MASON HAYES & CURRAN

Financial Services Sector Update

In Brief

Autumn 2024

MHC.ie

Welcome

Welcome to the autumn edition of our Financial Services Sector Update series. In this issue, we examine a selection of topics and trends impacting our clients.

Financial Services Sector lead partner, Liam Flynn introduces our autumn update, which focuses on three major themes impacting our clients including:

- Financial innovation and the digital economy
- Customers and treatment of consumers, and
- ESG and sustainability, a key priority for regulated firms

Key Contacts

Liam Flynn
Partner,
Financial Services Sector Lead
lflynn@mhc.ie

Neil Campbell
Partner,
Head of Financial Services
ncampbell@mhc.ie

Anthony O'Hanlon
Partner,
Financial Services
aohanlon@mhc.ie

Rowena Fitzgerald
Partner,
Co-head of Financial Regulation
rfitzgerald@mhc.ie

Contact our Financial Services Sector team

Top Questions Regulated Firms Should Ask About CSDDD

Liam Flynn
Partner,
Financial Services Sector Lead
lflynn@mhc.ie

Joanne O'Rourke
Of Counsel,
Financial Services
jorourke@mhc.ie

There has been much debate at European level as to how and to what extent Corporate Sustainability Due Diligence Directive (CSDDD) obligations should apply to regulated financial services providers (RFSPs). During the negotiation process, RFSPs argued that it was unreasonable to expect firms to conduct sustainability due diligence on all the financial services they provide to third parties.

However, a compromise has been reached. The official publication of the CSDDD confirms that certain RFSPs will be required to carry out due diligence regarding their own operations but will have a carve-out for the financial services they provide, i.e. their "downstream" activities.

Which financial institutions will CSDDD apply to?

CSDDD will apply to RFSPs, including banks, investment firms and insurance companies, which meet the size criteria set out in CSDDD. Essentially, CSDDD applies to companies with more than 1,000 employees on average and a net worldwide turnover of more than €450 million in the last financial year. It also applies to the ultimate parent company of a group which reached those thresholds in the last financial year. Certain non-EU companies and companies who enter into franchise or licence agreements may also fall within scope if they meet specific criteria.

When will CSDDD obligations apply to in-scope RFSPs?

CSDDD entered into force on 25 July 2024 and must be transposed into Irish law by 26 July 2026. CSDDD will apply on a phased basis:

- On 26 July 2027 for EU companies with more than 5,000 employees and which generated a net worldwide turnover of more than €1.5 billion in the previous financial year
- On 26 July 2028 for EU companies that had more than 3,000 employees and generated a net worldwide turnover of more than €900 million in the previous financial year, and
- On 26 July 2029 for EU companies with more than 1,000 employees and a net turnover in excess of €450 million

What will CSDDD compliance entail?

In-scope RFSPs will need to engage in risk-based human rights and environmental due diligence on their operations. This will include:

- Integrating due diligence into policies and risk management systems
- Identifying and assessing actual and potential adverse human rights impacts and adverse environmental impacts from their own operations

- Establishing and maintaining a complaints procedure for persons who have legitimate concerns regarding actual or potential adverse impacts of an RFSP's operations, and
- Monitoring the effectiveness of their due diligence policy and measures

In-scope RFSPs will also need to adopt and put into effect a transition plan for climate change mitigation. The transition plan approach aims to ensure, through best efforts, compatibility of the business model and of the strategy of the company with the transition to a sustainable economy, and with the limiting of global warming to 1.5C in line with the Paris Agreement.

Importantly, RFSPs which have already produced a transition plan for CSRD purposes will be deemed to comply with this CSDDD obligation.

Where should in-scope RFSPs start?

The transposition date of 2026 may seem far away to many. However, in-scope RFSPs should not underestimate the amount of preparatory and implementation work which will be required to meet CSDDD requirements.

RFSPs should take note that CSDDD's scope goes well beyond simply reporting sustainability data. CSDDD will require RFSPs to take a proactive stance when it comes to sustainability including:

- Preventing and mitigating potential and actual adverse impacts
- Bringing actual adverse impacts to an end, and
- Publicly communicating on due diligence

CSDDD will require an enterprise-wide level of engagement which Boards and senior management should prepare for. In addition, CSDDD will oblige in-scope RFSPs to consult with employees and their representatives and interested stakeholders.

Comment

In-scope RFSPs should note the potential for significant financial penalties for infringements of CSDDD. CSDDD provides that Member States shall ensure that the maximum limit of monetary penalties for infringements shall be not less than 5% of the net worldwide turnover of the company in the financial year preceding the decision to impose the fine.

We advise that in-scope RFSPs get a head start on CSDDD now. RFSPs should consider:

- Mapping chains of activities
- Identifying stakeholders who will need to be engaged
- Assessing contractual arrangements which will need to be uplifted
- Setting up a cross-functional team to execute an implementation plan, and
- Identifying a board member who can be an "ESG champion" to spearhead the process

Our Financial Regulation and Corporate Governance teams have extensive experience advising on sustainability matters and would be happy to provide support to your implementation plan.

A Welcome Update on MiCAR Authorisation Process

Rowena Fitzgerald
Partner,
Co-head of Financial Regulation
rfitzgerald@mhc.ie

Sarah Cloonan
Partner,
Financial Regulation
scloonan@mhc.ie

The Central Bank of Ireland (CBI) has provided further insight into its intended approach to the implementation of the Markets in Crypto Assets Regulation (MiCAR). In this article, we consider the key factors for firms intending to apply to the CBI for authorisation to provide crypto asset services in Ireland and the EU.

Overview

The main objective of MiCAR is to create a harmonised EU regulatory regime for crypto assets, that both promotes innovation and prioritises consumer protection. MiCAR will impose significant consumer protection measures on crypto asset service providers (CASPs), as well as obligations regarding areas including governance, minimum capital, transparency, and market abuse.

CASPs must be authorised by the CBI to operate within the EU as and from 30 December 2024. The CBI has been preparing for this and has established a cross-sectoral team to integrate MiCAR into its supervisory and authorisation processes.

Potential CASP applicants should note that the CBI's approach to regulation is underpinned by a strong consumer protection rationale. As such, the CBI will have high expectations regarding the ability of firms to manage consumer risk relating to its crypto products and services.

The CBI's general engagement principles and authorisation expectations

The CBI has outlined its main authorisation and supervisory expectations for CASPs as:

1. **Transparency**: firms must be fully transparent and open with respect to their MiCAR global and EU strategy
2. **Supervisability**: the CBI will not authorise a firm where it forms the view that the firm is not operating in an independent and autonomous manner
3. **Preparedness**: firms must be adequately resourced to engage with the CBI in a robust and timely manner throughout the authorisation process, and
4. **Consumer focus**: securing the interests of customers must be the focus of a firm's application, particularly for retail facing firms

The CBI has stated that it is "highly sceptical" of CASP business models which involve the marketing, offering or distribution of unbacked crypto assets to retail investors.

CASP authorisation process

The CBI has encouraged firms who intend to apply for CASP authorisation to engage with the CBI as early as possible, either via their existing supervisor, for firms with an existing regulatory relationship with the CBI, or via the CBI's Innovation Hub.

The CBI will then hold an introductory meeting with the firm, to outline its expectations and to allow the firm an opportunity to present an outline of its business model. A presentation on the firm's proposal should be submitted to the CBI at least five working days in advance of this meeting. The CBI will provide details to firms on the expected content of this presentation.

Following the introductory meeting, the CBI will arrange a more formal pre-application meeting with the firm, in advance of which the firm must submit a "Key Facts Document" (KFD) setting out an overview of the firm's proposed business plan and details of its shareholders. The CBI will publish a standard KFD template and guidance for firms in due course. At the pre-application meeting, the firm will be questioned by the CBI on its KFD and can ask questions of the CBI regarding the application process. The CBI will communicate to the firm any issues it has identified that need to be addressed before the application can proceed to the application phase.

Following this, the firm will be invited to submit a CASP authorisation application form. The CBI will have 25 working days to assess the completeness of the application and may request additional information within a timeframe set by the CBI if it deems the application incomplete. The CBI may refuse to review applications which remain incomplete after the expiry of the timeframe given to applicants to submit outstanding items.

When the CBI deems the application complete, it will begin the 40 working-day assessment of the application. The CBI may request additional information from the applicant, resulting in one suspension of the assessment period of no more than 20 working days.

Firms should be aware that they will have to devote significant time and resources to preparing and completing the application. The CBI will scrutinise the following aspects of a firm's application:

- Local governance and risk management arrangements, including the firm's substance and autonomy in Ireland. The CBI will expect the senior management to be crypto-competent with a good understanding of the regulatory environment in which the firm will operate.
- The firm's system to identify and remedy conflicts of interest and prevent risks to customers arising due to such conflicts.
- The protection of client assets. The firm must have full control over client crypto-assets and funds, including the proper segregation and reconciliation of same.
- The ownership and operating structure of the firm, including the identity of direct and indirect shareholders as well as any party who can exercise influence over the firm.
- The firm's business strategy, which must demonstrate the viability and resilience of the business model and reflect any vulnerabilities stemming from the product offering.
- The risk management practices and internal controls in place to ensure compliance with Irish anti-money laundering and counter terrorist financing legislation.
- The firm's plan to support the operational resilience of the firm.
- The firm's plan to support an orderly wind-down of its activities and the timely return of customer crypto-assets and funds.
- How the firm will secure the interests of customers and how the firm will assess the risk associated with its product offering.

When the CBI's assessment of the application is complete, it will communicate the outcome of the assessment to the applicant within 5 working days of its decision.

The CBI has indicated that the length of a CASP application will depend on the nature, scale and complexity of the firm and the extent of preparedness of the applicant. It also stated that it is important for applicants to distinguish between the 'pre-application'/initial engagement stage and the formal application stage.

The CBI is now advising all applicant VASPs to pursue a CASP application, on the basis that a VASP application takes at least 10 months. Any VASP not registered and operating as a VASP by 30 December 2024 cannot avail of the transitional arrangements under MiCAR. It also stated that any VASP not intending to apply for a CASP authorisation should establish clear wind-down plans and make arrangements to cease providing services by the end of the transitional period provided under MiCAR.

Consumer protection in the context of MiCAR

As mentioned, the CBI is mandated to ensure that the best interests of customers are protected through effective regulation. The CBI's Consumer Protection Code (CPC) is binding on regulated entities operating in the State, although its mandate regarding virtual asset service providers (VASPs) does not extend to consumer protection.

The CBI is currently conducting a comprehensive review of the CPC which is focused on securing consumers' interests. The CPC will be replaced by CBI Regulations which will be published in early 2025. A 12-month implementation period is proposed from the date of publication.

Firms intending to apply for authorisation as a CASP should be aware that the scope of the CPC is likely to be expanded to apply to CASPs. The CBI is currently considering how the CPC will interact with MiCAR and whether any gaps will exist in terms of consumer protection and how those gaps may be addressed through the CPC.

Conclusion

The CBI will publish its CASP application form in due course. Firms intending to apply should start preparing as soon as possible to ensure that they have all of the relevant information, policies and processes in place to ensure that they will be ready to submit their applications, having regard to the EBA and ESMA level 2 and 3 texts providing greater granularity on MiCAR requirements for CASPs.

Our Financial Regulation team has extensive experience advising crypto operators and is assisting firms who are interested in applying for authorisation under MiCAR. Please reach out to a member of our team should you require advice and support in this area.

Lessons from the Central Bank's Fitness and Probity Process Review

Liam Flynn
Partner,
Financial Services Sector Lead
lflynn@mhc.ie

Stephen McVeigh
Senior Associate,
Financial Regulation
smcveigh@mhc.ie

Assessment of the fitness and probity, or F&P, of senior executives of regulated firms is an important pillar of the Central Bank of Ireland's regulatory oversight. It is critical for both regulators and customers that senior managers of financial firms should be honest, highly competent and diligent. Ireland's F&P approval system has existed since 2010. However, partly due to fear of publicity in a small and close-knit business community, it has been very rare for firms and individuals to challenge negative Central Bank F&P decisions. This makes a recent Irish case and its aftermath more noteworthy. In this case, the Central Bank's approach to F&P assessment was severely criticised, resulting in an immediate independent review and recommended future process changes.

Independent review

The Irish Financial Services Appeals Tribunal delivered its ruling in *AB v the CBI* in February 2024[1]. The Appeals Tribunal ruling was highly critical of the approach adopted by the Central Bank in conducting interviews as part of its assessment of senior executives, known as pre-approval-controlled function-holders, or "PCFs". The ruling found that the Central Bank had given insufficient and inappropriate notice to the complainant regarding material to be discussed at interview. In addition, it was noted that the Central Band had adopted a detailed line of questioning which was more akin to an enforcement investigation than an assessment interview.

Following the ruling, the Central Bank commissioned Mr Andrea Enria, former Chair of the ECB Supervisory Board to lead an independent review of its processes.

The review report found overall that the Central Bank's F&P process is broadly aligned with the approach adopted by regulators in comparable jurisdictions and is neither more stringent nor more lenient. Despite this appraisal, the review report made recommendations to the Central Bank to enhance and improve the process, which the Governor has since publicly committed to implementing.

Findings and recommendations

The review report recommended that steps should be taken to improve the consistency of the F&P assessment process across firms of different sizes and operating in different financial sectors. Like the Appeals Tribunal, it highlighted concerns regarding the conduct of interviews by the Central Bank, noting issues concerning:

- Lack of timely notice
- Insufficient clarity on topics to be discussed, and
- A confrontational tone adopted at interviews.

The review report references interview processes employed by the Dutch and UK regulators to support recommended changes.

Senior managers and directors can expect revised and enhanced F&P standards and guidance to be published in due course by the Central Bank due to the review report.

[1] *Appeal No. 029/2022, available at https://www.ifsat.ie/decisions/ab-v-the-central-bank-of-ireland/*

Overall, the report recommends a reduction in PCF roles and the number of individuals called for interviews. However, this approach is not the case for fund directors where increased scrutiny is proposed due to the sector's systemic footprint.

The report calls for an enhanced review process within the Central Bank for applicant rejections, with proposed rejection decisions to be escalated to either a committee or senior decision-maker.

Most importantly and practically for individuals who are called to interview, the report recommends that they should be provided with at least five working days' notice. It also proposes that interviews themselves should be kept below 90 minutes and that the interview style should be conversational rather than investigatory. The report also states that the current Central Bank practice of conducting an initial 'appraisal' interview followed by a more formal interview where concerns are identified should not continue. The report confirms that the aim should be for only one interview with a candidate to be conducted.

The review report further comments on the Central Bank's current lack of clarity as to how collective suitability and diversity within boards and management teams is assessed and recommends that further guidance in this area should be provided. This is timely, given that on 24 July 2024, the European Central Bank launched a consultation on its revised draft guide on governance and risk culture for significant banks, which is set to replace the 2016 SSM supervisory statement on governance risk appetite.

The ECB draft guide places particular emphasis on the need for management bodies of regulated banks to have the right composition of members. While each member of the management body must be individually suitable, the ECB has stressed the need for F&P assessments to consider if a management body is collectively able to understand the risks facing a firm, proportionate to its size, complexity and risk profile. Regulated firms have grown accustomed to the Central Bank applying "soft pressure" to influence the composition, diversity and skillset of boards. The ECB draft guide suggests that inappropriate board composition could itself become a ground for refusing F&P approval going forward.

Comment

The introduction of the Central Bank's individual accountability and senior executive responsibility framework (IAF/SEAR) is, in our view, likely to be used over time by regulators to further increase their expectations of individuals working in the financial industry. In the UK, non-financial misconduct, i.e., behaviour by individuals in their personal lives, has been a basis for denying their F&P and withdrawing their ability to work in the industry since 2018. Indeed, the UK Financial Conduct Authority wrote to 180 London banks in February 2024 requesting information regarding sexual misconduct, harassment and bullying as part of a market review of non-financial misconduct. This approach indicates the FCA's focus on these areas is increasing. Regulators' scrutiny of individuals' actions, both at work and outside, is ever more intensive and the penalties that can be imposed are severe. It is therefore critical that regulators' processes are fair and that impacted individuals have robust and accessible means to challenge adverse decisions. Unlike the UK[2], Ireland does not yet have a culture of formal challenge to regulatory decisions, but its response to the recent Appeals Tribunal decision demonstrates that it has no reason to fear them.

In terms of practical steps, despite the work no doubt already done in the context of IAF/SEAR implementation, firms will need to review their F&P policies and processes and related arrangements when the Central Bank's full response to the review report is known. We recommend that they should also consider enhancing their onboarding processes for PCFs and ensure that PCFs are properly supported through the F&P assessment process. Deciding how and whether to support a PCF that is not approved will likely remain a case-by-case decision. That said, there is merit in firms considering in general terms whether and in what circumstances they may be prepared to support an aggrieved individual who wishes to challenge an F&P refusal or withdrawal.

For more information and expert advice in preparing for the implementation of IAF/SEAR and the anticipated changes that the Central Bank's response to the report will herald, contact a member of our Financial Regulation team.

[2] *See Financial Conduct Authority v Seiler [2024] EWCA Civ 852.*

Ireland's Leading Role in Investment Funds Litigation

Anthony O'Hanlon
Partner,
Investment Funds
aohanlon@mhc.ie

Maurice Phelan
Partner,
Head of Dispute Resolution
mphelan@mhc.ie

There are various causes for parties becoming embroiled in fund litigation. Often disputes can centre on investment restriction breaches, perceived losses of assets held in custody, and fund financing breaches. In this article, we look at the factors which can precipitate litigation and some of the means for avoiding costly disputes.

Investment restriction breaches and other fund errors

One of the more common situations which can lead to litigation between investors and service providers to investment funds in Ireland is breaches of either regulatory or self-imposed investment restrictions.

UCITS

The European Communities (Undertakings for Collective Investment in Transferable Securities) Regulations 2011, as amended – or UCITS Regulations – place a series of prescriptive diversification, counterparty and liquidity requirements on funds established as UCITS in Ireland. Often investment managers, with oversight from management companies, will have pre-trade compliance systems in place which are designed to minimise the possibility of investment breaches occurring. Where breaches do occur, the relevant depositary and board will need to be notified alongside the Central Bank of Ireland depending on the type of breach.

Breaches involving concentration limits and ineligible assets can on occasion be resolved by disposing of assets in a timely manner while taking into account market conditions and the best interests of investors. However, where assets have become illiquid, or shareholders have suffered a loss, disputes can arise between the board of a fund, its shareholders and service providers. In these situations, it is important to consider the obligations placed on boards and all service providers under the UCITS Regulations and the Central Bank (Supervision and Enforcement) Act 2013 (Section 48(1)) (Undertakings for Collective Investment in Transferable Securities) Regulations 2019 alongside any other regulations and guidance which may be relevant depending on the circumstances.

Alternative investment funds

Alternative investment funds are generally subject to less prescriptive product requirements. The European Union (Alternative Investment Fund Managers) Regulations 2013, as amended (AIFM Regulations) place obligations primarily on alternative investment fund managers. Boards and service providers also need to comply with the Central Bank's AIF Rulebook, any self-imposed investment restrictions included in offering and constitutional documents and other domestic and European regulations and guidance which may be relevant.

Other fund errors

Alongside investment restriction breaches, other common errors which can lead to disputes between service providers include:

- The incorrect charging of fund fees and expenses
- Net asset valuation calculation errors, and
- Control breach errors such as the payment of redemption monies to an incorrect investor account

Delegation is a common feature of Irish funds and is often used for portfolio management by engaging entities with specialist expertise. However, a party appointing a delegate is not released from its responsibilities and needs to carry out appropriate initial and ongoing due diligence alongside continued oversight.

Where a dispute between parties seems likely to become litigious, as a first port of call, examining the liability and indemnity provisions set out in the service provider agreements is prudent.

Safekeeping assets

Following the financial crisis, detailed regulatory frameworks were put in place which sought to clearly outline the role of depositaries in safeguarding investor assets. Both the UCITS Regulations and the AIFM Regulations impose a quasi-strict liability standard on depositaries for any loss of financial instruments held in custody. Depositaries also have an obligation to verify the ownership of assets not held in custody.

Disputes can arise between parties where there has been a perceived loss of assets held in custody either at the level of the depositary to a fund or one of its sub-custodians. In these situations, the depositary agreement should clearly reflect the corresponding safekeeping obligations included in the relevant regulatory framework. Identifying whether assets which have been lost were held in custody or not is crucial for determining the applicable liability standard for the depositary.

Fund financing breaches

Where leverage has been introduced into a fund platform through a subscription line or asset financing arrangement, disputes can arise between borrowers and lenders on repayment obligations, priorities and whether default events have occurred. In these situations, it is important to examine the security package and documents which were put in place at the time the facility was agreed.

Other common disputes

Management Companies	Issues with the oversight of delegates including investment managers and distributors.
Administrators	Net asset value pricing or calculation errors.
Administrators / MLROs	Failures related to onboarding investors including anti-money laundering and know-your-customer obligations.
Distributors	Issues with marketing material not correctly matching a fund's offering documents. Distributing a fund without appropriate marketing permissions.

Conclusion

Navigating the intricacies of fund litigation requires a deep understanding of the relevant regulatory frameworks and the corresponding obligations of all fund service providers. With specialised legal expertise and a robust commercial court system, Ireland is well-equipped to handle all types of fund disputes. For those managing or servicing funds, staying ahead of potential issues can make the difference between the timely resolution of an issue and a costly legal battle.

For tailored advice, our Investment Funds and Commercial Disputes teams are ready to assist.

4 Top Tips for Harnessing the Value of Your IP Assets

Hazel McDwyer
Partner,
Intellectual Property
hmcdwyer@mhc.ie

Businesses need capital to scale and grow. Yet when seeking finance, few businesses tap into one of their most valuable assets: their intellectual property. Lenders have traditionally taken security over borrowers' tangible assets, for example real estate assets and equipment. However, in recent years, there has been increased recognition of the realisable value of IP assets and the growing market for IP-backed loans.

IP-backed loans are loans offered using intangible assets as collateral, as opposed to physical collateral or personal guarantees. Many smaller businesses and startups, whose value primarily lies in intangibles, can find it difficult to access capital. This can lead to a growth funding gap, particularly if they do not wish to dilute existing shareholdings through further equity investment. IP-backed lending bridges this funding gap, allowing businesses to use their IP as a 'true asset' to secure finance.

While the market for IP-backed lending has generally been served by a small pool of specialty lenders, traditional lenders are beginning to recognise the opportunities presented by IP-backed finance.

In the United Kingdom, Natwest and HSBC have announced lending solutions aimed at physical-asset-light businesses. Under NatWest's "mass market" IP-backed loan solution, loan applicants who fail to meet conventional security criteria will be considered for funding on the basis of qualifying IP assets. It announced in May 2024 a £700,000 loan to Sci-Net, a business software solutions provider, to fund business growth.

The announcement aligns with broader trends in the financial sphere, where IP collateralised debt is gaining traction. However, companies need to undertake a risk benefit analysis as their IP is likely their most valuable asset. Valuation of IP assets can also prove difficult and there can be regulatory hurdles to IP backed lending in some countries.

Top tips

To effectively harness and leverage the value of their IP assets, businesses must recognise the importance of a strong IP strategy:

1. Conduct an IP Audit

This is a systematic and solution-focused review of the IP assets owned, used or acquired by a business. IP audits serve two primary purposes:

- To identify and evaluate IP assets, and
- To anticipate and manage the risks associated with IP portfolios

2. Register IP Rights

Register formal IP rights, i.e. trade marks, patents and industrial designs, with the relevant IP office. EU trade marks and Community designs provide protection across the 27 EU member states. Registered IP is particularly important when it comes to financing.

Copyright is not registrable in Ireland. It automatically arises on the creation of an original work.

3. Protect IP Rights

Ensure IP rights are adequately protected when negotiating and drafting commercial contracts by:

- Obtaining IP assignments from all third-party contractors
- Including appropriately drafted IP clauses in employment contracts, and
- Appropriately protecting IP in contracts with suppliers and customers

4. Keep an IP Register

An IP register is a schedule of IP assets owned, used, or acquired by a business. It lists information such as asset descriptions, age, type, and any valuation assessments that have been carried out. The IP register should be continuously updated for better management of the IP portfolio. It will also assist when it comes to due diligence during investment rounds and when seeking IP-based finance.

How we can help

We have extensive experience advising businesses in registering, managing, protecting and leveraging their IP assets to enhance their business. Please reach out to a member of our Intellectual Property or Banking teams should you require advice and support in this area.

Exploring DORA's Impact on Pension Schemes

Stephen Gillick
Partner,
Head of Pensions
sgillick@mhc.ie

The EU's Digital Operational Resilience Act (DORA) aims to manage digital risks in the financial sector and build financial institutions' resilience against IT-related disruptions, threats and cyberattacks. DORA applies to a wide range of financial entities, including occupational pension schemes having more than 15 members. Trustees of these schemes will need to implement several changes ahead of the compliance deadline of 17 January 2025.

Application

DORA places responsibility for ensuring a financial entity's compliance with the legislation on that entity's management body – in the case of an occupational pension scheme, its trustees. Trustees will bear ultimate responsibility for compliance, including where their scheme's Information and Communications Technology (ICT) functions are outsourced to a third-party provider.

Pension schemes having more than 15 but fewer than 100 members will be subject to a simplified ICT risk management framework. These schemes will be exempt from the requirement to perform advanced testing of ICT systems and the requirement to adopt a strategy on ICT third-party risk.

Risk assessment framework

DORA requires trustees to design and maintain an ICT risk management framework for their scheme and put in place comprehensive internal governance to support this framework. This includes:

- Building disaster recovery procedures and continuity plans
- Creating communication policies
- Carrying out adequate reviews to ensure improvements are made following significant issues
- Periodically testing ICT risk frameworks and addressing any deficiencies

The first step to designing an ICT risk management framework will be identifying the scheme's ICT risks. Trustees will already be familiar with carrying out own-risk assessments, which should include cyber security risks, under the requirements of the European Union (Occupational Pension Schemes) Regulations 2021 (IORP II). However, it is worth noting that DORA risk assessment frameworks will require an uplift of a scheme's existing frameworks to meet the new legislation's requirements.

ICT services contracts and outsourcing

Trustees will need to review any outsourcing contracts with third-party ICT providers. DORA requires outsourcing contracts to contain certain provisions with the aim of standardising terms and conditions to manage third party risk where this is practicable. Trustees should bear in mind, in this context, the requirements laid down in IORP II in relation to the content and notification of outsourcing arrangements.[1] However, DORA's scope is wider in that it includes the use of ICT Services, broadly defined, and may cover the procurement of services not previously thought to come under the definition of "outsourced".

Digital operational resilience testing

Under DORA, pensions trustees will be required to carry out testing to assess the effectiveness of their preventive, detection, response and recovery capabilities and to uncover and address potential ICT vulnerabilities. Testing should include a wide variety of tools and actions, ranging from the assessment of basic requirements to more advanced testing by means of threat-led penetration testing for pensions schemes having more than 100 members.

Incident management and reporting

Trustees are required to establish a robust incident management policy that includes adopting early warning mechanisms and ensuring the suitable classification of issues. Trustees will have to report major incidents to the Pensions Authority.

Conclusion

DORA will require the trustees of occupational pension schemes to take a number of actions in advance of the 17 January 2025 deadline. Trustees should familiarise themselves with the requirements under DORA, considering their new obligations alongside the pre-existing IORP II framework. Trustees should identify their ICT risks and review their existing ICT risk management framework, uplifting it to meet the DORA requirements. A review of existing contractual arrangements with third-party ICT service suppliers will also be necessary to ensure that DORA standards are met.

For more information and expert guidance, contact a member of our Pensions team.

[1] *European Union (Occupational Pension Schemes) Regulations 2021 (SI No. 128/2021), section 64AM; Pensions Authority guidance note: 'Own-risk assessment guidance for trustees', para 7.*

Information Exchange with Competitors: What are the Rules of Engagement?

Tara Kelly
Partner, Head of
Competition, Antitrust & Foreign Investment
tarakelly@mhc.ie

The Court of Justice of the European Union (CJEU) has ruled[1] that a standalone exchange of confidential and strategic information may infringe EU competition law without any need to assess the possible effects on competition. The judgment highlights the importance of adopting a holistic approach to assessing whether an information exchange is capable of restricting competition and identifies certain types of information that are, or may be, safe for competitors to share.

Background

The Portuguese Competition Authority in 2019 imposed on 14 banks, including the 6 largest in Portugal, a fine totalling €225 million for participating in an exchange of information over a period of more than 10 years. The exchange of information was 'standalone' because it was not linked to any agreement to restrict competition.

The banks brought an action to challenge the decision of the Portuguese Competition Authority before the Portuguese Competition Court. The court referred to the CJEU the question of whether, and under what circumstances, an exchange of information can be a restriction of competition by object, i.e. deemed by its nature to be harmful to competition without any need to assess the effects.

[1] *Case C-298/22 – Banco BPN v BIC Português and Others.*

What information was exchanged?

Two kinds of information concerning the home loans, consumer credit and corporate lending markets were exchanged amongst the banks on a monthly basis:

1. Current and future 'commercial conditions', namely, charts of credit spreads. The information also related to future changes to risk variables applied to spreads according to the risk profile of customers, and
2. Production volumes, i.e. individualised figures showing the amount of loans granted in the preceding month, broken down into detailed sub-categories.

Information sharing must be assessed in the round

The CJEU confirmed that an exchange of information may be regarded, by its very nature, harmful to competition if it is both confidential and strategic.

The CJEU found that, given the level of completeness and organisation of the information, it was not publicly available, or it was difficult to obtain or to organise. The court clarified the concept of 'strategic information'. The court described it as information that may reveal, once combined with other information already known to the participants in an information exchange, the strategy which some of those participants intend to implement.

The information regarding credit spreads related to future changes to those spreads and to the risk variables applying to those spreads. Therefore, the CJEU found that the exchange of this information must be regarded as a restriction of competition, without any need to consider whether it had any actual effects on competition.

The CJEU acknowledged that the information relating to production volumes, considered in isolation, was not strategic because it related to the past and, as such, did not reveal future intentions. However, the CJEU said it was necessary to consider the possibility of cross-referencing the different categories of information exchanged. The information on production volumes was combined with information that the court considered as clearly strategic. As a result, the CJEU considered it possible that the information could have allowed the banks to infer their competitors' future intentions or led the banks to follow the same course of conduct on the market.

This aspect of the judgment highlights the need to assess the information holistically, having regard to other information shared or already known. This then allows a determination to be made as to whether the information is confidential and strategic or not.

Permissible information exchange

It is widely recognised that information sharing between competitors can also have positive effects on competition and benefit consumers. For example, certain exchanges can create efficiencies and save costs. Additionally, shared knowledge about best practices can drive innovation and improve quality.

Consistent with this, the judgment highlights that certain types of information sharing between competitors may be permissible. In particular, the CJEU confirms that information exchanged in the following ways will generally not infringe the EU competition laws:

- **Legal obligation to exchange information**: an exchange of information made mandatory by national legislation cannot infringe the competition laws. This, however, is provided that the information exchanged is not capable of having any effect beyond that caused by complying with the legislation. The information exchanged must not go beyond that which is necessary to comply with the legislation.
- **Information-sharing not revealing future intentions**: in the absence of particular circumstances, the sharing of backward-looking information alone is not likely to infringe the competition laws. This is on the basis that the information does not allow inferences to be drawn about future intentions.
- **Aggregated information**: the exchange of aggregated information which does not identify the position of an individual business is generally non-problematic. However, competitors should be wary not to breakdown or disaggregate this information in a manner which identifies any market participant.
- **Pro-competitive benchmarking**: benchmarking or the exchange of information concerning the best management or production methods that generate efficiencies for consumers may be allowed between competitors. However, this does not apply to situations where confidential information relating to future intentions is shared.

- **Information publicly available at the time of exchange**: competitors may exchange information that is already in the public domain. However, competitors should not share public information in a manner which is more complete or systematically organised than equivalent data available in the public domain. Further, even information that is shared shortly before it is made public may still amount to 'confidential' information.

Comment

Banks, financial institutions and alternative lenders should exercise caution when sharing any confidential information with competitors. The assessment of whether information sharing may be harmful to competition is highly contextual and fact-specific. Therefore, we strongly encourage relevant organisations to engage with their competition law advisors before they share or receive information of this nature.

For advice on these and other competition law questions, please get in touch with a member of our Competition, Antitrust & Foreign Investment team for more information.

The Evolution of Digital Asset Exposure in Irish Investment Funds

Anthony O'Hanlon
Partner,
Investment Funds
aohanlon@mhc.ie

Crypto assets in a high-interest-rate world

Many market commentators had viewed crypto assets including crypto currencies as a traditionally speculative asset class which would only survive in a 'risk-on' environment. However, analysts have noted the resilience of established digital coins. Bitcoin in particular has continued to perform steadily despite repeated increases in interest rate levels since March 2022.

In the US, the options for investors seeking to obtain exposure to Bitcoin and Ethereum, the two largest crypto currencies by market capitalisation, have gradually grown. Initially, many investors purchased crypto currencies directly from exchanges. Subsequently, the SEC approved ETFs investing in Bitcoin and Ethereum futures. At the beginning of 2024, the SEC approved the first batch of ETFs directly investing in Bitcoin. More recently, spot Ethereum ETFs began trading in the US in July of this year. In the case of spot Ethereum ETFs, these products are not permitted by the SEC to engage in any 'staking' which would involve generating a yield by locking up underlying Ether holdings for a specified period of time.

The current state of play in the Irish market

When considering exposure to digital assets, the Central Bank of Ireland distinguishes between:

1. Tokenised traditional assets where the value is linked to an underlying traditional asset or a pool of traditional assets, such as financial instruments or commodities, and
2. Other digital assets that are based on an intangible or non-traditional underlying

The Central Bank has issued guidance for those digital assets which are based on intangible and non-traditional underlying assets, which includes crypto currencies.

Qualifying investor alternative investment funds

Qualifying investor alternative investment funds, or QIAIFs, can usually avail of a fast-track one-day regulatory approval process in Ireland. Pre-approval submissions are required by the Central Bank only for a limited cohort of QIAIFs with specific exposures. Subject to certain additional requirements which are primarily placed on the relevant alternative investment fund manager, closed-ended/limited liquidity QIAIFs and open-ended QIAIFs can obtain <u>indirect</u> exposure to crypto assets of up to 50% and 20% of net assets respectively without having to go through any additional Central Bank pre-approval process.

QIAIFs which intend to take indirect exposures above these thresholds need to make a pre-approval submission to the Central Bank.

A proposal to hold crypto assets directly would require a pre-approval submission to the Central Bank. The Central Bank has stated that it will not permit direct exposure to digital assets until such time as it is demonstrated to the Central Bank that a depositary can meet its obligations under AIFMD to provide custody or safe-keeping services for these assets. In addition to the Central Bank's focus on depositaries' safekeeping obligations for directly held crypto assets, depositaries can similarly have concerns from a safekeeping perspective depending on the operation of the digital 'wallet' which would store the crypto assets. Digital wallets which are held offline, often referred to as 'cold' wallets, may prove safer but operationally a fund holding crypto assets directly may have to connect a wallet to the internet from time to time in order to fund redemptions.

UCITS / Retail Investor Alternative Investment Funds (RIAIFs)

The Central Bank does not currently permit direct or indirect exposure to crypto assets in UCITS or RIAIFs.

While direct and indirect exposure to crypto assets in Ireland is not permitted through either UCITS or RIAIFs, these funds can still gain exposure to companies involved in the broader crypto asset ecosystem. For example, subject to the standard eligibility requirements, UCITS and RIAIFs can purchase traditional shares or fixed income instruments which issue from crypto miners, exchanges or other similar entities to provide a level of indirect exposure. This is similar to the approach taken for other asset classes including private equity where UCITS or RIAIFs can purchase shares in listed private equity managers to provide a level of exposure to the private equity market.

More recently, the European Securities and Markets Authority (ESMA) has issued a Call for Evidence as part of its review of the Eligible Assets Directive[1] (EAD). The EAD provides a framework for determining the eligibility of assets for UCITS products. There has been significant innovation and development in financial products and securities since the inception of the EAD in 2007, particularly in the digital asset space. ESMA's focus in reviewing the EAD is to push for a consistent approach across the EU where differing interpretations between national regulators has led to some fragmentation and inconsistent approaches in determining the eligibility of certain asset classes for UCITS. Interestingly, part of the Call for Evidence focuses specifically on direct and indirect exposures to crypto assets. However, it remains to be seen how ESMA will respond to feedback from industry on crypto asset exposure in UCITS products noting the focus of the UCITS regime as a retail framework.

Comment

While QIAIFs in Ireland can already access indirect exposure to crypto assets within certain thresholds without delaying the fast-track approval process, the regulatory landscape remains complex and evolving. Given the strong international brand name of the UCITS product, it will be interesting to see the output from ESMA following the completion of the Call for Evidence on the EAD. For asset managers and investors, staying informed of these regulatory shifts is crucial for navigating opportunities in the digital asset space. As the market continues to mature, strategic decisions made today could shape your competitive edge in this rapidly changing environment.

For more information and expert advice, contact a member of our Investment Funds team.

[1] *Commission Directive 2007/16/EC on UCITS eligible assets.*

Litigation Funding in Ireland

Key Considerations

Colin Monaghan
Partner,
Dispute Resolution
cmonaghan@mhc.ie

Dispute Resolution partner, Colin Monaghan, discusses the current prohibition on "for profit" third-party litigation funding in Ireland and change that may be on the horizon. For more information, please contact Colin or another member of our Dispute Resolution team.

Assessing Financial Services Workers' Status for Tax Purposes

Niamh Caffrey
Partner,
Co-head of Tax
ncaffrey@mhc.ie

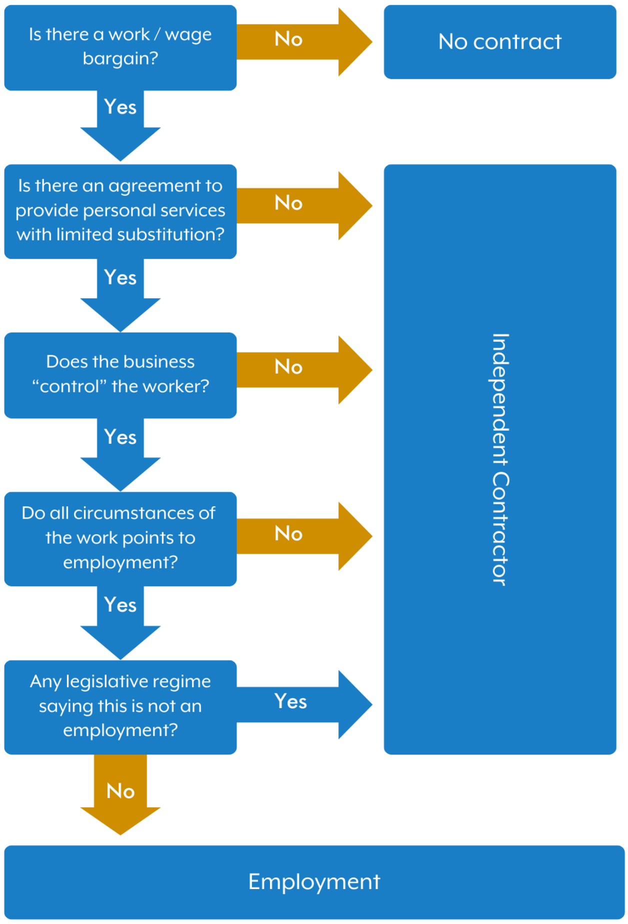
Kevin Mangan
Partner,
Co-head of Tax
kmangan@mhc.ie

The Revenue Commissioners (Revenue) recently published guidelines on determining employment status for tax purposes (the Guidelines). The Guidelines will be of interest to businesses in the financial services sector which engage independent contractors.

It is clear from the Guidelines that Revenue expect that there will be an increase in the number of workers that will be determined to be employees rather than independent contractors for tax purposes. This is an important issue for businesses because, where a worker is an employee for tax purposes, the employer must apply the pay as you earn (PAYE) withholding system on payments and benefits provided to that worker.

Five-step framework

The Guidelines were issued in light of a landmark decision of the Irish Supreme Court in *The Revenue Commissioners v Karshan (Midlands) Ltd. t/a Domino's Pizza*. In that decision, it was held that delivery drivers of Domino's Pizza should be treated as employees and not independent contractors for tax purposes. The Guidelines set out a five-step "decision-making framework". This framework is derived from the *Karshan* case to assist employers in identifying whether or not a worker is an employee.



Some important points for the financial services sector

Control test

Applying the control test at Step 3 for unskilled workers is generally relatively straightforward. It requires consideration of the extent to which the employer controls the means and manner by which the work is to be done. In the financial services sector, contractors will often be skilled workers. The application of the control test in the case of these workers is more difficult because skilled workers may need little or no specific direction in their daily activities. This does not mean however that such workers could not be employees for tax purposes. The control test may be met where the employer retains residual authority over the work. Some examples provided by Revenue in the Guidelines include the expectation to meet clearly defined deliverables, or meet clearly set targets, within defined deadlines. In applying the test for skilled workers, control would generally not extend to how work is undertaken, but rather what is required to be done and by when.

Part-time and casual workers

Revenue note in their Guidelines that there has been a perception that when workers were engaged on a part-time or casual basis, including specifically for one-off shifts, they were not employees as there was no continuous employment obligation. However, the arrangements with these workers should be analysed using the five-step framework in the same way as any other workers.

All of the circumstances of the work

Step 4 involves an examination of the terms of the contract interpreted in the light of all of the circumstances of the work to establish if the working arrangement is consistent with an employment or whether the individual is self-employed. The guidelines confirm that, while a detailed written agreement may carry significant weight, efforts to describe a relationship in a particular way which differs from the day-to-day reality may be challenged.

It is also confirmed that including phrases such as "as a self-employed contractor you will be responsible for your own tax" are not sufficient to ensure that a worker will not be treated as an employee for tax purposes.

The Guidelines note that there are no "static characteristics" of an employment arrangement but some of the factors considered by Revenue in the examples provided in the Guidelines include:

- The terms of the contract
- Control, which as discussed above may be different for skilled v unskilled workers
- Substitution rights
- Whether the person can profit beyond their normal payment if they do things more efficiently
- Use of their own materials, tools or equipment
- Level of integration to the business including use of uniform, email address, access to paid support staff
- Restrictions on the ability to refuse work and/or work for other businesses
- Entitlement to holiday pay, sick pay, notice periods etc.
- Whether the worker has their own insurance

Personal/managed services companies

It is common in the financial services sector for workers to be employed through personal/managed services companies. Helpfully, Revenue has confirmed that there is no change in the tax position for businesses who engage such companies to conduct work on their behalf. Revenue will generally not look behind corporate structures. However, businesses employing contractors through personal/managed services companies should be aware that it is important that the invoicing and payment arrangements are correctly administered by the company so that its operations are in line with the contractual arrangements. Also, Irish PAYE must be applied to payments for services of a director of an Irish incorporated company even if these are provided through a company.

The personal/managed services company will have a PAYE withholding requirement for payments to its directors and employees and whether workers are employees for tax purposes should be determined in line with the tests outlined above. A secondary liability to Irish PAYE may arise for the end-user businesses where an employee of a non-Irish company performs duties in Ireland. This means that the end-user business can be liable for the PAYE which should have been withheld by the personal/managed services company, so it is important that businesses are appropriately protected from this risk.

Agencies

It is also common in the financial services sector for workers to be employed through agencies. The Guidelines confirm that Revenue do not regard the taxation of workers employed through agencies any differently to the taxation of workers employed by any other means. For agency workers, the person who is contractually obliged to make the payment to an employee is the employer for the purpose of collecting income tax, USC and PRSI through the PAYE system.

Employment law implications

While the *Karshan* decision and Guidelines concern employment status for tax purposes, they may also be relevant in the context of determining employment status for employment law purposes. This is due to overlap in tests used by Revenue and bodies adjudicating on employment rights, such as the Workplace Relations Commission, Labour Court and civil courts, to determine employment status. Where an employee is misclassified as an independent contractor, this gives rise to significant liabilities under employment law, in addition to tax and social insurance liabilities.

Conclusion

Revenue indicate in the Guidelines that they expect businesses to review arrangements and apply the five-step framework to determine if a worker should be treated as an employee. Evidence should be retained of the analysis done to apply the framework when a worker is engaged and at regular intervals thereafter. This is especially important where a contractor's role may develop over time. Financial services businesses should take action to ensure that they are prepared in advance of any Revenue compliance intervention as it is clear that this is an area of focus for Revenue.

For more information and expert advice on all relevant taxation matters impacting your business, contact a member of our Tax team.

Financial Services Sector

The financial services sector has undergone unprecedented transformation from traditional banking to new developments like ESG and Fintech. Our lawyers are trusted advisors on the optimal adaptations and solutions for clients in responding to industry changes.

Now more than ever the financial services sector needs to respond and evolve. Our team is at the cutting-edge of these developments working in partnership with clients and drawing on our significant expertise in key areas such as insurance, financial regulation and data privacy.

Our objective is to help clients manage transitions and respond to the ever changing regulatory and political environment. We frequently operate at the intersection of law and technology finding the optimal balance between commercial and legal requirements. Our lawyers are renowned for their thorough and pragmatic approach supported by experienced project managers and bespoke systems to streamline the most complex mandates for clients.

Contact our Financial Services Sector team

About Us

We are a business law firm with 120 partners and offices in Dublin, London, New York and San Francisco.

Our legal services are grounded in deep expertise and informed by practical experience. We tailor our advice to our clients' business and strategic objectives, giving them clear recommendations. This allows clients to make good, informed decisions and to anticipate and successfully navigate even the most complex matters.

Our working style is versatile and collaborative, creating a shared perspective with clients so that legal solutions are developed together. Our service is award-winning and innovative. This approach is how we make a valuable and practical contribution to each client's objectives.

What Others Say

Our Financial Services Team

"Continuously demonstrate their capabilities and ability to deliver."

Legal 500

Our Financial Services Team

"The law firm has a superb team, easy to work with, supportive and fully understands the complexity of cases."

Chambers & Partners