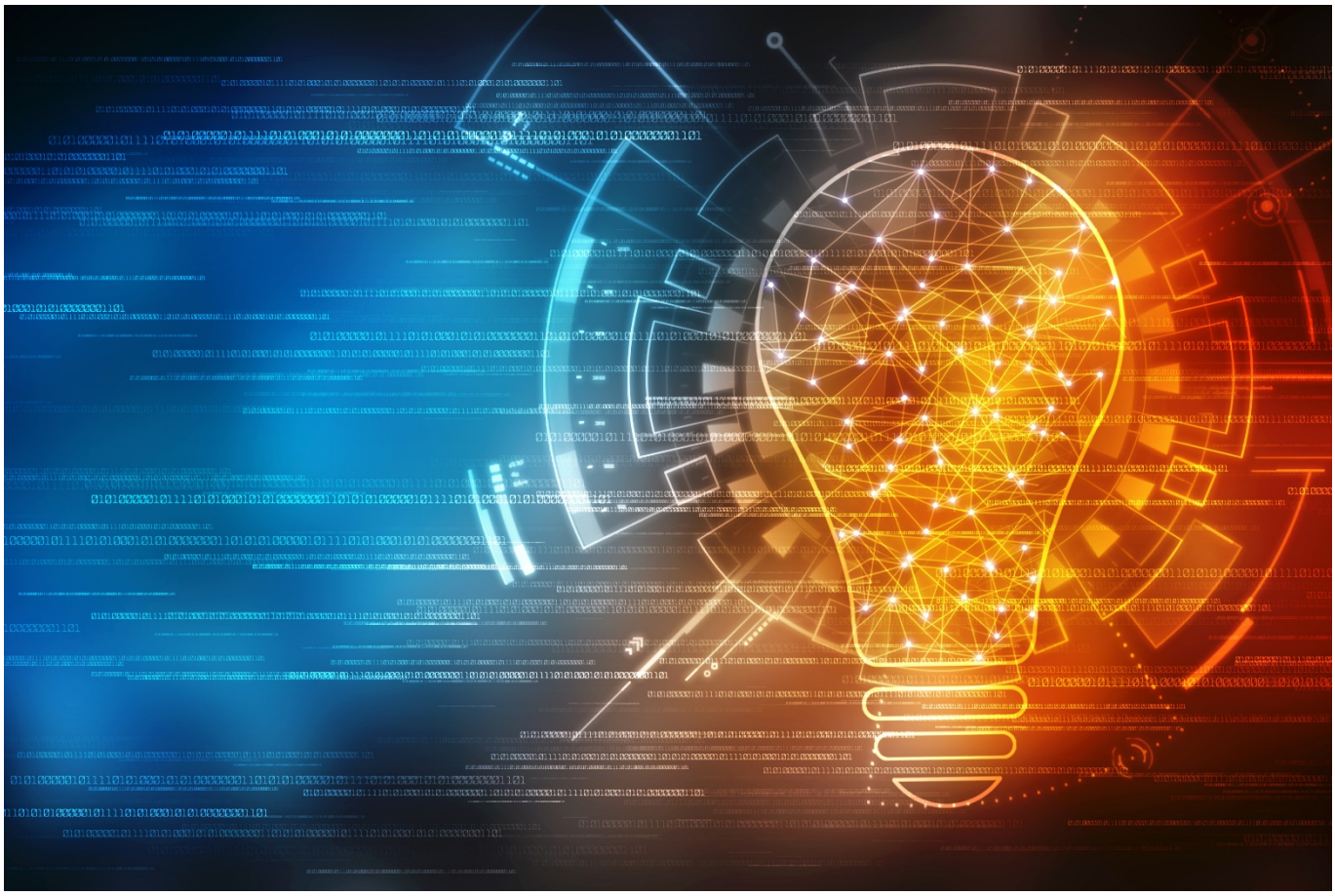
afme/
Finance for Europe

European Capital Markets in the Digital Age

AFME's vision for resilient, innovative, and competitive capital markets

September 2020



Association for Financial Markets in Europe
www.afme.eu

Contents

Foreword

AFME's Technology and Operations Division is pleased to publish our latest paper titled "*European Capital Markets in the digital age*", in which we discuss our vision for a Europe-wide digital regulatory framework. We believe this vision will promote innovation and competitiveness amongst capital market participants whilst ensuring the goal of a high level of resilience.

The European Commission's recent publication of their five-year digital agenda, '*A Europe Fit for the Digital Age'*,[1] recognises that new technologies will have a transformational impact across both Europe and the rest of the world.

The EU digital agenda is welcomed by AFME. We support the view that encouraging innovation, increasing technical capability, and improving the strategic competitiveness for the region can be best delivered by reinforcing the Union's harmonised values and rules.

A strong European digital agenda will enable closer European supervisory integration and help in the delivery of the Capital Markets Union (CMU), by reducing both the barriers to cross-border business and transactions costs. Europe's capital markets participants will equally play a key role in helping to achieve the ambitions of the EU digital agenda by driving the development of new technologies.

New technologies will help create new and innovative financial products and services, drive efficiencies in operations, improve the resilience of financial markets, attract new talent, and support new ways of working. Regulated appropriately, new technologies can support a vibrant and competitive European Digital Single Market and stronger, more efficient capital markets infrastructures. The recent COVID19 pandemic has reinforced this requirement, demonstrating how technology underpins the continued functioning and resilience of our capital markets.

It is also essential that the EU regulatory framework is supportive of technology adoption and innovation in capital markets. The regulatory framework should appropriately address any risks and emphasise the principle of 'same activity, same risk, same regulation' for all market participants.

As capital markets rapidly evolve in the face of technological innovation and global challenges, AFME continues to engage on policy initiatives for key technologies – artificial intelligence, cloud computing, crypto-assets – and related topics – data, cybersecurity, outsourcing and operational resilience. We look forward to continuing to collaborate with European and global regulators in fostering resilient, innovative, and competitive capital markets.

James Kemp
Managing Director
GFMA and AFME

[1] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

Executive summary

The AFME Technology and Operations Division believes that a European framework fit for the digital age should be developed based on the following four high-level objectives:

1. The European regulatory framework for innovative activities needs to be globally consistent, and based on global standards, to sufficiently mitigate risks and support the competitiveness of the EU. Given the global nature of capital markets, and leveraging the experiences in the implementation of the 2009 G20 derivatives obligations, any European developments on the regulation of activities using innovative technologies should be consistent with ongoing global risk assessments or initiatives (e.g. G7/G20, FSB, BIS, IOSCO). This will help to avoid gaps in regulation, which is critical for maintaining a level-playing field, reducing fragmentation, promoting financial stability, and ultimately protecting end users. This framework should be supported by European supervisory authorities and standard setting bodies, as well as global organisations, in coordinating to develop and maintain global standards.

2. The European Commission should develop a clear strategic vision that promotes the uptake of innovative technologies in the financial sector to enable a truly fit for purpose regulatory framework. This vision will provide clarity and support the coordination of efforts between various European authorities, market participants and Member States. This vision will enable a common understanding of shared European goals, removing duplicative or potentially conflicting European policy initiatives.

3. The European regulatory framework must remain technology neutral, principles-based and proportionate in order to support technology adoption. As technology continues to rapidly evolve EU legislation should be technology neutral and principles-based in order to provide the flexibility needed for firms to implement the appropriate controls for the activities they are conducting in a risk based and proportionate manner.

4. A competitive and level-playing field is needed to ensure all firms involved in capital markets adhere to the principle of 'same activity, same risk, same regulation'. A level playing field for all capital markets participants is essential to manage risk, whilst supporting competition and innovation. This means that existing regulation should be deployed and applicable to entities who may be currently outside the financial services regulatory framework but are conducting the same or similar activities as regulated financial institutions.

Priority areas

For the following three priority areas we recommend that European supervisors:

Priority 1: Cybersecurity and operational resilience:

- Remove fragmentation in operational resilience regulatory requirements (e.g. reporting, testing regimes, certifications), which create a significant and unnecessary burden for capital markets participants and diverts valuable resources away from protecting the financial system;
- Encourage better coordination of industry standards for operational resilience, to ensure a faster and more effective response to incidents; and
- Facilitate a coordinated global approach to operational resilience to avoid placing unnecessary burdens on firms and prevent isolated incidents from becoming systemic.

Priority 2: New technologies and innovation:

- Identify and address existing regulations which act as a barrier to both digitisation and improved operational resilience, therefore creating an innovation-friendly framework that encourages new opportunities whilst managing risks;
- Remove fragmentation in the regulatory treatment of crypto-assets to provide market participants with greater regulatory certainty, encourage innovation, and help realise potential benefits to end users such as reduced costs or improved auditability/supervision;
- Create a clear and risk-based framework that promotes the ethical and transparent use of AI in capital markets, to allow the technology to be used at scale. This should include addressing regulatory uncertainty by providing where necessary targeted clarifications, guidance, and recommendations to the existing regulatory framework; and
- Identify and address existing barriers to the adoption of cloud computing in capital markets (e.g. divergence in regulatory guidelines, a lack of support and awareness of the benefits to the industry). If used at scale by both supervisors and market participants, cloud computing can bring significant benefits to the industry, such as reduced costs and improved data analytics.

Priority 3: Data-sharing:

- Implement a cross-sectoral approach in further European data-sharing initiatives to support innovation and ensure a level-playing field;
- Address potential cyber risks relating to data-sharing and data access (e.g. through the use of technical standards and APIs) to protect end users and maintain market confidence;
- Ensure sufficient data portability for individuals and firms to allow users to share their data on a real-time, ongoing, standardised, and secure basis; and
- Coordinate greater standardisation of data types and formats within and across sectors to drive greater efficiencies in data-sharing and analysis.

The remainder of this paper provides further detail on each of the priority areas above and our recommendations for driving a regulatory framework that is fit for the digital age.[2]

[2] For further details, please see our response to the European Commission's consultation on a 'A New Digital Finance Strategy for Europe here or our dedicated webpage here.

Cybersecurity and operational resilience

The AFME Technology and Operations Division recognises the increasing importance of digitisation for capital markets and the wider economy. This has important implications for cyber and Information and Communication Technology (ICT) risks, which can also impact a firm's operational resilience. We believe the regulatory framework for cybersecurity and operational resilience should remain risk and principles-based, enabling firms to have the flexibility to identify their critical functions, metrics and testing scenarios that are most relevant and proportionate to their business and risk profile.

There is also a need to create a harmonised approach to the management of cyber and ICT risks in Europe. This will minimise the risk of diverging requirements across Member States and provide consistency and clarity of regulatory requirements; particularly for firms operating cross-border.

Cybersecurity and technology risks in Europe

Cybersecurity and technology risks are a challenge for firms due to their complex and cross-border nature. AFME is proactively engaged through the GFMA (Global Financial Markets Association)[3], with sister trade organisations (SIFMA,[4] in the US, and ASIFMA,[5] in APAC) on these related issues. We will continue to work with industry and government leaders to identify and communicate best practices and educate the industry on evolving threats.

Financial Institutions and Financial Market Infrastructures are often cited as a prime target for cyber-attacks due to their pivotal role in the economy. In an increasingly complex, interconnected and quickly evolving landscape, cybersecurity and technology risk policies should remain globally coordinated and proportionate so that firms can dedicate the appropriate resources and effectively respond to time-critical incidents.

Our recommendations:[6]

- ***Any proposed legislative changes for cybersecurity should remain principles based and focus on the minimum requirements for the management of ICT risks across the EU financial sector.*** Prescriptive policy proposals for the management of cyber and ICT risks could become obsolete over time and may not provide the level of flexibility required for firms to appropriately mitigate these risks.
- ***Any proposed legislative changes should be consistent and not duplicative of existing regional and global principles and standards for managing cyber and ICT risks.*** A thorough analysis regarding current and future resilience policy initiatives, will help to ensure that it complements, and does not overlap, with existing EU and international standards.
- ***Any proposed legislative changes should continue to support innovation in the European and global financial services sector.*** AFME welcomes efforts to support innovation in cyber and operational resilience in Europe, such as harmonising with international standards, reducing regulatory inconsistencies and fragmentation (e.g. incident reporting), and leveraging international cooperation where possible (e.g. sharing Threat Level Penetration Testing – TLPT – test results).

A European and globally coordinated framework for Operational Resilience

The Basel Committee for Banking Supervision has defined Operational Resilience[7] as the ability of firms and the financial system as a whole to deliver critical operations through disruption. This ability enables firms to identify and protect from threats and potential failures, as well as respond and adapt to, and recover and learn from, disruptive events to minimise their impact on the delivery of critical operations. Operational resilience is a key pillar underlying the safety and soundness of the wider economy. As authorities seek to establish how to appropriately assess and strengthen operational resilience of wholesale markets, there is a risk that national approaches will begin to diverge and become inconsistent. AFME is actively engaging through GFMA,

[3] https://www.gfma.org/
[4] https://www.sifma.org/
[5] https://www.asifma.org/
[6] Please see our response to the European Commission's consultation on *Digital Operational Resilience* here for further details.
[7] https://www.bis.org/bcbs/publ/d509.pdf (p.3)

with sister trade organisations (SIFMA and ASIFMA), to ensure a globally coordinated and consistent approach is developed across the industry.

Operational resilience is extremely important for the public and private sectors to maintain confidence in financial markets. This has been further emphasised this year in the context of COVID19, as technology has played an increasingly important role in ensuring continuity of services throughout the crisis.

Our recommendations:

- ***Regulators should ensure global coordination and alignment on policy outcomes, terminology and supervisory approaches to operational resilience.*** Establishing a consistent and globally recognised international approach would:
    - Provide a minimum agreed upon objective for the definition and measurement of operational resilience;
    - Help to facilitate the sharing of best practise in operational resilience capabilities across jurisdictions, to increase the industry's preparedness, response and recovery from operational incidents;
    - Help to prevent fragmentation during the development and implementation of operational resilience approaches globally;
    - Allow firms to apply these principles consistently across global, cross-border business services in a manner suited to their varying and unique business models, sizes and complexities; and
    - Mitigate the extraterritorial impacts of jurisdiction-specific approaches.
- ***Any legislative proposal aimed at increasing the level of operational resilience in financial services should complement and leverage existing standards, regulations and expectations.*** Operational resilience is connected to a number of existing processes that firms currently manage. This includes but is not limited to: business continuity management; enterprise risk management; disaster recovery; cyber security; third-party vendor management; technology management; operational risk; recovery and resolution planning. It is therefore extremely important that the global approach to increasing the financial sector's operational resilience should be complementary to, and not duplicative of, or in conflict with, other existing resilience-related regulations and supervisory expectations.
- ***Any legislative proposal on operational resilience should seek to mitigate risks to financial stability, including, where relevant, dependencies with firms outside of financial services***. The potential dependencies and connectivity between the financial sector and other sectors – including utilities, critical infrastructure and critical shared services – can impact a firm's operational resilience. On this basis, a cross-sectoral approach to the development of global operational resilience principles would be valuable.
- ***Any legislative proposal on operational resilience should be driven by public and private sector collaboration***. It is widely recognised that strengthening operational resilience will be an iterative process that requires effective collaboration among financial institutions and global regulators on an ongoing basis. Recent events highlight the importance of global leadership in the development of aligned principles as the next step in this process.

New technologies and innovation

Whilst innovation in capital markets is not new, the pace continues to be significant. Innovative technologies, such as artificial intelligence (AI), cloud computing and crypto-assets have the potential to drive capital markets efficiencies across a broad range of functions (e.g. equity issuance, corporate governance, asset management, post trade market infrastructure technology, operations).

An EU framework for markets in crypto-assets

Crypto-assets have the potential to bring benefits to market participants and support a competitive, dynamic business environment. It is crucial that Europe makes use of the potential benefits of crypto-assets to strengthen European financial markets.

Crypto-asset-related policy initiatives should aim to provide legal certainty to market participants looking to issue or trade crypto-assets. This will allow participants to benefit from efficiency gains, and support wider adoption, while ensuring consumers/investor protection and maintaining financial stability. Furthermore, harmonisation of regulatory approaches across Member States is crucial to prevent market fragmentation and contribute to a truly (digital) single market.

Our recommendations:[8]

- ***A crypto-asset taxonomy should be established as a first step towards developing a globally consistent regulatory treatment for crypto-assets that is calibrated to the risks and level of oversight required.*** This will help foster common understanding, facilitate collaboration across jurisdictions, and provide greater regulatory certainty for market participants engaged in cross-border activity. It is essential that authorities provide globally consistent definitions of different types of crypto-assets as part of this taxonomy. Classification may be based primarily on a crypto-asset's economic function; however, a secondary and more detailed analysis is also required to consider additional functionalities of more complex crypto-assets, such as hybrid tokens.[9]
- ***Regulators should apply existing regulation to crypto-assets, with any necessary amendments or additional guidance where possible.*** The use of Distributed Ledger Technology (DLT) to record traditional assets does not necessarily indicate the creation of a new asset. Regulators should apply the principle of 'same activity, same risk, same regulation' to identify if existing regulations apply. A bespoke regime would only be appropriate in cases where current regulations cannot adequately address the novel or unique risks that certain crypto-assets may create. Existing regulations should also apply to other entities who may be currently outside the regulatory perimeter that conduct the same or similar activities as regulated banks or financial institutions. Further, it will also be important to differentiate between a traditional financial activity that simply uses new technologies such as DLT, where existing regulations should apply, versus new financial activities related to potentially higher risk-crypto assets.
- ***Regulators should provide additional clarification on how existing regulations will apply to crypto-assets, as these regulations were not originally designed with crypto-assets in mind.*** This includes, for instance, the clarification of certain definitions or activities in existing legislation (e.g. MiFID II, CSDR, SFD, MAR, DGSD, etc.). There is a need to clarify how crypto-assets may fall in scope of these regulations. For instance, in CSDR, there is a need to clarify the potentially new role of a Central Securities Depository in security token settlement, which could include overseeing the DLT network and holding validation rights to record, control and facilitate the transfer of legal titles of securities.
- ***Regulation should be technology agnostic to address the risks associated with the underlying crypto-asset or activity in order to encourage innovation***. This will help ensure the regulatory framework is future-proofed while the market continues to quickly evolve. Increases in technology and operational risk should be mitigated by leveraging existing risk management frameworks where possible.

[8] Please see our response to the European Commission's consultation on *An EU Framework for Markets in Crypto-assets* here for further details.
[9] The GFMA has developed an initial approach to the classification of crypto-assets, which can be found here in Annex A of the GFMA response to the BCBS Discussion Paper on *Designing a Prudential Treatment for Crypto-assets*.

- ***It is important to ensure that the regulatory treatment of crypto-assets is globally aligned, wherever possible, to sufficiently mitigate risks.*** International consistency is important to avoid gaps in regulation and provide clarity around what determines jurisdictional oversight, as currently it is not always clear what regulations may apply (e.g. depending on where the issuer validator node or wallet provider is located). There may also be a need for global minimum operating and conduct standards for currently unregulated crypto-asset activities.

A European approach to artificial intelligence

As the adoption of artificial intelligence (AI) and machine learning (ML) in capital markets continues at pace, attention is increasingly focusing on how firms can demonstrate a responsible approach to the use of this technology. Capital markets market participants should continue to engage with regulators to ensure the European approach to AI is principles-based in order to support innovation.

Our recommendations:[10]

- ***AI Regulation should remain technology-neutral, proportionate and principles-based to avoid creating unnecessary barriers to the development and adoption of AI***. Regulation that focuses on a particular technology (such as a specific AI technique) does not address underlying behaviours or practices that AI relies on as a tool to perform certain activities. Further, given the speed of technology advances, technology-specific regulation will struggle to maintain pace with market developments, which can create barriers to the adoption of new technologies.
- ***Where uncertainty on how to meet current regulatory requirements exists, authorities should strive to provide additional clarifications, guidance and recommendations on how to meet those requirements***. This would be particularly helpful in complex and evolving areas such as AI/ML 'explainability' or avoidance of unjustifiable bias, where the regulatory framework is already comprehensive but its practical application to the use of AI continues to generate discussion.
- ***Policymakers and authorities should seek to avoid duplication with existing regulatory requirements, particularly for sectors that are already highly regulated such as capital markets.*** These sectors have already developed processes for identifying and mitigating a variety of risks, which will also be applicable to firms' use of AI. The imposition of a new, horizonal regulatory framework is likely to conflict with the work completed to date and be less effective in mitigating risks.
- ***Harmonisation of supervisory expectations and participation in global networks is key in avoiding fragmentation.*** Partnership with the industry in harmonising expectations will be crucial, particularly where rapid technological change continues to prompt discussion in setting appropriate standards. We encourage deep EU and Member State involvement in the global innovation networks, where best practices can be shared.

The adoption of cloud computing in Europe

Cloud Computing (and more broadly outsourcing) remains an important topic for policymakers, regulators and financial services firms in capital markets.

Cloud (and particularly public cloud) is expected to expand significantly across the capital markets value chain[11], with key benefits including greater business agility and innovation; improved cost management and efficiency; enhanced client experience and service offerings; and more effective risk mitigation strategies. Cloud also provides firms an opportunity to strengthen their resilience (both operational and cyber) and operational efficiency; highlighted as an important factor in the response to COVID19.

A key priority for the industry is ensuring that these benefits can be realised from wider adoption of cloud computing, while avoiding any risks to the secure, reliable, and efficient operation of financial markets and the safe handling of client transactions and data. Regulators also have an important role in continuing to

[10] Please see our response to the European Commission's consultation on *Artificial Intelligence – A European Approach to Excellence and Trust* here for further details.
[11] For more information, please see the AFME's paper on *The adoption of Public Cloud Computing in Capital Markets* here.

promote harmonised, and technology-neutral and risk-based legislation, for the use of public cloud at the regional and global level, in particular to develop cloud understanding and expertise, and periodically review whether considering cloud as a form of outsourcing sufficiently supports financial stability and allows firms to manage their risks effectively.

However, many barriers remain for increased cloud adoption, including: banks legacy IT complexity; regulatory concerns and perception; a lack of standardisation in cloud service offerings; and long-term considerations on concentration risks. A lack of understanding and acknowledgment across the industry (for both banks and authorities) of the benefits of cloud for the capital markets industry is also a key barrier to change.

Our recommendations:

- ***Regulators and market participants should continue to prioritise developing their understanding and expertise in cloud computing to support a more targeted supervisory approach.*** Regulators should also periodically review whether cloud, as a form of outsourcing, sufficiently supports financial stability and allows firms to manage their risks effectively.
- ***The industry must continue to share knowledge, best practice, and promote standardisation and consistency in how public cloud is adopted.*** Cloud Service Providers (CSPs), banks, and regulators must continue to actively engage and collaborate. This engagement is vital to building the capabilities and assurances required for increased cloud adoption (e.g. legal, regulatory, privacy). Increasing standardisation of service offerings can also satisfy regulatory requirements.
- ***Regulators should carefully assess, with the industry, approaches to support both banks and cloud service providers in addressing any sector risks such as concentration risk.*** While banks already address potential cloud adoption risks, such as concentration risk, as part of their own risk assessments and due diligence, they require support from regulators to address sector-wide risks. It is important that authorities avoid placing additional complexity or restrictions on banks' ability to make commercial decisions and adapt to emerging business models and technologies, as some solutions to address concentration risk currently proposed by authorities (e.g. exposure limits, rotation mechanisms) may limit the firms' ability to make commercial decisions and adapt to emerging business models and technologies.
- ***Regulators should support greater regional and global harmonisation in public cloud adoption requirements and supervisory practices in order to remove barriers to adoption.*** We encourage regulators to facilitate and/or participate in multi-stakeholder technology forums and 'compliant by design' solutions, to aid in early identification and resolution of key regulatory issues and concerns.

Data-sharing

The benefits of new technologies can often be realised through new business models offered by both incumbent institutions and new entrants to the market. Banks are continuing to look for opportunities to deliver efficiencies and improve service to clients while also being under pressure to reduce bottom line costs, manage new regulatory requirements and address legacy technology platforms.

The use of data provides many opportunities to drive greater innovation and acts as a fundamental building block for several other technologies. We believe is particularly important to ensure a level playing field among all participants and ensure data-sharing is cross-sectoral (not limited to the banking sector) to ultimately drive benefits for end-users.

A European Data Economy

We welcome the Commission's efforts to enable a European Data Economy[12] that is built on a robust legal framework and promotes policy measures that address issues related to interoperability, data standardisation, a level playing field and cyber security.

A clear roadmap towards a European Data Economy will be important for ensuring European markets can remain competitive and promote the individual's rights to data sharing. A cross-sectoral approach to a European data economy is a necessary pre-requisite to ensuring that the digital economy creates mutual benefits and empowers end-users.

Our recommendations:[13]

- ***Regulators should apply a cross-sector approach to data sharing.*** Any open data policy should be cross-sectoral to bring benefits to end-users, particularly as new entrants emerge. Any mandatory requirements should be applied equally to market participants to maintain a level playing field. It is also important to address data localisation restrictions across jurisdictions, which act as a barrier to greater data sharing.
- ***Regulators should clarify the different types of data that could be shared.*** Action is needed from the European Commission to delineate clearly between raw/observed data and elaborated/inferred data insights. In line with the Article 29 Working Party,[14] we believe that elaborated or inferred data insights should not be subject to mandatory sharing requirements between businesses, except as part of specific competition policy interventions.
- ***Regulators should enhance data portability under GDPR to allow individual users or firms to share data on a real-time, ongoing, standardised and secure basis.*** We believe data portability should also be extended to non-personal data under the Data Act/Digital Services Act (e.g. by applying ex-ante rules in the Digital Services Act to business users' data held by digital platforms).
- ***It is important to ensure the secure transmission of data by creating operational standards for data access to ensure data can be seamlessly connected in a secure environment.*** Application Programming Interfaces (APIs) are the preferred industry method for the transmission of data as they are secure, efficient and can provide access on a real-time and/or regular basis. Interoperability between APIs will be essential to make data sharing a reality (both within and across sectors).
- ***Increased standardisation of data types, and formats within and across sectors is needed to ensure data can be shared and analysed efficiently and safely.*** European supervisory authorities and standards setting bodies, as well as global organisations, will have an important coordinating role to play in achieving these objectives. Regulators should also prioritise international coordination on common data inputs and consistency in reporting requirements.
- ***Regulators should provide further clarity on what Common European Data Spaces (CEDS) will entail, including on their potential role, scope, purpose, operation, technology and governance***. Further assessment and clarification is required on how CEDS will operate to ensure that a level

[12] https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy
[13] Please see our responses to the European Commission's consultations on data here and here for further details.
[14] https://edpb.europa.eu/our-work-tools/article-29-working-party_en

playing field across financial market participants is achieved, and that security and privacy concerns from such approaches are adequately addressed.

About the Association for Financial Markets in Europe (AFME)

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues. We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

We represent 177 members – universal banks, investment banks, and other relevant institutions such as law firms and credit rating agencies – who have operations in 30 European countries.

We work through 15 dedicated Divisions, supported by some 13 Committees and over 90 working groups, and are also members of the Global Financial Markets Association (GFMA) that includes sister organisations in North America (SIFMA) and Asia (ASIFMA).

About AFME's Technology and Operations Division

AFMEs Technology and Operations Division was formed in 2016 to focus on the application of technology and security policy within Europe's capital markets. The Division develops thought leadership, promotes best practice and is responsible for associated advocacy in relation to European regulatory plans and in conjunction with our GFMA partners at a global level.

This focus ensures that our members can leverage technical innovations whilst promoting the optimum regulatory and security frameworks. The Division is led by a senior Committee of technology and operations leaders from AFME board member firms.

The Division also holds an annual conference which brings together over 300 senior AFME members, supervisors, and technology providers who are driving strategic change in Europe's leading organisations.

AFME Technology and Operations Contacts

James Kemp, Managing Director, GFMA and AFME, +44 20 3828 2705
Andrew Harvey, Managing Director, aharvey@gfma.org, +44 20 3828 2694
David Ostojitsch, Director, david.ostojitsch@afme.eu, +44 20 3828 2761
Emmanuel Le Marois, Associate Director, emmanuel.lemarois@afme.eu, +44 20 3828 2674
Fiona Willis, Associate Director, fiona.willis@afme.eu, +44 20 3828 2739
Hélène Benoist, Manager, helene.benoist@afme.eu, +32 2 788 39 76
Madeline Taylor, Associate, madeline.taylor@afme.eu, +44 20 3828 2688

London Office
39th Floor
25 Canada Square
London E14 5LQ
United Kingdom

Switchboard:
+44 (0)20 3828 2700

Brussels Office
Rue de la Loi, 82
1040 Brussels
Belgium

Switchboard:
+32 (0)2 788 3971

Frankfurt Office
Neue Mainzer Straße 75
60311 Frankfurt am Main
Germany

Switchboard:
+49(0)69 153 258 963

AFME is registered on the EU Transparency Register, registration number 65110063986-76