

A EUROPEAN UNION FIT FOR THE DIGITAL AGE

On 24 September 2020 the European Commission (Commission) set out a new, ambitious approach to encourage responsible innovation to benefit consumers and businesses.

The Digital Finance Package, which includes Digital Finance and Retail Payments Strategies, and proposals for regulations on crypto-assets and digital resilience, aims to boost Europe's competitiveness and innovation in the financial sector. The Commission aims to give consumers more choice and opportunities in financial services and modern payments, while at the same time ensuring consumer protection and financial stability.

The Commission hopes the measures will unlock new ways of channelling funding to Europe's businesses, while also playing a key role in delivering the European Green Deal¹ and the New Industrial Strategy for Europe.² By making rules safer and more digital-friendly for consumers, the Commission wants to boost responsible innovation in the EU's financial sector, especially for highly innovative digital start-ups, while mitigating any potential risks related to investor protection, money laundering and cyber-crime.

The Digital Finance Strategy

The aim of the Digital Finance Strategy (DFS) is to make Europe's financial services more digital-friendly and to stimulate responsible innovation and competition among financial service providers in the EU. The Commission's aim is to reduce fragmentation in the Digital Single Market, so that consumers can have access to financial products across borders and that financial technology (FinTech) start-ups can scale up and grow. The DFS will help ensure that EU financial

services rules are fit for the digital age, for applications such as artificial intelligence and blockchain.

Data management is also at the heart of the DFS. In keeping with the Commission's broader Data Strategy, the objective of the measures is to promote data sharing and open finance,

while maintaining the EU's very high standards on privacy and data protection.³

Finally, the DFS aims to ensure a level playing field among providers of financial services, be they traditional banks or technology companies.

The DFS sets out four main priorities:



REMOVING FRAGMENTATION IN THE DIGITAL SINGLE MARKET FOR FINANCIAL SERVICES

Scaling up across borders, which is seen as essential as online services are costly to develop but cheap to reproduce and often require deployment at considerable scale. A larger potential market operating across borders makes it easier to raise the funds needed to develop such services and gives consumers genuine access to cross border services. Firms achieving scale may also be able to provide such services at a lower price and higher quality.



ADAPTING THE EU REGULATORY FRAMEWORK TO FACILITATE DIGITAL INNOVATION

The regulatory framework for financial services should ensure that distributed ledger technologies (DLT) and artificial intelligence are used in a responsible way. Faster, more open and collaborative innovation cycles call for regular examination of, and adjustments to, EU financial services legislation and supervisory practices, to ensure that they support digital innovation and remain appropriate and relevant in an evolving market.



PROMOTING DATA-DRIVEN INNOVATION, INCLUDING ENHANCED ACCESS TO DATA AND DATA SHARING WITHIN THE FINANCIAL SECTOR

Further steps towards enhanced data sharing and openness across and within sectors, in compliance with data protection and competition rules, will enable the financial sector to fully embrace data-driven innovation. This will encourage the creation of innovative products for consumers and businesses, and will support broader policy objectives such as the creation of a single market for data. It will also contribute to facilitating access to data needed to channel funding in support of sustainable investments.



ADDRESSING THE CHALLENGES AND RISKS WITH DIGITAL TRANSFORMATION, INCLUDING ENHANCING THE DIGITAL OPERATIONAL RESILIENCE OF THE FINANCIAL SYSTEM

The Commission has found that financial services migrate to digital environments with fragmented ecosystems, comprising interconnected digital service providers falling partially outside financial regulation and supervision. Digital finance may therefore make it more challenging for the existing regulatory and supervisory frameworks to safeguard financial stability, consumer protection, market integrity, fair competition and security. To ensure that digital finance enables better financial products for consumers and businesses the Commission believes these risks must be addressed. The Commission will therefore pay particular attention to the principle "same activity, same risk, same rules", not least to safeguard the level playing field between existing financial institutions and new market participants.

By mid-2022 the Commission aims to propose amendments to the existing financial services legislative framework, and to introduce new laws where necessary, with a view to implementing the elements of the Digital Finance Strategy by 2024.

The Retail Payments Strategy

The Retail Payments Strategy (RPS) aims to bring safe, fast and reliable payment services to European citizens and businesses. Its objective is to make it easier for consumers to pay in shops and make e-commerce transactions safely and conveniently. It seeks to achieve a fully integrated retail payments system in the EU, including instant cross-border payment solutions and will take into account the findings of the Commission's review of the Payment Services Directive

(PSD2). This should facilitate payments in euro between the EU and other jurisdictions and will promote the emergence of home-grown and pan-European payment solutions.

The RPS focuses on four, interlinked, key pillars:

- Increasing digital and instant payment solutions with pan-European reach;
- Innovative and competitive retail payments markets;
- Efficient and interoperable retail payment systems and other support infrastructures; and
- Efficient international payments, including remittances.

The Commission aims to implement the key actions of the RPS by 2023.

Crypto-assets Regulation

The proposed Regulation on Markets in Crypto Assets (MiCA) aims to boost innovation while preserving financial stability and protecting investors from risks. The intention is that this should provide legal clarity and certainty for crypto-asset issuers and providers. The new rules aim to allow operators authorised in one Member State to provide their services across the EU (passporting). Safeguards include capital requirements, custody of assets, a mandatory complaint holder procedure available to investors, and rights of the investor against the issuer. Issuers of significant asset-backed crypto-assets (so-called “stablecoins”) would be subject to more stringent requirements (e.g. in terms of capital, investor rights and supervision).

The draft regulation is intended to provide legal certainty for crypto-assets not covered by existing EU financial services legislation and establish uniform rules for crypto-asset service providers and issuers at EU level. It will establish specific rules for stablecoins, including when these are classified as e-money.

Applying to crypto-asset service providers and issuers, MiCA establishes uniform requirements for transparency and disclosure in relation to issuance, operation, organisation and governance of crypto-asset service providers, as well as establishing consumer protection rules and measures to prevent market abuse.

MiCA includes the regulation of offerings and marketing to the public of crypto-assets, the authorisation of e-money token issuers, crypto-asset service providers and stablecoin issuers, and prohibitions and requirements to prevent market abuse involving crypto-assets.

Alongside MiCA, the Commission is also proposing a clarification that the existing definition of ‘financial

instruments’ - which defines the scope of the Markets in Financial Instruments Directive (MiFID II) - includes financial instruments based on DLT.

In addition, the Commission is also proposing a pilot regime for market infrastructures that wish to trade and settle transactions in financial instruments in crypto-asset form.

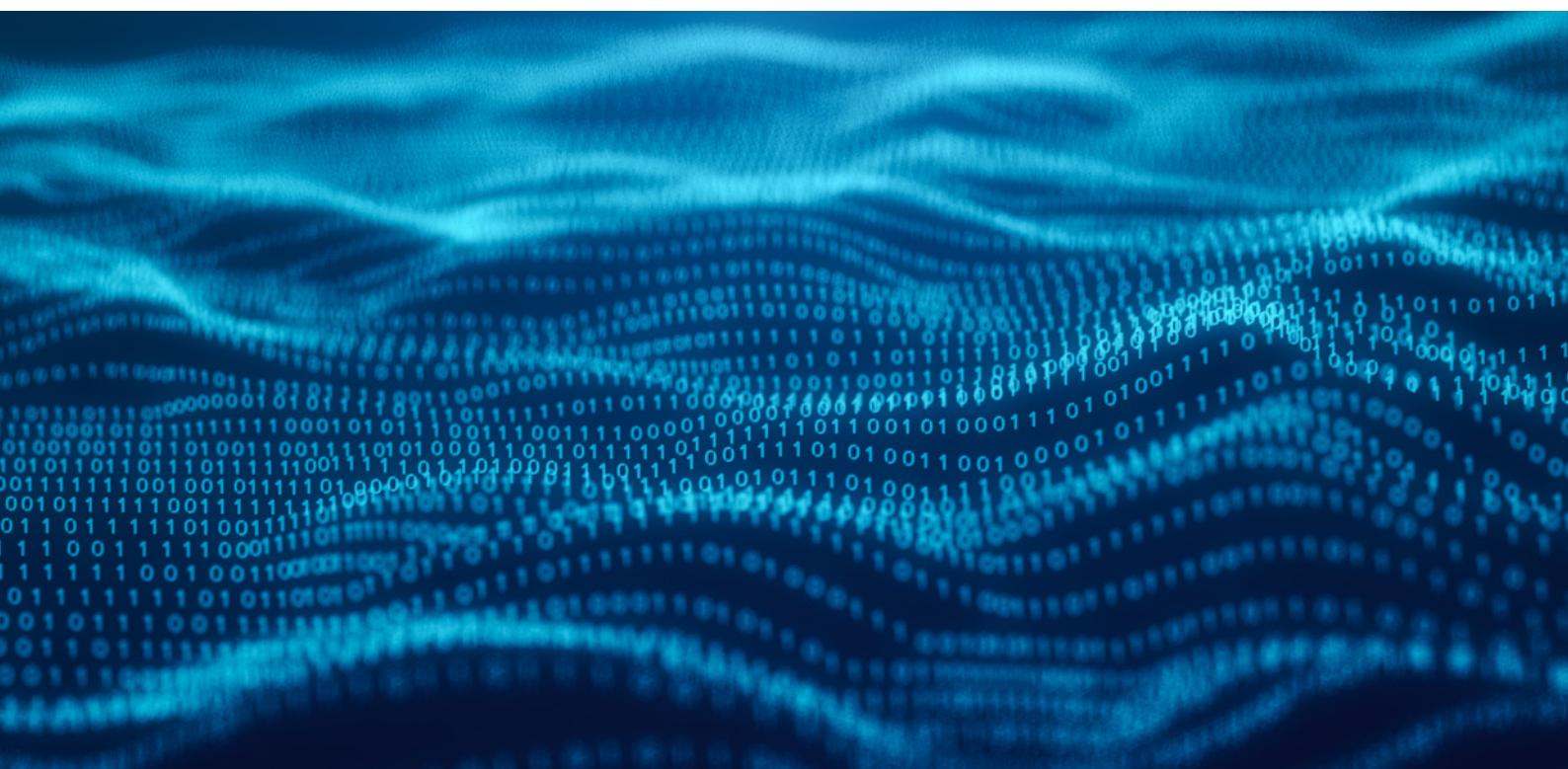
The proposal has four objectives:

- Legal certainty - for secondary markets in crypto-assets to develop the Commission has to determine where the EU financial services regulatory framework is not fit for that purpose;
- Support innovation - to promote the update of technology and responsible innovation, the pilot regime will ensure that more wide-ranging changes to existing financial services legislation are evidenced based;
- Instil consumer and investor protection and market integrity; and
- Ensure financial stability.

The pilot regime represents a sandbox approach which allows temporary derogations from existing rules so that regulators can gain experience on the use of DLT in market infrastructures, while ensuring that they can deal with risks to investor protection, market integrity and financial stability. The sandbox also allows companies to test and learn more about how existing rules fare in practice, enabling experimentation within a safe environment and providing evidence for possible further amendments.

Digital Operational Resilience

The proposed Digital Operational Resilience Act (DORA) aims to ensure that all participants in the financial system have the necessary safeguards in place to mitigate cyber-attacks and other risks. The proposed legislation will



require all firms to ensure that they can withstand all types of Information and Communication Technology (ICT) related disruptions and threats. DORA also introduces an oversight framework for ICT providers, such as cloud computing service providers.

DORA covers a very wide range of financial entities regulated in the EU, for example investment firms, managers of alternative investment funds, management companies, credit institutions, central securities depositories, amongst many others.

However, despite the seemingly one-size-fits-all scope of DORA, the Commission recognises that significant differences exist between financial entities in terms of size, business profiles, or in relation to their exposure to digital risk. As a result, the regulation takes steps to drive a proportionate, risk-based approach to ICT risk oversight.

DORA is designed to better align financial entities' business strategies and the conduct of ICT risk management. Management bodies will be required to maintain an active role in steering the ICT risk management framework, with DORA setting out a set of specific requirements, such as the assignment of clear roles and responsibilities for all ICT-related functions, continuous engagement in the control of the monitoring of ICT risk management, as well as in the full range of approval and control processes and appropriate allocation of ICT investments and training.

To keep pace with a quickly evolving cyber threat landscape, financial entities will be required to set-up and maintain resilient ICT systems and tools that minimise the impact of ICT risk, to identify on a continuous basis all sources of ICT risk, to set-up protection and prevention measures, promptly detect anomalous activities, put in place dedicated and comprehensive business continuity policies and disaster and recovery plans as an integral part of the operational business continuity policy.

Financial entities will have to establish and implement a management process to monitor and log ICT-related incidents, followed by an obligation to classify them based on criteria which is detailed in DORA and will be further developed by the ESAs. ICT-related incidents that are deemed major must also be reported to the competent authorities. Financial entities will be required to inform their users and clients where the incident has or may have an impact on their financial interests.

The capabilities and functions included in the ICT risk management framework need to be periodically tested for preparedness and identification of weaknesses, deficiencies or gaps, as well as the prompt implementation of corrective measures. DORA allows for a proportionate application of digital operational resilience testing requirements depending on the size, business and risk profiles of financial entities.

Third-party ICT risk is addressed in DORA through principles-based rules applying to financial entities' monitoring of risk, together with harmonisation of the key elements of the service and relationship with ICT third-party providers.

To enable effective oversight the contracts that govern the relationship between the financial entity and the third-party provider will be required to contain a complete description of services, indication of locations where data is to be processed, full service level descriptions accompanied by quantitative and qualitative performance targets, relevant provisions on accessibility, availability, integrity, security and protection of personal data, and guarantees for access, recovery and return in the case of failures of the ICT third-party service providers, notice periods and reporting obligations of the ICT third-party service providers, rights of access, inspection and audit by the financial entity or an appointed third-party, clear termination rights and dedicated exit strategies.

Where the ICT third-party is established in a non-EEA country the financial entity will need to also consider, at a minimum, factors covering data protection, effective enforcement of DORA, insolvency law provisions that would apply in the event of the ICT third-party provider's bankruptcy, and any potential constraints on the urgent recovery of the financial entity's data.

Finally, DORA allows financial entities to set-up arrangements, such as industry bodies, to exchange amongst themselves cyber threat information and intelligence, to raise awareness on ICT risk, minimise its spread, and support financial entities' defensive capabilities and threat detection techniques.

In addition to DORA the Commission has also proposed amendments to eight Directives, including the UCITS Directive, AIFMD, MiFID II and CRD, introducing precise cross-references to DORA which aims to ensure legal clarity.⁴

If approved, the proposed regulation could apply from Q1 2022 at the earliest. Given that proposals are at an early stage of negotiation, and given their wide scope, stakeholders will be interested in engaging in the legislative review process.

We will continue to track what has, to date, generally been welcomed by the industry.

¹ See A European Green Deal at ec.europa.eu.

² See European industrial strategy at ec.europa.eu.

³ See A European Strategy for Data at ec.europa.eu.

⁴ Proposed amendments to Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341 EU/2016/2341.

Please contact for further details:

David Morrison

Global Head of Trustee and Fiduciary Services
david.m.morrison@citi.com
 +44 (0) 20 7500 8021

Ann-Marie Roddie

Head of Product Development Fiduciary Services
annmarie.rodzie@citi.com
 +44 (1534) 60-8201

Amanda Hale

Head of Regulatory Services
amanda.jayne.hale@citi.com
 +44 (0)20 7508 0178

Caroline Chan

APAC Head of Fiduciary Business
caroline.mary.chan@citi.com
 +852 5181 2602

Shane Baily

EMEA Head of Trustee and Fiduciary Services
 UK, Ireland and Luxembourg
shane.baily@citi.com
 +353 (1) 622 6297

Jan-Olov Nord

EMEA Head of Fiduciary Services
 Netherlands and Sweden
janolov.nord@citi.com
 +31 20 651 4313

www.citibank.com/mss

The market, service, or other information is provided in this communication solely for your information and "AS IS" and "AS AVAILABLE", without any representation or warranty as to accuracy, adequacy, completeness, timeliness or fitness for particular purpose. The user bears full responsibility for all use of such information. Citi may provide updates as further information becomes publicly available but will not be responsible for doing so. The terms, conditions and descriptions that appear are subject to change; provided, however, Citi has no responsibility for updating or correcting any information provided in this communication. No member of the Citi organization shall have any liability to any person receiving this communication for the quality, accuracy, timeliness or availability of any information contained in this communication or for any person's use of or reliance on any of the information, including any loss to such person.

This communication is not intended to constitute legal, regulatory, tax, investment, accounting, financial or other advice by any member of the Citi organization. This communication should not be used or relied upon by any person for the purpose of making any legal, regulatory, tax, investment, accounting, financial or other decision or to provide advice on such matters to any other person. Recipients of this communication should obtain guidance and/or advice, based on their own particular circumstances, from their own legal, tax or other appropriate advisor.

Not all products and services that may be described in this communication are available in all geographic areas or to all persons. Your eligibility for particular products and services is subject to final determination by Citigroup and/or its affiliates.

The entitled recipient of this communication may make the provided information available to its employees or employees of its affiliates for internal use only but may not reproduce, modify, disclose, or distribute such information to any third parties (including any customers, prospective customers or vendors) or commercially exploit it without Citi's express written consent. Unauthorized use of the provided information or misuse of any information is strictly prohibited.

Among Citi's affiliates, (i) Citibank, N.A., London Branch, is regulated by Office of the Comptroller of the Currency (USA), authorised by the Prudential Regulation Authority and subject to regulation by the Financial Conduct Authority and limited regulation by the Prudential Regulation Authority (together, the "UK Regulator") and has its registered office at Citigroup Centre, Canada Square, London E14 5LB and (ii) Citibank Europe plc, is regulated by the Central Bank of Ireland, the European Central Bank and has its registered office at 1 North Wall Quay, Dublin 1, Ireland. This communication is directed at persons (i) who have been or can be classified by Citi as eligible counterparties or professional clients in line with the rules of the UK Regulator, (ii) who have professional experience in matters relating to investments falling within Article 19(1) of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 and (iii) other persons to whom it may otherwise lawfully be communicated. No other person should act on the contents or access the products or transactions discussed in this communication. In particular, this communication is not intended for retail clients and Citi will not make such products or transactions available to retail clients. The information provided in this communication may relate to matters that are (i) not regulated by the UK Regulator and/or (ii) not subject to the protections of the United Kingdom's Financial Services and Markets Act 2000 and/or the United Kingdom's Financial Services Compensation Scheme.

© 2020 Citibank, N.A. (organized under the laws of USA with limited liability) and/or each applicable affiliate. All rights reserved by Citibank, N.A. and/or each applicable affiliate. Citi, Citi and Arc Design and other marks used herein are service marks of Citigroup Inc., used and registered throughout the world.

GRA32015 11/20

