds as part of a single template, with the effect that firms have only to triage and collate one report while in the midst of responding to an incident.

Additionally, there is opportunity for targeted simplification within the DORA regime itself, particularly with regards to the incident reporting obligations and Registers of Information. Currently, there is reams of information which financial entities are having to provide which has no value for the purposes of risk management, despite representing a significant operational burden. This is borne out in the incident reports where there are data fields which are neither tangible nor actionable, and in the Register templates compelling financial entities to artificially dissect global, multi-year agreements into annual, per entity estimates.

Topic	Issues	Recommendations
Overlap DORA - CRA	Currently there is significant overlap between the provisions of DORA and the Cyber Resilience Act. The essential requirements for products with digital elements are extensively achieved, and exceeded, through the application of DORA for financial services. In fact, even though DORA is not product-specific, it applies to the very systems in which these digital financial products operate. The comprehensive gap analysis conducted by AFME is clear evidence that financial services should be exempted from the CRA on the basis this creates significant operational burden for firms with no net benefit in terms of risk management. The application of the CRA is also undermining the harmonisation objective of DORA.	Risk Management obligations should be harmonised by exempting financial services from horizontal frameworks where sectoral rules provide for an equivalent level of protection: specifically this should be applied with regard to the Cyber Resilience Act, where the "products" within scope are effectively covered by DORA as financial services offered through digital channels. This would be a prime example of removing overlap and duplication across departments. Accordingly, we request the Commission either to: • exercise its delegated powers under the CRA to exempt digital products offered by financial institutions, as already subject to DORA. This would align with the Commission's broader agenda of regulatory simplification outlined in the 2025 Work Programme, which emphasizes the need for consistency in cybersecurity and data protection rules. • Or to be more ambitious and mirror the treatment of DORA under the NIS2 Directive, where DORA is recognized as *lex specialis*. A similar, sectoral exemption from the CRA would ensure legal clarity and avoid overlapping obligations.
Duplicate incident reports under CRA	DORA successfully aggregated disparate incident reporting regimes for financial services, including PSD2, NIS and ECB cyber reporting This will be undermined by the incoming application of the Cyber Resilience Act (CRA) which will require banks to submit duplicate reports to financial supervisors (under DORA) and to ENISA or national cybersecurity authorities (under CRA). It is critical that firms' limited resources are utilised effectively during the management of a live incident / vulnerability.	Duplicative incident reports can be avoided through: • Information Sharing Agreements between authorities either by the leveraging of existing bodies such as the SCICF (Systemic Cyber Incident Coordination Framework) or through the establishment of an EU Incident Reporting Task Force with representatives from all relevant authorities to develop a unified incident reporting framework • In the event that there is no sectoral exemption from the Cyber Resilience Act, the vulnerability notifications to Computer Security Incidence Response Teams (CSIRTs) should only be required where the issue would not be captured by the incident reporting obligations under DORA to avoid duplicate reporting. • If the EU proceeds with the proposed DORA incident reporting hub, the EU should ensure that information submitted through the hub is transferred to other relevant authorities, including those listed under the Cyber Resilience Act. • The alternative proposal for an EU-wide hub for incident reporting raises serious questions. This reflects AFME's response to the ECB feasibility study on a reporting hub for DORA reports. It appears inevitable that the hub will itself become a target for malicious actors who will be aware it holds highly sensitive information. Significant levels of resourcing are further required to ensure the hub is in a position where it can support effective incident

		management and response, including swift detection and escalation of any incident which has the potential to cause wider systemic impact. Without such an underpinning the hub risks becomes an overarching data analytics centre or data collection entity which only risks detracting from that goal and could add to resource demands on firms during a live incident. We would in addition strongly caution that any hub, which serves only as a repository for multiple, divergent submissions, rather than bringing about an aggregation of reporting obligations, will have limited if any value.
DORA Incident Reports	The first quarters of DORA implementation have highlighted that: · The reports are at risk of proving ineffective for the purposes of incident management by seeking information which bears no relevance to this goal, being neither actionable nor tangible. · There are certain data fields and inputs which have not only proved burdensome but at times to be lacking in feasibility. · Despite DORA's intention to focus on major incidents and harmonise the process of reporting, the current configurations are capturing minor instances which some NCAs have informed members should not be regarded as major but which are falling foul of the thresholds · There is considerable variation between NCAs, for example Bank of Portugal's 'Instruction 21/2019' on cyber reporting has yet to be repealed, resulting in two separate, and different incident reporting processes,, or for example through the method of DORA incident reporting differing across national competent authorities (i.e. the CBI requires upload of Excel forms through their dedicated portal, whereas the ACPR use a JSON file format; this poses unnecessary operational burden for firms operating across the EU).	Simplified Incident Reporting Templates: The Commission should review the early implementation of the DORA incident reporting obligations: • We would strongly urge authorities in the DORA reports to only seek information which relates to incident management or which provides important insights into the scale of the incident under review. Data fields relating to BAU functions or longer term resolution would not fall within these categories, and risk turning DORA incident reports into generic data analysis. • In remedying these oversights, we would encourage the EU institutions to embed greater optionality within the reporting requirements in line with DORA's overarching proportionality principle. Further, as part of the EU's wider simplification agenda, we would encourage authorities to view incident reporting as an area of low-hanging fruit, where investments from authorities in their own systems would result in material savings for industry. As an illustrative example, the incident duration criterion is of questionable applicability: end-to-end management of an event within large financial institutions often exceeds 24 hours, especially when measured from the time of occurrence. Therefore, this criterion does not appear suitable for defining a major incident within the DORA framework. It is thus proposed to remove this criterion from the parameters used to classify major incidents under the regulation • We would strongly urge recalibrating those thresholds which have in practice proven to represent a very low bar. This can in part be achieved through supervisory clarifications, but a more holistic and ambitious response is warranted, for example abolishing the recurring incidents criteria on the basis it is not meeting the original Level 1 goals of DORA. • NCAs must, at the earliest opportunity, harmonise their incident reporting requirements to align with DORA. As part of this, NCAs should agreement on a single format for submission of incident reports, in line with the objectives of DORA and wider EU simplification to harmonise reporting and reduce regulatory burden.
DORA Registers of Information	The submission of the DORA Registers of Information is in need of coordinated streamlining. · Lack of alignment between NCAs, and between NCAs and ECB/ ESAs, created unnecessary complexity. · Insufficient and inconsistent guidance, combined with inconsistent and inaccessible approaches to validation, left firms unclear on how to comply and resolve issues. · Tools and support mechanisms were often not fit for purpose, complicating firms ability to resolve issues efficiently. · Compressed timelines and limited deadline visibility placed avoidable pressure on firms and authorities.	Coordinated streamlining across NCAs and ECB • We strongly encourage authorities to use the existing joint supervisory forums to share their own approaches, and any lessons learned, from the first submission of the Register. • We would encourage the authorities to undertake a review of common errors, and to publish ahead of the 2026 submission a set of expanded local guidance which takes these into account, having coordinated in advance on the preferred solution with fellow NCAs. • We would encourage greater signposting of upcoming updates, which should be published in a coordinated way across authorities. We also stress that without significant upgrades to technical instructions, for example the level of detail on error messages, financial entities will continue to seek bilateral supervisory assurances.

		• We would strongly urge the authorities to coordinate and align on the timeframes for submission at CA level, and to ensure that any future updates to RoI guidance or validation rules are published well in advance of these deadlines. • Consistent and comprehensive alignment with DORA in the upcoming EBA non-ICT Third Party Risk Management Guidelines, especially with regards to the definition of Critical and Important Functions where the current hybrid approach, incorporating both the DORA definition and the broader approach of the 2019 Guidelines will cause divergence.
DORA Risk Management Frameworks	Several of the requirements within DORA relating to the Risk Management Framework have proved technically or operationally unfeasible. We recommend these provisions are removed to ensure the legal obligations remain practicable.	We therefore recommend to: • Remove references to the encryption of data "in use" from the DORA Risk Management Framework. • Remove references to the segregation and segmentation of ICT systems, • Include a reference to the IT Risk Management Framework within the DORA RMF concerning the requirement to submit a separate DORA RMF Framework Review. • Remove references to obligate ICT third party services providers to participate and fully cooperating in a financial entities TLPT.

Artificial Intelligence Act

As highlighted by the FSB, AI offers benefits such as increased operational efficiency, regulatory compliance, financial product customisation and advanced analytics; the growth of generative AI (GenAI) is expanding the range of use cases. We welcome the Commissions focus on stimulating and supporting AI uptake across industries through the AI Continent Action Plan and upcoming Apply AI Strategy. For the EU to remain competitive globally, it must ensure that its financial institutions can deploy AI effectively and responsibly.

Many financial institutions have been integrating artificial intelligence (AI) into their operations across a wide range of business functions and use cases. Firms have utilised "traditional" forms of AI and machine learning for many years, and consequently have developed governance processes to oversee, manage and monitor their application of AI. Financial services is a highly regulated sector and existing regulations largely address and mitigate the key risks which might be caused or increased by the use of AI.

With the EU Artificial Intelligence Act, whilst we acknowledge that some guidance has already been published, there remains much to be done. There are significant areas where clarity is required as to how the financial services industry can best comply with the requirements and guidance set out. However, the timelines for compliance set out by the Act are short – there is less than a year before the majority of the Act begins to apply. We see that the pressures of this timeline are beginning to be understood at a policymaker level, noting for example the recent remarks by Mario Draghi[1]. We would encourage the European authorities to consider carefully whether the current timeline is sufficient for the preparation and publication of the various guidelines and technical standards, also taking into account reasonable implementation time for firms. Overall, AFME would be supportive of a revision of the implementation timeline to ensure this legislation is delivered and embedded as thoroughly as possible.

In relation to the specific areas where clarity is required for financial services firms:

Topic	Issues	Recommendations
Definition of AI system	Within the **definition of an "AI system"**, the definitions of "autonomy" and particularly the term "varying levels of autonomy" need to be clarified.	• Any AI model that relies entirely on human input for its design and training (e.g. to preprocess data, select features and interpret results), and which does not have capacity to take decisions independently which directly influence the

[1] https://commission.europa.eu/document/download/0951a4ff-cd1a-4ea3-bc1d-f603decc1ed9_en?filename=Draghi_Speech_High_Level_Conference_One_Year_After.pdf

		final user, should not be considered autonomous, and therefore should not be considered an AI system. • Within the definition of an "AI system'", clarify the definitions of "autonomy" and particularly the term, "varying levels of autonomy". • Additionally, in the AI system definition guidelines, confirm across the board that logistic regression – when used on a standalone basis – should not be subject to the EU AI Act's regulatory requirements. Conversely, if logistic regression is integrated into an AI approach (such as machine learning), it should be encompassed by the AI Act.
Definition of High Risk AI under Annex III	Employment, workers management and access to self-employment - Art 6(2) Annex III para 4.	• The specific use cases in paragraph 4 are all examples of high risk processing since they are all examples of automated processing of personal data for the purpose of analysis, evaluation, classification, profiling and monitoring. These are all types of processing which are subject to existing regulation under GDPR and detailed guidance such as the Article 29 Working Party guidance on automated decision making. There is therefore already some duplication of the obligations under GDPR and the EU AIA. • Such GDPR guidance already mandates obligations for controllers regarding hidden bias, data accuracy, consideration of the representativeness of datasets, consideration of the data lifecycle and the suitability of the data (and context of collection) against the intended purpose of processing. Similarly for impact assessments on data subjects.
Definition of "substantial modification"	The definition of "**substantial modification**" as stated in Article 25(1)(b) of the AI Act, that could lead to an operator being deemed a provider, is unclear. Recital 128 refers to substantial modification as being in line with established EU law, which we read as a broad test to refer to a change to an AI system after its placing on the market or putting into service, which (i) is not foreseen or planned in the initial conformity assessment and affects compliance of the AI system with the requirements in Chapter III, Section 2, or (ii) results in a modification to the intended purpose.	• Further metrics and examples of the most commonly applicable use cases, particularly in reference to High-Risk AI Systems and clarity on the threshold definition of when minor changes becoming "substantial" e.g. reformatting output, should be provided. • Our members would appreciate specific clarity from the Commission that, as is commonly understood in relation to existing EU legislation, the substantial modification of an AI system would have to go to the heart of its purpose, as opposed to changes such as refinements and fine tuning. • Under EU Product Laws – the operator role of manufacturer is only triggered when a product has a name or trademark applied ***and*** placed on the market. This necessitates commercial distribution or use as a trigger. Under the AI Act, the application of a name or trademark in the ordinary course of use by a deployer without placing on the market, would trigger provider obligations. Such branding would be consistent with internal use and would not alter the risk profile of an AI system and yet under Article 25 this would trigger provider obligations. To align with product safety laws, the application of a name or trademark should only fall within the scope of Article 25 when placing on the market and this should not apply when an AI system is put into service.
General Purpose AI	**GPAI** - Recital 97 provides that (i) when a provider of a general-purpose AI model incorporates their model into an AI system that is then made available on the market or put into service, the model is considered to be "placed on the market." In such cases, the regulatory obligations for both the model and the AI system apply; and (ii) the obligations for models do not apply if the model is used solely for internal processes that are not essential for providing a product or service to third parties, and where the rights of natural persons are not affected. This exemption recognises that internal uses, which do not impact external stakeholders or infringe on individual rights, do not necessitate the same level of regulatory oversight. However, it is unclear	• Clarifications in relation to General Purpose AI models. • Additionally, our members would appreciate additional clarity on the timeline on which the metrics (such as the 10^25 FLOPS) for compute thresholds designating general purpose AI models as those with systemic risk will be recalibrated and updated. • Notwithstanding the provisions of the AI Act on GPAI models and the GPAI Code of Practice, it is increasingly difficult for downstream providers to obtain information on the computational power of models in order to assess whether a model is a GPAI model within the scope of the Act given the proprietary nature of this information. This makes assessment of GPAI models increasingly difficult for downstream providers.

	whether a deployer would be designated as a provider if a firm develops General Purpose AI (GPAI) based on systemic GPAI registered in the EU GPAI Register, which should be exempt for the same reasoning as above.	• Clarity in relation to the meaning of word "own" provided in Recital 97 where it states the obligations for models do not apply when "*an own model is used for purely internal processes*".
Transparency Obligations for Gen AI Systems	Article 50 requires that Providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated. Providers shall ensure their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible, taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art, as may be reflected in relevant technical standards.	• Given that the providers of AI systems are likely to rely upon foundation model providers for the generation of output in compliant formats, this appears to be an obligation which would be better directed at the GPAI model providers, since the markings need to be machine readable and robust.
Interaction with GDPR	There is a growing legal and regulatory gap between how automated decision-making is interpreted under GDPR Article 22 (as clarified by the Schufa case) and how high-risk AI systems are defined under the EU AI Act, particularly in employment contexts. AI tools that contribute significantly to decisions about employees — even if not making the final call — may fall under both regimes, yet current guidance lacks clarity on how these frameworks interact. For example "AI intended to be used to make decisions affecting terms of the work related relationships" does this mean only use cases in which the decision is made by the AI tool or does this also bring in use cases in which the AI contributes input which informs an overall decision (e.g. a tool used to assess employee performance) then output from this is combined with other data to assign a performance rating. This is automated processing under GDPR and thus high risk. Does this also meet the high risk use definition in the AI Act even if the AI is only a contributory aspect?	• The Commission should clarify in this context how the AI Act defines automated decision making supported by AI tools and how they would resolve the discrepancy with how the courts are interpreting GDPR Art 22,

Financial Data Access regulation (FiDA)

While the EU has now set important objectives to strengthen its competitiveness, the Financial Data Access (FiDA) Regulation proposal raises crucial concerns in terms of disproportionate burden, scale of requirements and lack of a thorough assessment that reflects the radically changed environment since the Regulation was first proposed. In its current form, FiDA adds regulatory burdens at a time when Europe is grappling with a loss of competitiveness compared to other jurisdictions.

The FiDA proposal, considering its disproportionate burdens, scale of requirements and lack of clear link with market demand, needs to be carefully reassessed to ensure it is in line with the EU's competitiveness and simplification objectives. Also, data sharing in the financial sector cannot be considered in isolation but should be coherent with EU's Data Union Strategy and its objective to simplify data sharing rules.

Topic	Issues	Recommendations
Complexity and need for link with market demand	The FIDA proposal is overly complex in its current form. In addition, FiDA adds regulatory burdens at a time when European financial institutions are already facing high economic and compliance challenges, including in terms of cost of the digital	• A market-driven, gradual, and demand-based approach to FiDA implementation is necessary to ensure that IT investments, human and financial resources are allocated based on proven customer demand.

	transition. In the absence of customer demand, these requirements impose disproportionate costs. The co-legislators have now been acknowledging these issues, and the EC has taken a step in the right direction by proposing measures to reduce the scope. However critical issues remain unaddressed: the lack of a market driven approach, the need for a gradual implementation timeframe, the excessively broad customer and data scope, as well as a lack of reciprocity with digital gatekeepers.	• FiDA should focus on data sharing for mass retail clients, and exclude other clients from its scope. Moreover, the scope should only include: (i) raw data in natively digital form, and (ii) a very limited number of data categories, on the basis of an assessment of market demand. • Adequate extension of implementation timelines is a critical point that has been acknowledged in the Council and Parliament positions. Furthermore, historical data should be limited to at most 2 years from the data request at the notification date of the scheme . • We support the proposal to exclude gatekeepers and their affiliates from the Financial Information Service Provider (FISP) licensing regime

Contacts:

Stefano Mazzocchi
Managing Director, Advocacy
stefano.mazzocchi@afme.eu

Coen ter Wal
Director, Technology & Operations
coen.terwal@afme.eu