Bird & Bird

Commission Digital Finance Package Strategies

On 24 September 2020, the European Commission unveiled its Digital Finance Package. The package covers 5 key areas:

1 Digital finance strategy (DFS)

2 Retail payments strategy (RPS)

3 Draft Regulation Of Crypto-assets (MiCA)

4 Pilot regime for market infrastructures based on distributed ledger technology (DLT)

5 Digital operational resilience / cloud computing (DORA)

Our International Finance and Financial Regulation Group have reviewed the package and have summarised their key findings below.

1. Digital Finance Strategy (DFS)

The European Commission has set out a strategic objective addressing the need to drive and harness digital transformation within the EU financial sector by promoting new opportunities and tackling the risks and benefits to consumers and businesses, while ensuring an integrated and level playing field for existing and new market players.

The implementation of this strategy is based on **four instrumental targets** ("*priorities*"):

1. removing fragmentation in the Digital Single Market for financial services;
2. adapting the EU regulatory framework to facilitate digital innovation;
3. establishing a European financial data-space to promote data-driven innovation in finance;
4. addressing key-challenges and risks associated with digital transformation of the financial sector.

To achieve the **first target**, the Commission will carry out the following actions:

- implementing a harmonised pan-EU regulatory framework on the use of an interoperable digital identity, enabling consumers and firms to have quick and easy access to cross-border digital financial services which will enable safe remote "on-boarding" by financial institutions;
- redefining and harmonising customer-due-diligence (CDD) requirements to avoid having different processes in each EU Member State.

In this respect, changes and innovations to the Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) rules as well as the Electronic identification and trust services for electronic transaction Regulation (e-IDAS Regulation) will be introduced by 2024.

The new legal framework should also determine the basis which the 'on-boarding' information may be reused (e.g., 'on-boarding' with another provider, and access to other non-banking services).

- examining the need to introduce additional harmonised licensing and passporting regimes in the areas with high potential for digital finance. This would be reached through close work with the European supervisory authorities (ESAs) and the European Forum of Innovation Facilitators (EFIF);

- establishing a new EU digital finance platform to encourage cooperation between private (e.g. fintech start-ups etc.) and public stakeholders (supervisory authorities; national innovator facilitators etc.).

For this **second target,** the Commission announced specific initiatives:

- by 2024 the EU should implement **a new comprehensive legal framework for distributed ledger technology (DLT) and crypto-assets in the financial sector**, with differentiation based on a taxonomy of types of crypto-assets. In addition to this, the Commission will consider updating the prudential rules for crypto-assets held by financial firms.

Alongside these measures, the Commission supports the work of central banks, and in particular, the ECB, in considering issuing a retail central bank digital currency (CBDC) available to the general public, while safeguarding the legal tender of euro cash.

- a proposal to launch a European cloud services market by the end of 2022, integrating the various (alternative) cloud service offerings on the market, to promote the use of cloud computing solutions;

- promoting investments in software by adapting prudential rules (in the form of regulatory technical standards (RTS)) on intangible assets, in order to facilitate a transition to a more digitalised banking sector;

- promoting adoption of artificial intelligence tools by providing legal clarity – through joint work between the Commission, ESAs and ECB – **on the use of artificial intelligence (AI) applications in financial services**, possibly by developing regulatory and supervisory guidance.

This guidance should follow the upcoming proposal for a new regulatory framework for AI planned in 2021.

Finally, the Commission aims to ensure that the EU regulatory requirements for financial services do not create obstacles to the use of new technologies, through regular legislative reviews and interpretative guidance.

In relation to the **third target**, setting up a common financial data space helps integrate European capital markets, channel investments into sustainable activities, support innovation and bring efficiencies for consumers and businesses. To achieve this target, the Commission proposed a number of specific measures:

- ensuring by **2024 that publicly released information under EU financial services legislation to be disclosed in standardised and machine-readable formats**;

The Commission will implement EU infrastructure and interoperability to facilitate access to all publicly available disclosure relevant to capital markets (as part of the Capital Markets Union Action Plan).

- **development of a strategy on supervisory data in 2021** - together with the ESAs - to help ensure that supervisory reporting requirements are unambiguous, aligned, harmonised and suitable for automated reporting;

- **a legislative proposal for a new open finance framework** for business-to-business customer data sharing in the EU financial sector by **mid-2022**, building on and in full alignment with broader data access initiatives (including the upcoming Data Act, and the Digital Services Act) **and in coordination with the review of the Payment Services Directive (PSD2) in 2021**.

The PSD2 review will include an assessment of its scope in order to make a further step towards the sharing and use of customer-permissioned data by banks and third party providers to create new services.

Regarding the **fourth target,** the Commission presented proposals to address the challenges and risks associated with digital transformation of the new financial ecosystem:

- by 2024, the EU prudential and conduct regulation and supervision should be adapted to be future proof for the new financial ecosystem, including traditional regulated financial institutions and technology providers offering financial services (click here for full details);

Tech companies, especially large ones, are becoming an integral part of the financial ecosystem playing different roles at the same time: some offering payments and others financial services; others acting as intermediaries by bundling various services and products with associated financial services, thus becoming marketplaces for financial services; the big tech companies also providing the financial industry with digital technology solutions (including hardware, software and cloud-based services).

- by mid-2022, the Commission will also propose **the necessary changes to existing financial services legislative framework with respect to consumer protection and prudential rules** to protect end-users of digital finance, safeguard financial stability, protect the integrity of the EU financial sector, and ensure a level playing field between existing financial institutions and new market entrants such as technology companies;

- a proposal for a new EU framework for strengthening digital operational resilience of financial market participants and infrastructures.

2. Retail Payment Strategy (RPS)

The Retail Payment Strategy (**RPS**) follows up on the public consultation that the EC organised by the EC during the first quarter of 2020.

In the context of the upcoming review of the second Payment Services Directive (**PSD2**) in Q4 2021, this RPS provides a clearer vision of the EC's priorities and gives an indication of potential legislative proposals aim at:

- supporting innovation and digitalisation of the payment landscape, while enhancing customers' protections;
- facilitating intra-EU and extra-EU cross-border payment transactions; and
- promoting home-grown and pan-European payment solutions.

Instant payments as the 'new normal'

Instant payment means that funds are 'instantly' (more precisely, in under 10 seconds) available to the payee. This solution has been available since 2017, when the European Payment Council (**EPC**) developed the Scheme for instant payments (**SCT Inst.**). However, unlike SEPA direct debits and credit transfers, adherence to SCT Inst. is not mandatory and continues to be unpopular in many EU countries.

The EC is aiming for a full uptake of instant payments and will take the following actions:

- In November 2020, the EC will examine the number of payment service providers (**PSPs**) and accounts that are reachable under SEPA SCT Inst. It will assess whether it is appropriate to propose a legislation mandating PSPs' adherence to this scheme by the end of 2021, including adherence to additional

functionalities that would allow innovative point-of-interaction (POI) payment solutions (e.g. QR-codes). This proposal would also lay down the criteria for determining which PSPs should be subject to mandatory participation.

- Instant payment instruments are to be put on an equal footing with other payment instruments in terms of consumers' protection and fees. For example, they should be provided with a right to a refund in case of erroneous or unauthorised transactions, similar to chargebacks that are offered when using payment cards. Additionally, charges on instant payments should not be higher than those levied on regular direct debits or credit transfers (although the EC notes that there can be additional costs for the provider if some features and add-ons, such as chargebacks, are offered with instant payments).

- The EC (together with the European Banking Authority – **EBA**) will assess the resilience of payment systems, and will focus on the increased liquidity risks for financial institutions that result from instant payments.

European payment solutions

The EC will continue to play an active political role and support the development of competitive pan-European payment solutions that rely extensively on instant payments.

By the end of 2023, the EC will explore several options in this respect, such as the feasibility of developing a 'label' for eligible pan-European payment solutions, the development of European specifications for contactless card-based payments (CPACE), as well as the modernisation and simplification of EU merchants' (SMEs in particular) payment acceptance facilities.

Other actions

Other initiatives will be taken by the EC in order to promote digital and new payment solutions with pan-EU reach:

1 Reaping the full potential of the SEPA Regulation, by investigating IBAN discrimination issues and ending any illegal activity with the appropriate sanctions.
2 By 2024, adopting a sound legal framework enabling the use of interoperable digital identity solutions for customer authentication. The EC will explore the possibility of using electronic identity (eID) and solutions based on trust services (i.e. eIDAS Regulation) to support the fulfilment of Strong Customer Authentication (SCA).
3 In 2022, the EC will carry out a study on the level of acceptance of electronic payments in the EU and, if there are low levels, assess whether legislative proposals would be appropriate.
4 The EC will continue supporting the acceptance of cash payments, which still largely remain in use in the EU.
5 The EC will also propose Regulation on digital operational resilience for the financial sectors across the EU, with a view to enhancing the ICT risk management of various financial institutions, including PSPs.

Innovative and competitive retail payments markets

While PSD2 introduced open banking (i.e. access to payment accounts), some jurisdictions already offered broader open services. With this in mind, the EC plans to present a legislative proposal a new 'Open Finance' framework by mid-2022.

At the end of 2021, the EC will launch a comprehensive review of PSD2, which may potentially lead to several amendments in the following areas:

1. The EC will monitor the implementation of SCA requirements and assess its impact on the level of fraud. It will also explore whether additional measures are to be considered to address new types of fraud, in particular with regard to instant payments. The EC will in particular (together with the EBA) will re-examine the existing legal limits on contactless payments, with a view to striking a balance between convenience and fraud risks.

2. The EC will consider the potential risks associated with unregulated technical activities (in light of e.g. the Wirecard scandal) and assess whether those should be brought under the scope of PSD2.
3. Aligning PSD2 and the Electronic Money Directive (EMD2) frameworks by including the issuance of e-money as a payment service in PSD2.

Efficient and interoperable retail payment systems and other support infrastructures

1. Ensuring full, pan-European reachability for SCT Inst. is a priority for both domestic and cross-border transactions. In this respect, the EC will adopt measures by the end of 2021 that will enhance the interoperability between clearing and settlement systems (TARGET2, or TARGET Instant Payment System - **TIPS**). Additionally, these infrastructures must be available to a much greater number of other EU currencies. For example, TIPS was made available to Swedish krona in April 2020.

2. As part of the Settlement Finality Directive (SFD) review in Q4 2020, the EC will consider extending the scope of the SFD (which is mainly limited to banks) to include e-money and payment institutions.

3. The EC will promote access to technical infrastructures that are considered necessary to support the provision of innovative payment solutions, such as the NFC technology in mobile phones in order to allow contactless payments. This is of course a direct reference to the technical lock that Apple have placed around the NFC antenna in iPhones – see our previous alerts on this topic here, here and here. It will assess whether a legislative proposal is needed and consider the potential security and other risks such access could pose. In particular, it would lay down the criteria for identifying the necessary technical infrastructures and determining to whom and under what conditions access rights should be granted.

Efficient international payments, including remittances

Cross-border payments involving non-EU countries must become faster, more affordable, more accessible, more transparent and more convenient. The EC holds the view that it would encourage greater use of the euro and strengthen its position as a global currency.

The following actions can be expected:

1. Facilitating linkages between European payment systems (e.g. TARGET2, TIPS) and instant payment systems of third countries, or even with other types of payment systems (e.g. retail payment systems). This would be subject to appropriate level of consumer protection, fraud and ML/TF prevention and interdependencies risks mitigation measures.
2. Implementing (by the end 2022) global international standards which facilitate inclusion of richer data in payment messages (e.g. ISO 20022) and using SWIFT's Global Payment Initiative (GPI), which facilitates the tracking of cross-border payments for participating institutions in real time.
3. In the context of the PSD2 review, assessing the appropriateness of requiring that the maximum execution time in 'two-leg' transactions also applies to 'one-leg' transactions. Additionally, the EC is following the ongoing work carried out in the framework of the EPC on possible further harmonisation of business rules and messaging standards for one-leg transactions with great interest. This should determine whether it is necessary to make these changes mandatory.

3. Draft Regulation Of Cryptos (MiCA)

With the MiCA proposal, the EU wishes to pursue the Digital Finance Strategy. Common regulations for all EU Member States are meant to address the opportunities and risks in the best possible way. Germany had already taken the lead in implementing the fifth EU Money Laundering Directive (AMLD5) by regulating the crypto-custody business as a new financial service. At the same time, Germany is working on an act for electronic securities (eWpG), which covers and further regulates the crypto-asset sector.

The proposal on MiCA aims to regulate these issues at EU level and to create legal certainty across Europe. This would allow a larger number of investors to be active in this field and to use distributed ledger technology (DLT). At the same time, innovation and development will be encouraged. The MiCA rules are designed to ensure that financial stability is guaranteed.

Aim: What is regulated?

The MiCA's proposal aims to establish a harmonised set of transparency and disclosure requirements for the issuance and trading of crypto-assets. There will also be rules on the admission and supervision of providers of crypto-assets and their issuers – the focus will be on issuers of asset-referenced tokens and e-money tokens. The Regulation is intended to regulate the operation, organisation and management of issuers of asset-referenced tokens and e-money tokens as well as crypto-assets service providers. There will also be consumer protection rules for the issuance, trading, exchange and custody of crypto-assets. The draft Regulation also include measures to prevent market abuse in order to ensure the integrity of the crypto-asset markets.

Crypto-assets: What is covered?

The MiCA is designed to complement existing regulations. It is intended to cover companies that issue crypto-assets or provide services related to crypto-assets. Explicitly excluded from the scope of application are crypto-assets that are already covered by other regulations, such as financial instruments under MiFID II, e-money under the E-Money Directive (EMD2), deposits under the Deposit Guarantee Directive or securitisations under the Securitisation Regulation.

In addition, the Regulation will not apply to certain organisations. The exceptions include, among others, any company providing crypto-asset services to group companies only. Credit institutions, financial services institutions and payment institutions are exempted from certain provisions of the MiCA.

In detail: What is a crypto-asset?

The MiCA draft defines a crypto-asset as the digital representation of a value or right, which may be transferred and stored electronically, using the DLT or similar technology. The draft MiCA divides crypto-assets into the following subcategories:

- asset-referenced tokens: This refers to such crypto-assets whose main purpose is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of several fiat currencies, one or several commodities, or one or several crypto-assets, or a combination of such assets. This category includes stablecoins.
- electronic money token or e-money token: This refers to crypto-assets whose main purpose is to be used as a means of exchange and that purports to maintain a stable value by being denominated in (units of) a fiat currency. The scope of application needs to be clearly defined, as according to EMD2 crypto-assets which are electronic money are not covered by MiCA.
- Utility Token: This refers to crypto-assets which are intended to provide digital access to an application, services or resources available on a distributed ledger and are accepted only by the issuer of that token to grant access to such application, services or resources available.

Asset-referenced tokens and e-money tokens can each be classified as significant asset-referenced tokens or significant e-money tokens under the draft Regulation. In this case, issuers are subject to more stringent requirements.

Offer and marketing of crypto-assets

The MiCA will establish rules for the offering and marketing of crypto-assets by their issuers. A distinction will be made between asset-referenced tokens and e-money tokens on one hand and other crypto-assets on the other. For the other crypto-assets, the issuer must prepare and publish a whitepaper and notify the competent authority. The whitepaper must describe, among other things, the main features of the crypto-asset and the risks associated with them. It is therefore similar to a prospectus requirement. The issuer must also be a legal entity and must comply with certain conduct requirements.

There are exceptions to these regulations, e.g. free offers of crypto-assets or if the total consideration of the offering does not exceed EUR 1,000,000 within 12 months.

Issuance of asset-referenced tokens

Stricter requirements are imposed on the issue of asset-referenced tokens. The issuer must meet certain requirements and must have a licence from the competent authority. Whilst credit institutions do not need a special licence they must comply with the general rules. Asset-referenced tokens are also subject to a kind of prospectus requirement. However, not only does the whitepaper have to be published, it must also be approved by the competent authority.

The general requirements for the issuer of asset-referenced tokens stipulates the issuer must be an established legal entity within the EU. The issuer is subject to certain rules of conduct; issuers must also meet capital requirements of at least EUR 350,000 in own funds. An authorisation as issuer to issue asset-referenced tokens should be valid throughout the EU. However, supervision will remain with the competent authority of the EU Member State where the issuer has its registered office. If an issuer issues significant asset-referenced tokens, it will be subject to more stringent requirements. Supervision would then be carried out by the EBA.

The rules should not apply if the asset-referenced tokens are distributed only and can only be held by professional investors or, if the number of asset-referenced tokens issued does not exceed EUR 5,000,000 over a period of 12 months. Stablecoins, which obtain their value through an algorithm that regulates the value by the number of tokens referenced on supply and demand, also fall outside the scope of this regulation.

Issuance of e-money tokens

The MiCA will also have special requirements for the issuance of e-money tokens. It is envisaged that e-money tokens may only be issued by credit institutions and e-money institutions. A whitepaper must also be prepared for e-money tokens and notified to the competent authority. Moreover, many provisions in the E-Money Directive are also applicable, such as the prohibition of interest. In this context, e-money tokens are not e-money - the MiCA does not apply to crypto-assets that represent e-money under the e-Money Directive.

These rules do not apply if the e-money tokens are only distributed and can only be held by professional investors or the number of e-money tokens issued does not exceed EUR 5,000,000 over a period of 12 months.

Licensing and operating conditions for crypto-asset services providers

The provision of crypto-asset services will also be regulated. Only legal entities established and licensed in the EU will be allowed to provide these services - the licence would be valid for the whole EU (passporting). This offers a decisive advantage when compared to individual national regulations currently in force, which have to be examined separately by companies - which regularly means a great effort In addition to capital requirements (dependant on the type of service provided), there are requirements for the management (necessary good repute and competence, in terms of qualifications, experience and skills, committing sufficient time). The shareholders of the service providers must also be of the necessary good repute and competence.

The service providers also make provisions for conflicts of interest, information requirements and outsourcing. Depending on the activity the service provider offers, further requirements will apply - ESMA is to maintain a register of service providers.

Conclusion

After a first review of the draft MiCA, it can be concluded that the proposed rules provide a clear regulatory framework for the European crypto-asset sector. This proposal will ensure that national regulations do not hinder the development of the crypto-asset sector. The fact that a regulation rather than a directive has been chosen as the means of regulation may initially seem surprising, yet it will prevent Member States from being "gold-plated", which will make this sector even more harmonised than other financial services.

4. Pilot regime for market infrastructures based on distributed ledger technology

It is considered that existing provisions in EU legislation may inhibit the use of DLT in relation to regulated securities trading but that it would not be wise to make wholesale changes to such legislation without testing out changes on a more limited pilot basis. The Proposal is part of a wider effort to establish a regulatory framework for DLT and crypto-assets (most of which are not regulated securities) which encourages innovation while sufficiently mitigating risks. The Proposal implicit acknowledges that there are limits to reliance on only the "technology neutral" approach (i.e. applying existing regulation purposively to new technological approaches) and that sometimes specific enabling regulation changes are required.

The Regulation is, at this stage, only a draft proposal for a regulation which is yet to go through the normal EU legislative process.

Four objectives of the Proposal:

The Proposal has four general objectives:

1. **Legal Certainty**: for secondary markets in those crypto-assets which qualify as regulated securities, to develop a pilot EU framework which will enable them to be traded using DLT;

2. **Supporting Innovation**: to promote the uptake of technology and responsible innovation (the core of the Commission's financial services strategy) by removing potential obstacles derived from regulation;

3. **Consumer & investor protection and market integrity**: to develop and implement appropriate safeguards for DLT-based trading in appropriate financial instruments; and

4. **Financial stability**: to acknowledge that DLT technologies should nonetheless not be exempt from financial stability requirements.

Specific provisions of the Proposal:

Below we set out an overview of the provisions of the proposed Regulation:

Article 1 and 2 – Scope and definitions

The Regulation concerns 'DLT market infrastructures' meaning:

- a 'DLT multilateral trading facility' (a **DLT MTF**) – a multilateral trading facility (as defined in the Markets in Financial Instruments Directive II - **MiFID II**) which only admits 'DLT transferable securities' to trading; and
- a 'DLT securities settlement system' (a **DLT SSS**) - a securities settlement system operated by a central securities depository (as defined in the Central Securities Depositories Regulation, a **CSDR**), which settles transactions in DLT transferable securities.

A 'DLT transferable security' is any transferable security (as defined in MiFID II) which is issued, recorded, transferred or stored using DLT.

Article 3 – limitations on DLT transferable securities

Article 3 outlines the limitations in terms of DLT transferable securities that can be admitted to trading on a DLT MTF or recorded by a DLT SSS. These include:

1. a limit, to less than EUR 200m, on the market capitalisation of issuers of shares traded on DLT marketplaces

2. a limit, to less than EUR 500m, on the issuance size of debt instruments traded using DLT technology;

3. a limit, to EUR 2.5 billion, on the total market value of DLT transferable securities that can be recorded within a DLT SSS; and

4. a restriction on the trading of sovereign bonds using DLT technology.

Article 4 – requirements for a DLT MTF

Article 4 sets out the requirements for a DLT MTF. While the operator of a DLT MTF will generally be subject to the same requirements as for operating a traditional multilateral trading facility, some requirements will not apply if certain conditions are met – most notably the requirement for transferable securities to be recorded with a central securities depository.

Article 5 – requirements for a DLT SSS

Article 5 sets out the requirements which apply to a DLT SSS. These requirements are generally the same as those for a traditional central securities depository but this Article also sets out certain potentially available exemptions.

Article 6 – additional requirements for DLT market infrastructures

Additional requirements in this Article, some of which apply to the operator of a DLT MTF and others to the operator of a DLT SSS, are designed to address new forms of risk raised by the use of DLT and include: (i) providing all members, clients, participants and investors with clear and unambiguous information on how they carry out their functions, services and activities and how these differ from a traditional multilateral trading facility or central securities depository; and (ii) ensuring that the IT and cyber security arrangements used for DLT market infrastructures are adequate.

Articles 7 and 8 – specific permission to operate a DLT MTF or DLT SSS

These Articles set out the procedure for obtaining permission to operate a DLT MTF or DLT SSS and includes details as to the information which must be submitted when applying for permission. The Regulation anticipates that permissions will be granted by the national competent authority in close co-operation with the European Securities and Markets Authority (**ESMA**). A permission is valid throughout the Union for a six-year period. These Articles also set out circumstances where a previously-granted permission can be withdrawn.

Article 9 – cooperation between a DLT market infrastructure, the competent authorities and ESMA

Article 9 outlines what cooperation is required between a DLT market infrastructure and its national competent authority and ESMA – for example a requirement to notify:

1. proposed material changes to its business plan;

2. evidence of hacking, fraud or malpractice;

3. material changes to information contained in the initial application;

4. technical or operational difficulties in delivering the activities or services covered by its permission; and

5. any risks to investor protection, market integrity or financial stability that may have arisen.

This information will clearly be important in making the assessment referred to in Article 10.

Article 10 – report and review

This Article provides that, no later than five years after the application of the Regulation, ESMA will produce a detailed report on the pilot regime to the Commission. The Commission will use this assessment to determine whether the pilot regime should be maintained in its current form, amended and/or extended (e.g. to cover further new categories of financial instrument) or terminated and whether targeted amendments to EU legislation should be considered to enable a widespread use of DLT.

5. Digital operational resilience / cloud computing

Proposal on digital operational resilience for the financial sector

The proposal is part of a digital finance package that aims to support the future potential of digital finance in terms of innovation and competition while mitigating the risks entailed. The goal is to prepare the EU economy for a digital revolution, and to ensure that it embraces it.

According to European Commission (EC), until now there has been a limited and incomplete regulatory focus on ICT (Information and Communication Technologies) risks, especially in the EU financial sector. The proposal aims to regulate these issues at EU level and harmonise the requirements in all Member States.

The idea is to achieve a high level of harmonised digital operational resilience applicable to all financial entities in the EU. Current disparities in this area have been identified by the EC as obstacles to achieving harmonization and the resilience that will produce. The EC also argues that ICT risks pose a challenge to the performance and stability of the EU economy.

It has also been observed that competition amongst similar financial entities operating in different Member States may be distorted, especially in areas where Union harmonisation has been absent or very limited, for example: digital operational resilience testing or the monitoring of ICT third-party risk.

Name of the draft Regulation

Proposal for *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014 and (EU) No. 909/2014* (the "**Regulation**")

The Regulations that will be amended

1. Regulation of the European Parliament and of the Council on credit rating agencies
2. Regulation of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories
3. Regulation of the European Parliament and of the Council on markets in financial instruments and amending Regulation (EU) No 648/2012
4. Regulation of the European Parliament and of the Council on improving securities settlement in the European Union and on central securities depositories

Application: Whom will it concern?

The Regulation applies mainly to **financial institutions.** In Article 2 the following entities are listed:

- credit institutions
- payment institutions
- electronic money institutions
- investment firms
- crypto-asset service providers
- issuers of crypto-assets

- issuers of asset-referenced tokens and issuers of significant asset-referenced tokens
- central securities depositories
- central counterparties
- trading venues
- trade repositories
- managers of alternative investment funds
- management companies
- data reporting service providers
- insurance and reinsurance undertakings
- insurance intermediaries and ancillary insurance intermediaries
- institutions for occupational retirement pensions
- credit rating agencies
- statutory auditors and audit firms
- administrators of critical benchmarks
- crowdfunding service providers
- securitisation repositories
- ICT third-party service providers

Summary

The Regulation will introduce unified standards for:

1. **ICT risk management** (directed towards financial institutions), including: the governance and organisation thereof; the creation of a regularly reviewed and audited ICT risk management framework; protection and prevention (ICT security strategies, policies, procedures, protocols and tools); detection, response and recovery; backup, information sharing and competence building measures;

2. **A unified reporting scheme** (directed towards financial institutions), including: the classification of ICT-related incidents; content and format reporting; and the centralisation of reporting;

3. **Digital operational resilience testing** (directed towards financial institutions and testers), including: testing tools and processes (technical standards to be prepared by the **ESA - European Supervisory Authorities**, which is a joint name for the EBA, ESMA and EIOPA);

4. **Measures for sound management by financial entities of ICT third-party risk,** including:

– requirements in relation to contractual arrangements concluded between ICT third-party service providers and financial institutions

– an oversight framework for **critical ICT third-party service providers** when providing services to financial entities, including procedures and conditions for the designation of critical ICT third-party service providers, Lead Overseers (EBA, EIOPA, ESMA), tasks, and enforcement mechanisms. Imposing daily **Administrative penalties** amounting to 1% of the average daily worldwide turnover of the ICT third-party service provider in the preceding business year, but imposed for a period of no more than six months. **Criminal liability** will be decided at the Member State level, and Member States are to ensure that appropriate measures are in place so that the competent authorities have all the necessary powers to liaise, and the ability to cooperate with other competent authorities and the EBA, ESMA or EIOPA as mentioned above.

Critical ICT third-party service providers

The proposal provides a definition of 'critical ICT third-party service provider' that refers to key ICT providers for the financial sector. To ensure that ICT third-party service providers fulfilling a critical role in the functioning of the financial sector are commensurately overseen on a Union scale, one of the ESAs will be designated as **Lead Overseer** for each critical ICT third-party service provider. Critical ICT third-party service providers are **administratively designated**, in a similar manner to the way key service operators or critical infrastructure operators are designated under the Directive on security of network and information systems (NIS Directive) and its local implementations.

The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum, would designate ICT third-party service providers that are critical, and would appoint either an **EBA, ESMA or EIOPA** as a Lead Overseer for each critical ICT third-party service provider.

The designation of critical ICT third-party service providers will be based on the following criteria:

1. The systematic impact on the stability of the financial market in the event of the ICT third-party service provider facing large-scale operational failure (the number of financial entities affected);

2. The systemic importance of the financial entities that depend on the ICT third-party service provider;

3. The critical nature of the financial institution functions and processes supported by the ICT third-party service provider;

4. The degree of substitutability of the ICT third-party service provider;

5. The number of Member States in which the ICT third-party service provider provides services;

6. The number of Member States in which the financial institution using the ICT third-party service provider operates.

Timing

Currently, this is only a proposal, and will take time until it becomes binding law.

According to the proposal, the Regulation would enter into force 20 days after it is published.

It would apply from 12 months after its entry into force, except for Articles 23 and 24 (advanced testing and requirements for testers), which would apply as from 36 months after its entry into force.

Conclusion

The work on the proposed Regulation should be closely monitored by EU financial entities and major ICT third-party service providers – especially big cloud service providers.

Currently, it is difficult to assess which specific entities would be designated as critical ICT third-party service providers. It appears that only the largest ICT/cloud computing service providers will meet the criteria.

In practice, financial entities will need to ensure their agreements with ICT third-party service providers comply with the key contractual provisions required by the Regulation and allow them to monitor ICT-related risks and fulfil their new reporting duties.

This may require a review of contractual arrangements at many levels of the outsourcing chain, and will not only affect CT third-party service providers, but potentially their subcontractors too.

However, such reviews will not be necessary until the Regulation has entered into force, as now its final scope is known. We believe that it may take several months before the Regulation is adopted, and even then, additional technical regulatory standards will continue be proposed in the year after the Regulation enters into force (Article 27).

twobirds.com

Abu Dhabi & Amsterdam & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw & Satellite Office: Casablanca