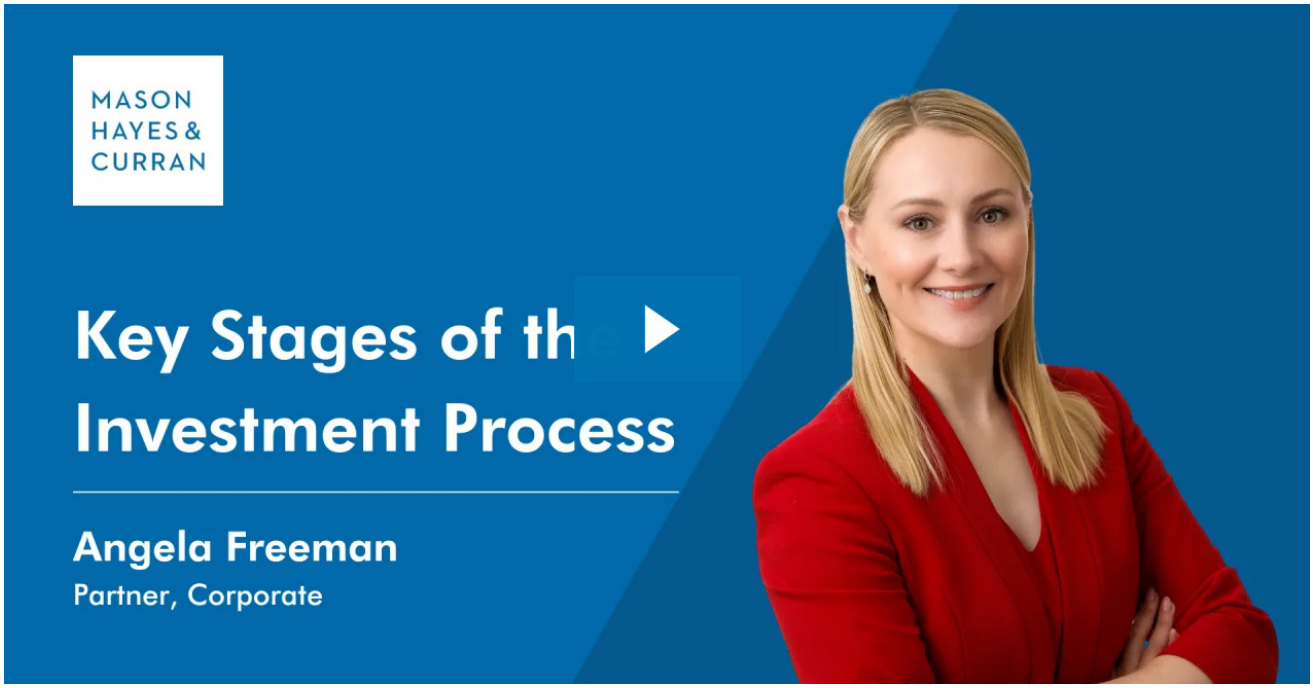
MASON HAYES & CURRAN

# Technology Sector Update

## In Brief

Summer 2024

# Welcome




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

First up, in the above video, Corporate partner Angela Freeman outlines the three key stages to the investment process in Ireland. Other popular insights featured in this edition include:

- The AI Act is Adopted: New Compliance Obligations
- AI and Digital Health Products – EU Product Liability Reform
- EU Cybersecurity Law - What's on the Horizon?
- Wave of Dawn Raids Prompts Welcome Clarifications
- New EU Cybersecurity Directive – NIS2

## Key Contacts

**Oisín Tobin**
Partner,
Technology Sector Lead
otobin@mhc.ie

**Philip Nolan**
Partner, Chair and
Head of Technology
pnolan@mhc.ie

Contact our Technology Sector team

# The AI Act is Adopted

## Compliance Obligations on the Horizon

**Brian McElligott**
Partner, Head of
Artificial Intelligence
brianmcelligott@mhc.ie

**Philip Nolan**
Partner, Chair and
Head of Technology
pnolan@mhc.ie

The Council of the EU approved the AI Act on 21 May 2024 and it is now expected to enter into force by June 2024. With the exception of certain provisions of the AI Act, such as prohibited AI, the main obligations will apply two years after it commences. Oversight will be managed by national supervisory authorities including:

- The AI Office
- The AI Board
- A scientific panel, and
- A stakeholder advisory forum.

Following the announcement of the adoption of the AI Act, Ireland's Department of Enterprise, Trade and Employment announced the opening of the public consultation on the implementation of the AI Act. The consultation is open until 5pm, Tuesday 16 July 2024.

## Obligations and requirements

The EU Transport, Telecommunications and Energy Council (Telecoms Council) adopted the AI Act on 21 May 2024. The AI Act, the first of its kind in the world, seeks to protect the health, safety and fundamental rights of individuals while also fostering safe, innovative and trustworthy AI. While the AI Act recognises the significance of innovation, it aims to balance this against the importance of ethical and responsible AI.

The AI Act adopts a risk-based approach and will regulate AI by imposing obligations such as transparency and conformity requirements. The provisions will apply to various persons including AI providers, deployers, importers, distributors and users in the EU. The obligations will be phased in over a period of three years, with the first key obligations on prohibited AI applying six months after the AI Act comes into force.

## Governance structure

The European Commission has initiated the development of the EU-level governance structure, setting up the AI Office within DG CNECT in February 2024. The AI Office will be tasked with implementing, monitoring, and supervising AI systems and general-purpose AI models under the AI Act. An independent scientific panel will support the AI Office. In addition, an AI Board composed of Member States' representatives will serve as an advisory body, guiding the Commission on the design of codes of practice for foundational models. An AI Committee will be established to adopt Commission implementing acts. Member States will designate market surveillance authorities who will oversee the regulation of AI systems under the Market Surveillance Regulation.

## Consultation opens

The Department of Enterprise, Trade and Employment (DETE) will lead the national implementation of the AI Act in Ireland. In association with other government bodies, the DETE is exploring various approaches to the enforcement of the AI Act. The DETE has published its consultation on the national implementation of the AI Act. The consultation aims to shape Ireland's strategy for implementing the AI Act, and in particular, the designation and responsibilities of competent authorities here in Ireland.

The consultation contains four questions which cover issues such as:

- Who should be designated as the national competent authority,
- What potential synergies between the AI Act and other digital legislation can be realised, and
- How implementation can accelerate investment and innovation of AI in Ireland while also supporting Ireland's national AI strategy.

The consultation is open to all stakeholders, including businesses and civil society organisations. The consultation will close at 5pm on Tuesday, 16 July 2024.

## Next steps

The AI Act is expected to enter into force before the end of June 2024 with the first provisions on prohibited AI applying from sometime in December 2024. All businesses involved in the development, deployment, oversight or utilisation of AI will need to assess their use of AI to ensure compliance with the AI Act. In particular, providers of AI systems in medical devices, software as medical devices and invitro medical devices should take note that the 3 year implementation period for high-risk AI systems will shortly begin. Those who wish to participate in the consultation should start preparing responses.

For more information, guidance and expert advice, contact a member of our Artificial Intelligence team.

# AI and Digital Health Products: EU Product Liability Reform

**Michaela Herron**
Partner,
Head of Life Sciences
mherron@mhc.ie

**Jamie Gallagher**
Partner,
Product Regulatory & Liability
jamesgallagher@mhc.ie

As part of its holistic approach to AI policy, the European Commission has proposed a package of reforms to adapt EU product liability rules to the digital age and AI, including through the revision of the Product Liability Directive 85/374/EEC (the PLD). As discussed in our previous article on the PLD, this revised Directive is intended to be complementary in nature to current EU product safety frameworks, such as:

- The EU Medical Devices Regulation (EU) 2017/745 (MDR)
- The In-Vitro Diagnostic Medical Device Regulation (EU) 2017/746 (IVDR), and
- The recently adopted AI Act

These interlinked frameworks give rise to a complex new legislative environment that stakeholders must navigate with care. We highlight some important connections between these frameworks that developers of software medical devices that will be regulated as AI systems should be mindful of.

## Broader scope of the PLD

The PLD seeks to update the EU's strict liability regime applicable to products, including software and by extension, AI systems. Accordingly, claims for damage allegedly caused by AI-enabled digital health products and services will fall within the scope of the PLD. This is because the PLD expands the definition of a 'product' to include software:

*"'product' means all movables, even if integrated into, or inter-connected with, another movable or an immovable; it includes electricity, digital manufacturing files, raw materials and software".*

While the term 'software' is not defined in the PLD, the recitals to the PLD make clear that it applies to software of all kinds, including:

- Operating systems
- Firmware
- Computer programmes
- Applications, and
- AI systems

It also acknowledges that software is capable of being placed on the market as a standalone product and may subsequently be integrated into other products as a component. Accordingly, software will be a product for the purposes of applying no-fault liability under the PLD. This applies irrespective of the mode of its supply or usage and whether it is stored on a device or accessed through a communication network, cloud technologies or supplied through a software-as-a-service model.

Insofar as an AI system qualifies as a 'product' and 'software', it is proposed to fall within the scope of the PLD. At a high-level, this will mean that the PLD will apply to most, if not all, consumer or public-facing systems, or systems that are components of hardware that qualify as a physical 'product'. Accordingly, digital health products and services delivered using AI-enabled technologies such as wearable devices, telemedicine platforms and health apps will be affected.

Two noteworthy exclusions regarding the scope of the PLD are as follows:

- The new product liability rules contained in the PLD will apply to products placed on the market or put into service 24 months after its entry into force. The current Product Liability Directive 85/374/EEC will be repealed with effect from 24 months after the PLD's entry into force. However, it will continue to apply to products placed on the market or put into service before that date.
- The PLD will not apply to pure information, such as the content of digital files or the mere source code of software. It will also not "*apply to free and open-source software that is developed or supplied outside the course of a commercial activity*" unless it is subsequently integrated by a manufacturer as a component into a product in the course of a commercial activity.

## Defectiveness

Under the PLD, the criteria for determining the defectiveness of a product, including an AI system, will be expanded. Some of these additional criteria, which are non-exhaustive in nature, are particularly relevant to AI systems and link back to AI Act requirements:

- In the first instance, the PLD provides that a product will be considered defective "*if it does not provide the safety that a person is entitled to expect or that is required under Union or national law*". Consequently, an AI system may be deemed defective for the purposes of a product liability claim by virtue of being non-compliant with requirements under the AI Act, the MDR and/or the IVDR.
- Additional defectiveness criteria specified under the PLD include a product's interconnectedness, self-learning functionality and safety-relevant cybersecurity requirements.
- In reflecting the relevance of product safety and market surveillance legislation for determining the level of safety that a person is entitled to expect, the PLD also provides that, in assessing defectiveness, interventions by competent authorities should also be taken into account. This includes "*any recall of the product or any other relevant intervention by a competent authority or by an economic operator as referred to in Article 8 relating to product safety*".

Accordingly, an AI-enabled product's compliance with requirements under the AI Act, the MDR and/or the IVDR and interventions by competent authorities in respect of same, will weigh in the balance in terms of assessing the 'defectiveness' or otherwise of an AI system.

## Rebuttable presumption - defectiveness

Under the PLD, the burden remains on a claimant to prove:

- The defectiveness of the product
- The damage suffered
- The causal link between the injury or damage sustained, and the allegedly defective product

These elements must be proven in accordance with the standard of proof applicable under national law in the relevant Member State(s). The PLD acknowledges, however, that injured parties are often at a disadvantage compared to manufacturers in terms of accessing and understanding information about how a product was produced and how it operates, particularly in cases involving technical or scientific complexity. Accordingly, the PLD introduces a rebuttable presumption of defectiveness where:

1. The claimant demonstrates that the product does not comply with mandatory product safety requirements laid down in Union law or national law.
2. The claimant demonstrates that the damage was caused by an "*obvious malfunction*" of the product during "***reasonably foreseeable***" use or under ordinary circumstances.
3. A defendant fails to comply with a court order to disclose relevant evidence at its disposal.

In the context of AI systems, the rebuttable presumption of defectiveness triggered under the PLD by a product's non-compliance with mandatory product safety requirements laid down in Union law or national law could therefore be triggered by an act of non-compliance with requirements under the AI Act, the MDR and/or the IVDR.

## Rebuttable presumption - causation

The PLD also provides for the presumption of a causal link between a product's alleged defectiveness and the damage suffered, where it has been established that the product is defective, and the damage caused is of a kind typically consistent with the defect in question.

A rebuttable presumption will arise where a national court must presume a product's defectiveness or the causal link between its defectiveness and the damage suffered, or both, where, despite the disclosure of evidence by a manufacturer, and taking all relevant circumstances into account:

- The claimant faces excessive difficulties, in particular due to technical or scientific complexity, in proving the product's defectiveness or the causal link between its defectiveness and the damage, or both, and
- The claimant demonstrates that it is likely that the product is defective or that there is a causal link between the defectiveness, the damage, or both.

On the interpretation of 'excessive difficulties', Recital 48 of the PLD refers to AI systems specifically. It provides that in determining technical or scientific complexity, national courts must do this on a case-by-case basis, taking into account various factors, including:

- The complex nature of the technology used, such as machine learning.
- The complex nature of the causal link such as a link that, in order to be proven, would require the claimant to explain the inner workings of an AI system.

It further provides that, in the assessment of excessive difficulties, while a claimant should provide arguments to demonstrate excessive difficulties, proof of these difficulties should not be required. For example, in a claim concerning an AI system, the claimant should neither be required to explain the AI system's specific characteristics nor how those characteristics make it harder to establish the causal link.

## Manufacturer's control

The PLD introduces various new provisions that recognise that, in the case of technologically sophisticated products, a manufacturer's responsibilities do not necessarily crystallise at the factory gates. This is particularly significant for connected products, where the hardware manufacturer retains the ability to supply software updates or upgrades to the hardware by itself or via a third party.

The PLD provides that the developer or producer of software, including an AI system provider, should be treated as a manufacturer. While the 'provider of a related service' is recognised as an economic operator under the PLD, related services and other components, including software updates and upgrades, are considered within the manufacturer's control where they are integrated, inter-connected or supplied by the manufacturer or where the manufacturer authorises or consents to their supply by a third party.

A 'related service' is defined in the PLD as "*a digital service that is integrated into, or inter-connected with, a product in such a way that its absence would prevent the product from performing one or more of its functions*". For example, where a manufacturer consents to the provision by a third party of software updates for its product or where it presents a related service or component as part of its product even though it is supplied by a third party. However, a manufacturer isn't considered to have consented to the integration or interconnection of software with its product merely by providing for the technical possibility to do so, or by recommending a certain brand or by not prohibiting potential related services or components.

Additionally, once a product has been placed on the market, it is considered within the manufacturer's control insofar as it retains the technical ability to supply software updates or upgrades itself or via a third party.

This means that manufacturers of products with digital elements may be liable for damage arising from changes to those digital elements that occur after the physical product is placed on the market. This is a significant shift to more of a 'lifecycle' approach. This aligns with the approach adopted under various pieces of EU product safety legislation, including the MDR, where manufacturers must continuously evaluate the impact of software updates and upgrades in products on the market. The consequence for manufacturers of AI-enabled products is that greater attention will need to be paid to:

- The degree of control it exercises over its products once placed on the market.
- Where its products remain within its control, the extent to which changes like software updates and upgrades impact on not just safety but also product liability exposure.
- What 'related services' form part of its products and the level of control exerted over these 'related services', including the nature of the relationship with any third-party providers of related services and the potential consequences of same from a product liability perspective.

## Substantial modification

The PLD maintains the general limitation period of 3 years for the initiation of proceedings for the recovery of damages. This limitation period runs from the day on which the injured person became aware, or should reasonably have become aware, of all of the following:

1. The damage
2. The defectiveness, and
3. The identity of the relevant economic operator that can be held liable for the damage.

The PLD contains two modifications to the current 10-year longstop provision in the existing Product Liability Directive. First, an extension to 25 years in certain cases involving latent personal injuries unless the injured person has, in the meantime, initiated proceedings against a potentially liable economic operator. Second, where a product has been 'substantially modified', the calculation of time runs from the date that the substantially modified product has been placed on the market or put into service.

In that regard, the PLD defines 'substantial modification' as the modification of a product after it has been placed on the market or put into service:

1. That is considered substantial under relevant Union or national rules on product safety, or
2. Where relevant Union or national rules do not provide such a threshold, that:
    - Changes the product's original performance, purpose or type without being foreseen in the manufacturer's initial risk assessment, and
    - Changes the nature of the hazard, creates a new hazard, or increases the level of risk.

What amounts to a 'substantial modification' can be quite case specific. However, the reference in the definition to modifications that are "*considered substantial under relevant Union or national rules on product safety*" engages the AI Act. This is because it contains references to substantial modification in the context of 'high-risk AI systems', i.e. most software medical devices regulated as AI systems owing to the application of MDR, Annex VIII, Rule 11 and Article 6 of the AI Act. One such example is high-risk AI systems that continue to learn after being placed on the market or put into service.

Where no thresholds are provided under the relevant Union or national rules on product safety, for example in cases involving regulated AI systems that are not high-risk under the AI Act, the threshold is assessed by the extent to which the modification changes the product's original intended functions or affects its compliance with applicable safety requirements or changes its risk profile.

We expect that the practical application of these concepts in the context of AI systems will require complex and case-specific analyses on liability exposure and mitigation.

Irrespective of which threshold criteria is applicable to a specific AI-enabled product, AI system providers and providers of products with AI components, will need to carefully track how relevant AI systems are changing and the legal consequences of those changes.

## Conclusion

On one hand, digital health stakeholders of products regulated under the MDR and/or the IVDR may be uniquely well-placed to adapt to these changes given their experience of complying with the sophisticated EU medical device regulatory framework. On the other hand, however, the move to bring the EU product liability regime up to speed with updated product safety legislation is likely to give rise to increased litigation risks that will require careful management, particularly for liability exposure in respect of software as a 'product' for the purposes of product liability claims. To prepare for these incoming changes, digital health stakeholders with products on the EU market should carefully consider their potential liability exposure under the PLD.

We would recommend that they carefully analyse their existing product portfolio to:

- Identify what products would fall within the scope of the PLD, including a review of third-party software and 'related services', i.e. digital services embedded in their hardware products.
- Review the warnings and disclaimers provided to users relating to risks or potential harm associated with using their products and related services, particularly having regard to the extended definition of damage.
- Incorporate the necessary screens and protocols into their product roadmaps in order to identify and mitigate EU product liability exposure.

Digital health stakeholders should also review their:

- Product liability insurance to ensure, amongst other things, that their coverage includes all damage envisaged under the PLD. Specifically, they should ensure that coverage extends to destruction or corruption of data and medically recognised damage to psychological health and to ensure that related services are also covered.
- Contractual arrangements with other economic operators to ensure there are adequate liability and indemnity provisions in place. This is particularly important given the new provisions in the PLD around service providers and what is considered to be within the manufacturer's control – even if a third party is carrying out certain tasks or services on their behalf.

For more information, contact a member of our Product Regulation & Consumer team.

# EU Cybersecurity Laws

## What's on the horizon?

**Julie Austin**
Partner,
Privacy & Data Security
jaustin@mhc.ie

**Oisín Tobin**
Partner,
Technology Sector Lead
otobin@mhc.ie

In recent years, there has been a marked increase in the amount of legislation generated at an EU level with a view to improving cybersecurity across Europe. The Network and Information Security Directive (NIS2), the Cyber Resilience Act, the Digital Operational Resilience Act (DORA) and the EU Cybersecurity Act are each aimed at strengthening the EU's cybersecurity framework in light of the heightened threats to cybersecurity in the digital age. In this article, we explore these four key pieces of legislation, and what they might mean for you.

## NIS2 Directive

### What is it?

In 2018, the Network and Information Security Directive (NIS1) harmonised national cybersecurity capabilities, cross-border collaboration and the supervision of critical sectors across the EU. However, a common criticism levied against NIS1 is that it is inconsistently applied across Member States resulting in divergent security requirements and incident notification requirements. The European Commission conducted a review of NIS1 and developed a proposal for a revised directive, EU Directive 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). NIS2 will repeal and replace NIS1.

The goal of NIS2 is to expand the scope of NIS1, making it "future-proof". It provides legal measures which are geared towards boosting cybersecurity in the EU.

NIS2 builds on three elements of NIS1:

1. *Competent authorities*: Improve the level of joint situational awareness and the collective capability to prepare and respond, by:
    - Taking measures to increase the level of trust between competent authorities. In Ireland, this is the National Cyber Security Centre (NCSC)
    - Sharing more information
    - Setting rules and procedures in the event of a large-scale incident or crisis
2. *Reduce inconsistencies in resilience*: Further aligning:
    - The de facto scope
    - The security and incident reporting requirements
    - The provisions governing national supervision and enforcement
3. *Increase the level of cyber-resilience*: NIS2 puts in place rules that ensure that public and private entities across the internal market, which fulfil important functions for the economy and society as a whole, such as energy, banking and financial markets, are required to take adequate cybersecurity measures.

### Who does it apply to?

NIS2 extends to a larger part of the economy than NIS1. It applies to entities from a number of "critical sectors" including:

- The energy sector
- Financial market infrastructures
- ICT Service Management (managed service providers and managed security service providers)
- Waste management
- Food
- Machinery and equipment
- Digital providers (online marketplaces, online search engines and social networks)

NIS2 defines two categories of public and private entities within scope: "essential" entities and "important" entities, with more onerous obligations for 'essential' entities.

### When does it come into effect?

NIS2 was published in the Official Journal on 14 December 2022. As a directive, it must now be transposed into national law by each Member State of the EU. Member States must adopt and publish the measures necessary to comply with NIS2 by 17 October 2024.

The EU Commission will periodically review the functioning of the Directive and report on it to the Council for the first time by 17 October 2027.

### What will enforcement look like?

Most entities will fall under the jurisdiction of the Member State in which they have their main establishment. NIS2 provides a wide range of enforcement measures which Member State authorities may take to supervise entities, including regular and targeted audits, on-site and off-site checks, and requests for information. NIS2 also sets up a framework of sanctions across the Union, to include a minimum list of administrative sanctions.

Regarding sanctions, NIS2 distinguishes between essential and important entities. For essential entities, Member States must provide for administrative fines for a breach of NIS2 of up to €10,000,000 or 2% of total worldwide annual turnover for the preceding financial year, whichever is higher. For important entities, NIS2 requires Member States to provide for a maximum fine of at least €7,000,000 or at least 1.4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

## Cyber Resilience Act

### What is it?

The Cyber Resilience Act is a proposal for a Regulation on cybersecurity requirements for products with digital elements. It aims to address the perceived inadequate level of cybersecurity in many products, as well as addressing the inability of consumers and businesses to determine which products are cybersecure.

According to the EU Commission, the Regulation, once implemented, will guarantee harmonised rules for products or software with a digital element. It will also introduce a duty of care obligation for the entire lifecycle of such products, as well as a framework for cybersecurity requirements governing a number of aspects, with a view to providing for obligations to be met at every stage of the value chain.

The main obligations covered by the proposal include cybersecurity by design, vulnerability management and market surveillance.

### Who does it apply to?

When in force, the Regulation will apply to "critical" products with digital elements, ie a product with digital elements that presents a cybersecurity risk in accordance with the criteria set out in the proposal.

The obligations will differ depending on whether the product is a Class 1 or Class 2 product.

### When does it come into effect?

EU Member States and the European Parliament have come to a provisional political agreement on the Regulation. The European Parliament and EU Council must approve the Regulation before it moves to the next stage of the legislative process.

Once adopted, it will enter into force 20 days after its publication in the Official Journal.

### What will enforcement look like?

The draft proposal provides for a number of administrative fines for various offences. These fines can be up to €15,000,000 for a breach of certain obligations, or 2.5% of an undertaking's total worldwide annual turnover in the preceding year, whichever is higher.

## DORA

### What is it?

DORA is a package of two pieces of European legislation, a Regulation and a Directive, which aims to strengthen the IT security of financial institutions.

### Who does it apply to?

DORA will apply to financial institutions including banks, insurance companies and investment firms but will also have substantial implications for IT service providers who count these institutions as customers.

### When does it come into effect?

DORA was adopted in December 2022 and will enter into force in January 2025. 2024 is therefore a critical year for financial institutions to prepare for compliance. Compliance will undoubtedly be aided by the publication of policy documents by EU supervisory entities: the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA).

The first set of final draft technical standards was published on 17 January 2024 and offers clarity on required elements of the risk management framework, the criteria for classifying ICT-incidents and the measures applying to outsourcing, among other things.

The second set of draft technical standards was published on 8 December 2023 and remains open for public consultation until 4 March 2024. A finalised version of the second set of technical standards is scheduled for publication in July 2024.

### What will enforcement look like?

DORA imposes a uniform set of rules for ICT risk management, incident reporting and operational resilience testing for financial institutions as well as for managing the risk posed by third-party ICT-providers. To this end, DORA will impose requirements on the contractual arrangements between financial institutions and ICT providers and will set the parameters of an oversight framework for managing these third-party risks. Several of DORA's key requirements are undergirded by a risk-based approach designed to mitigate the compliance burden on financial institutions. It also contains provisions requiring information and intelligence sharing among financial institutions to mitigate risks on a system-wide level.

## Cybersecurity Act

### What is it?

The Cybersecurity Act is an EU Regulation which came into force in April 2019. It established the EU Agency for cybersecurity (ENISA) and is the basis for an EU-wide framework for the cybersecurity certification of ICT products, processes and services. The European Commission proposed an amendment to the Cybersecurity Act in April 2023 which would enable the adoption of European cybersecurity certification schemes for 'managed security services' covering areas such as incident response, penetration testing, security audits and consultancy.

Certification is key to ensure a high level of quality and reliability of these highly critical and sensitive cybersecurity services which assist companies and organisations to prevent, detect, respond to or recover from incidents. These certifications could be used to demonstrate compliance with the security obligations under the GDPR.

## Who does it apply to?

The proposed new system would apply to those who provide managed security services within the EU. Managed security services are defined as "*carrying out, or providing assistance for, activities relating to... customers' cybersecurity risk management*".

## When does it come into effect?

It is not yet clear when the proposed amendment will come into effect but, as of March 2024, the proposed amendment remains the subject of discussion within the European Council. It is expected to progress through the legislative process during the course of the year. Both providers and users of managed security services should be cognisant of the effects of the amendment and may wish to monitor its progress.

## What will enforcement look like?

While the text of the amendment has not been finalised, the proposed amendment is intended to mirror the language of, and therefore complement, the NIS2 Directive. Certification of the providers of these services will act as a mark of quality for potential customers with the scheme aiming to ensure that these services are "*provided with the requisite competence, expertise and experience*".

The amendment would have particular implications for service providers as it would aim to ensure that the service provider has "*appropriate internal procedures in place to ensure a high level of quality*". While implementing legislation would be required to define the exact standards to be adhered to for certification, the amendment does contemplate a tiered certification system with "basic", "substantial" and "high" levels of assurance proposed.

# Contact our team

For more information and expert advice, contact a member of our Privacy & Data Security team.

# Wave of Dawn Raids Prompts Welcome Clarifications

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

**Liam Heylin**
Partner, Competition, Antitrust & Foreign Investment
lheylin@mhc.ie

In the space of just three months, three rounds of dawn raids were conducted by the Competition and Consumer Protection Commission (CCPC). Separately, the Commission for Communications Regulation (ComReg), which regulates the communications sector in Ireland, carried out a dawn raid of Eircom Limited's (Eir) premises last year. These are some of the first dawn raids since the Supreme Court handed down a landmark judgment in 2017 harshly criticising the CCPC's over-inclusive approach to seizing documents.

These dawn raids present a welcome opportunity for the CCPC's and ComReg's approach to seizing documents during a dawn raid to be clarified and refined. This is especially important for documents that may be the subject of privacy or legal professional privilege (LPP) claims. In fact, recent High Court proceedings appear to have set this train in motion.

This wave of dawn raid activity occurs against the backdrop of the implementation of the Competition (Amendment) Act 2022 (2022 Act) in September 2023. It is expected to continue in view of the CCPC's and ComReg's newly acquired powers to impose significant administrative fines. Meanwhile, other regulators in Ireland, including the Data Protection Commission (DPC), also have extensive investigative powers.

## Significant investigative powers

Since their inception, the CCPC and ComReg have had extensive powers to investigate suspected competition law infringements. These include the powers to:

- Summon witnesses
- Examine witnesses under oath
- Require witnesses to produce any books, documents and records in their possession or control
- Conduct dawn raids, on foot of a District Court warrant, which includes the powers to:
    - Enter into and conduct searches in any premises used for or in connection with business activities or individuals engaged in the business
    - Seize and retain any electronic or hardcopy books, documents or records relating to the business activities under investigation
    - Inspect and take copies or extracts of any such books, documents or records, or
    - Require any persons in the business to provide any information required for carrying out an investigation or to provide any records under the person's control

The CCPC and ComReg now have the option of initiating administrative proceedings, instead of criminal proceedings. They can impose administrative fines of up to €10 million or 10% of a company's total worldwide turnover, whichever is the greater, on parties that have infringed competition law. These fines are subject to court approval. On the criminal front, the 2022 Act substantially increased the potential criminal penalties for hardcore cartel offences to €50 million or 20% of global turnover.

Historically, the CCPC's practice following the conclusion of an investigation was to agree legally binding commitments with the party(ies) under investigation. In return, the CCPC would agree to discontinue its investigation and not bring criminal proceedings. The CCPC could then apply to the High Court to have the agreement made an order of the court. In light of the CCPC's new power to impose administrative fines under the 2022 Act, this practice may be discontinued.

## Limitations on search and seizure

The CCPC and ComReg's extensive search and seizure powers are not without limits. The Competition and Consumer Protection Act 2014 Act (2014 Act) sets out specific rules for the CCPC's treatment of legally privileged material during an inspection or investigation. If there is a dispute as to whether documents are protected by LPP, the CCPC may compel their disclosure provided confidentiality can be maintained pending a determination by the High Court or an independent adjudicator. By contrast, the Data Protection Act 2018 (the 2018 Act), does not provide for the compelled disclosure of legally privileged information. If a controller or processor refuses to produce legally privileged documents, the DPC must apply to the High Court for a determination as to whether the information is privileged, and the controller or processor is required to preserve the information pending the High Court determination. Neither the 2018 Act nor the 2014 address the treatment of documents that are potentially outside the scope of the investigation.

Conversely, the Communications Regulation Act 2002 which sets out ComReg's investigation powers, deals with the treatment of both privileged and irrelevant/private material.

The scope of the CCPC's search and seizure powers came under scrutiny in *Irish Cement Limited v the CCPC (Irish Cement)*. The Supreme Court ruled that emails seized during a CCPC dawn raid were outside the scope of the CCPC's search warrant. The Court heavily criticised the seizure of an entire mailbox as disproportionate and "an unnecessary, irrational, incursion which went well beyond what should have been the objective sought to be achieved". Further, the Court recommended that the CCPC develop a Code of Practice for future dawn raid searches.

Following the Supreme Court decision, regulators needed to take a more cautious, refined, and nuanced approach to search and seizure. Against this backdrop, in March 2023, the CCPC published a Statement on Privacy and Legal Professional Privilege Rights. This Statement provided guidance on the treatment of material seized during a dawn raid. However, we understand that the CCPC's position on privacy and LPP rights may be under review by the CCPC. It is possible this is as a result of court proceedings arising from the recent dawn raids.

## High Court proceedings

In recent months, the CCPC and ComReg have carried out the following unannounced inspections:

### Ryanair

The CCPC assisted the Italian competition authority, in March 2024, in searching Ryanair's headquarters in a probe related to complaints by online travel agencies.

### Home alarm systems

The CCPC, supported by the Garda National Economic Crime Bureau and An Garda Síochána, carried out a number of searches of businesses active in the home alarm industry in February 2024. This was part of an on-going criminal investigation into potential breaches of competition law.

## Public transport

The CCPC, in December 2023, searched the offices of businesses in Cork as part of a criminal investigation into potential competition law breaches in the publicly funded transport sector. As the investigation is still ongoing, full details are not yet public.

## Telecommunications sector

ComReg conducted an unannounced search of the premises of Eir in summer 2023. This search was regarding a proposed discount scheme for access to its fibre to home/businesses scheme by its wholesale customers. It was suspected that it did not meet regulatory requirements and gave rise to concerns about the impact on competition.

In *ComReg v Eircom Limited*, ComReg asked the High Court to rule on a step plan which it had proposed for the review of 320,000 digital documents for privileged and irrelevant confidential material that were seized during the raid at Eir's offices. The Court confirmed it has jurisdiction to approve the use of a step plan which provides for the use of keywords to determine whether seized information is privileged or irrelevant. While it recognised Eir's right to maintain privilege and confidentiality, it determined that the search for these documents must be conducted by ComReg in accordance with an agreed step plan. It appears from this case that the Court does not have the power to order that search terms are used if an agreement is not reached. However, it may give other directions, including to appoint an independent legally qualified person to prepare a report to assist the Court in determining whether the seized information is privileged or irrelevant to the CCPC's investigation. The more recent case of CCPC v Homesecure and CCPC v Phonewatch has been adjourned in the hope that the parties will agree a step plan with search terms to identify legally privileged materials.

These recent High Court proceedings reveal that the regulators are responding to the concerns raised in the Irish Cement case. Regulators are attempting to formalise their approach to searching documents by agreeing a proposed 'step plan' with the parties involved and, where agreement cannot be reached, requesting the High Court to intervene.

This brings welcome clarity. However, there are important nuances between the inspection powers of the various regulators, which is likely to result in different regulators taking diverging approaches to the search and seizure of documents during an inspection. It is crucial to be aware of, and give due consideration to, these nuances.

# Preparing for a dawn raid

This trend of greater dawn raid activity is expected to continue. Given the increased likelihood of dawn raids, the reputational risks involved and the potential for fines, it is more important now than ever that businesses prepare for and respond appropriately to an unannounced inspection. This includes making appropriate privacy and legal privilege claims over documents early in the investigation. Dawn raids happen quickly and can come with or without advance notice, so it is crucial to have adequate protocols in place.

Our cross departmental dawn raid response team is market leading and internationally recognised. We advise clients to put in place and maintain robust competition law compliance protocols to lower any risk of being subject to competition law enforcement proceedings. We also provide bespoke advice to clients to ensure they are 'dawn raid ready' by providing training and guidelines so staff know what to do in the event of a dawn raid.

If you have any queries about dawn raids and how you can prepare for them, please contact a member of our Competition, Antitrust & Foreign Investment team.

# New EU Cybersecurity Directive – NIS2

**Julie Austin**
Partner,
Privacy & Data Security
jaustin@mhc.ie

**Jevan Neilan**
Head of
San Francisco Office
jneilan@mhc.ie

With the threat of cybersecurity attacks on the rise, including those targeting critical industries and essential infrastructure, the new Network and Information Systems Directive (NIS2) will raise the bar for cybersecurity in the EU. NIS2 must be transposed by Member States on 17 October 2024. It places obligations on Member States and individual organisations in critical sectors. Affected organisations will need to assess their obligations and develop a compliance plan to avoid potential sanctions. These sanctions include administrative fines and personal liability for those in senior management positions regarding certain obligations.

NIS2 essentially functions as an update to the previous NIS Directive (NIS1) which was implemented in 2016. The updates include broadening the scope of cybersecurity regulations to include new industries, organisations and sectors that were not previously captured by NIS1. These include medical devices, pharma, R&D of medicinal products and wholesale food businesses.

The goal of NIS2 is to further enhance the work started by NIS1 to build a high common level of cybersecurity across the EU. The key points of NIS2 include:

- **Increased scope**: NIS2 casts a wider net than NIS1 encompassing not just critical infrastructure sectors like energy and transportation, but also important sectors like:
  - Online marketplaces
  - Food production, and
  - Certain manufacturers.

Entities regulated under NIS2 are categorised as 'Essential' or 'Important' depending on factors such as size, industry sector and criticality.

- **Notification obligations**: NIS2 imposes phased notification obligations for cybersecurity incidents which have a 'significant impact' on the provision of an organisation's services. These notifications must be made to the relevant competent authority or the Computer Security Incident Response Team (CSIRT).
- **Cybersecurity risk management measures**: Essential and important entities will need to take appropriate and proportional technical, operational, and organisational security measures. These measures aim to manage the risks posed to the systems underpinning their services and to prevent or minimise the impact of incidents on their and others' services. NIS2 includes a non-exhaustive list of 10 key measures including supply chain security, and human resources security.

- **Supervision**: The NIS1 concepts of "operators of essential services" and "digital service providers" will be replaced by "Essential" and "Important" entities under NIS2 - in basic terms, these are entities in sectors which are essential for the economy and society. Essential entities will face increased supervision including regular audits, inspections, and information requests from authorities. Important entities will face checks triggered by incidents, related company issues, or random checks.
- **Fines and enforcement**: NIS2 provides national authorities with a minimum list of enforcement powers for non-compliance. It mandates increased fines and penalties in the event of failure to comply with NIS2:
    - Essential entities could face administrative fines of up to €10 million or 2% of total annual worldwide annual turnover, whichever is higher. However, individual EU countries may set the maximums even higher.
    - Important entities could face administrative fines up to €7 million, or 1.4% total annual worldwide turnover, whichever is higher.
- **Leadership accountability**: Senior management can be held liable for failing to have cybersecurity risk management measures in place. These measures will be provided for in national legislation.

## Next steps

NIS2 affects more industry sectors, has stricter reporting and supervisory requirements, and carries heavier fines for non-compliance than NIS1. With Member States required to transpose NIS2 by 17 October 2024, organisations should now take steps to consider whether NIS2 applies and, if so, how they plan to prepare for these increased cybersecurity rules.

For more information and expert advice, contact a member of our Privacy & Data Security team.

# Technology Sector

Our Technology team are the 'go to' lawyers for technology. We provide cutting edge advice on a range of complex legal matters to the world's leading tech and data driven companies.

From first round funding and global privacy structures, to strategic outsourcing partnerships and intellectual property management, we give smart advice. We regularly advise on topics at the intersection of law and new technology such as AI and Fintech, frequently when there is no definitive regulatory guidance. Clients trust us to steer them through new and sometimes unforeseen legal situations.

Central to our work in the technology sector is our market leading advice on data privacy and protection. We work closely with organisations to help them balance the often conflicting needs of monetisation and data protection. Our lawyers have also worked on some of the most high profile data breaches both locally and internationally, with a keen eye on the legal, commercial and reputational issues that arise.

**Contact our Technology 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 Technology Team

"Unrivalled legal and industry knowledge. They are the go-to firm for anything information technology related."

Legal 500

### Our Technology Team

*"At the cutting edge of the post-GDPR data privacy/protection world. They advise many of the world's biggest companies on GDPR compliance and in ground-breaking regulatory inquiries"*

Legal 500