WILLIAM FRY

EU Digital Reforms: Are you ready?

May **2025**

Strong Technology Regulation

Leo Moore
PARTNER
Head of Technology

For many years, Europe led the way with its privacy regulation, influencing the adoption of similar laws around the world. The next phase of EU regulation will see a seismic shift that will affect the entire technology sector. Inevitably it is going to have a profound impact on the use of technology by businesses and consumers. These changes will impact key areas such as non-personal data, content, technology platforms, cyber-security and artificial intelligence (AI).

Embark on a journey of digital excellence with William Fry. Let us guide you through the stages of assessing, preparing, and implementing compliance readiness, empowering your business to flourish in the digital age. Contact us today for a consultation and let us help you ensure a compliant and innovative future for your business.

EU Digital Reform Package – Current Status

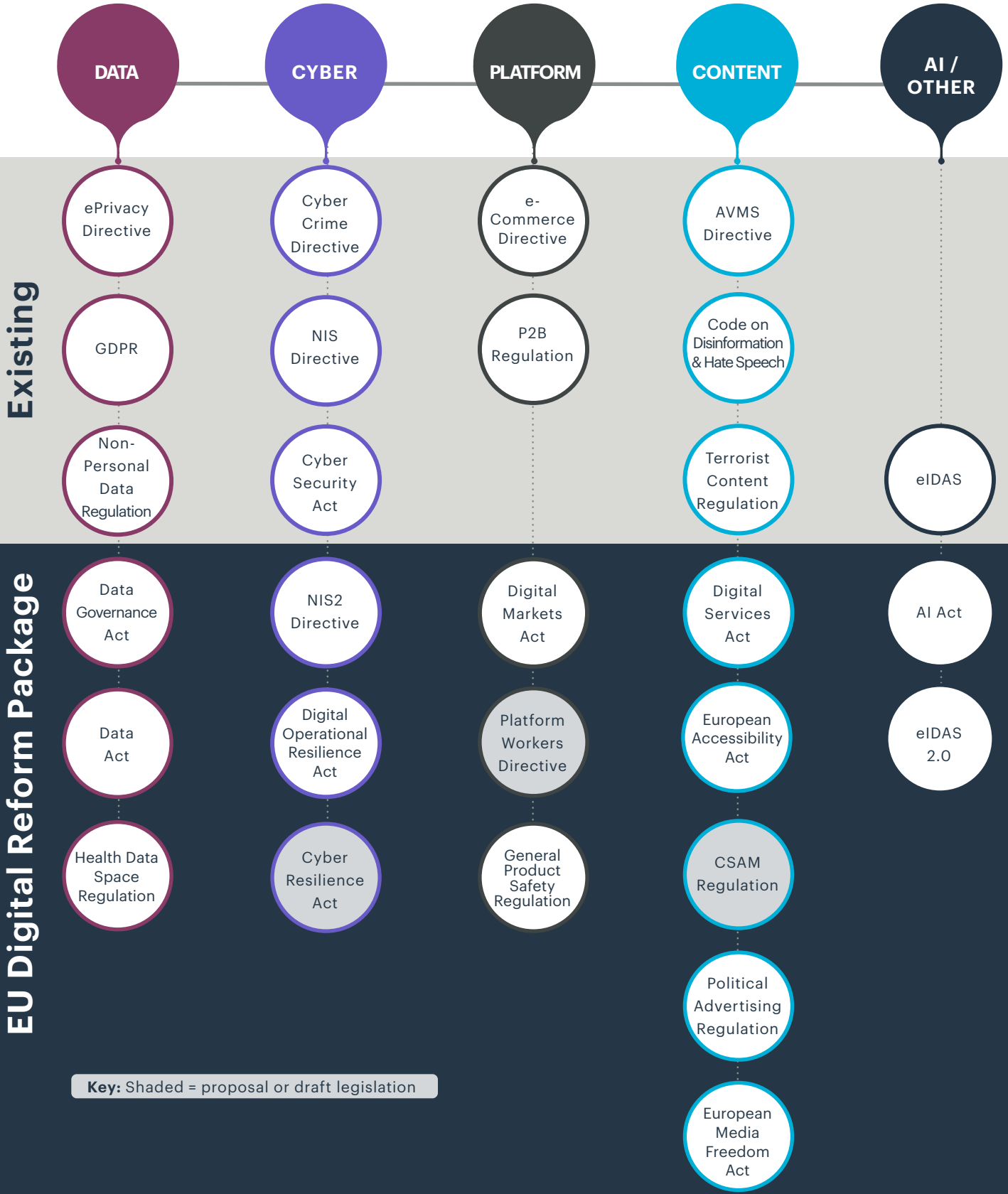


Table of contents

How to use this playbook

The purpose of this playbook is to give key stakeholders in your business a high level overview of what is to come and the impact this is expected to have on your business. This will help guide you in compliance, resource and legal budget planning over the next few years.

To assist you with analysing the impact of the EU Digital Reforms package on your business, we have assigned business impact ratings to the regulations, directives and acts. These outline the expected impact that each will have and help you identify if your business is within scope.

Business Impact Ratings

4-5	The regulation, directive or act will have far reaching and disruptive impacts on businesses.
3	The regulation, directive or act will have significant impacts on businesses.
1-2	The regulation, directive or act will have limited impact on businesses.

How we can help you

Our mission is to empower your business to navigate the complexities presented by the EU Digital Reforms Package and to thrive in the digital era. We will do this by working seamlessly with you to achieve a state of compliance readiness, whilst harnessing the wonderful benefits available from technological innovation. We understand that change in the technology and data sectors can be fast, that's why we pride ourselves on our agility and expertise in providing solutions to our Irish and international clients.

Our dedicated team provides comprehensive and innovative legal solutions to guide clients in navigating the myriad of complex technology regulations relating to data, cyber, content, platform and AI. The team assists clients on their journey by offering expert insights, strategic guidance, and tailored compliance readiness strategies.

We have formulated a proprietary, state of the art, three stage process to enable clients to ready themselves for compliance. Our goal is to simplify and streamline our advice to you in the most efficient way possible.

As a law firm, we have the unique benefit of being able to provide our reports under privilege. This facilitates a full, frank and productive exchange with all stakeholders to find the best solution for you.

Our 3 Stage Approach to Readiness

1 Stage One

ASSESSING APPLICABILITY

Using our unique solution, we can rapidly review your operations, industry, and digital initiatives, to determine the specific laws that are relevant to your organization. Our proprietary and easy process ensures that you are well-informed about the ever-evolving regulatory landscape. This enables you to make the right strategic decisions, as well as allowing you to prioritise compliance efforts effectively. To the extent you require input on only specific pieces of law, please let us know as we can customise our tool to suit your needs.

We will provide you with an **Impact Assessment Report** which sets out what regulations apply to you and our tailored recommendation of the next steps necessary for your business in order to be ready for the new laws.

2 Stage Two

READINESS ASSESSMENT

With a clear understanding of what laws apply to your business, our next step is to assess your business's readiness for achieving compliance. We engage with you and your stakeholders to provide an in-depth readiness assessment that evaluates your existing policies, processes, and technological infrastructure. Through this assessment, we will pinpoint key areas that require attention and optimisation, empowering you to pro-actively address problematic and costly compliance gaps.

We will provide you with a **Readiness Report** which sets out key gaps in compliance and what actions you need to take to enable your business to be ready for the applicable new or incoming regulation.

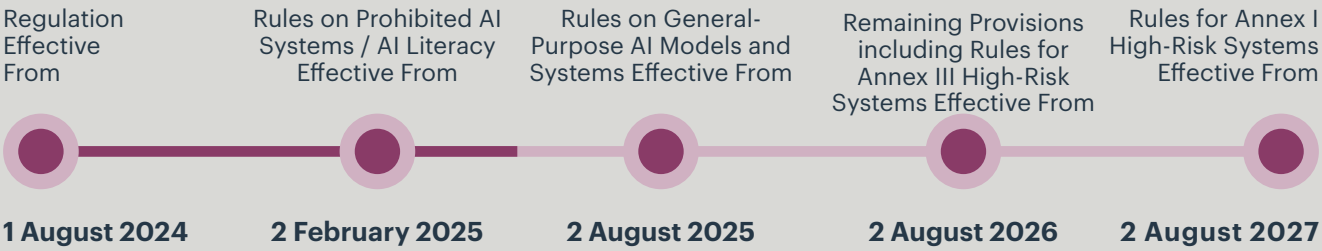
3 Stage Three

IMPLEMENTATION AND ONGOING SUPPORT

The final stage is implementing the actions identified in our Readiness Report. Our collaborative approach is designed to ensure that your compliance strategy aligns seamlessly with your business goals and budgets. Our team remains constantly available as needed, assisting with the practical implementation of compliance measures and helping you achieve and maintain regulatory adherence. We also provide you with access to exclusive content and insights from our leading experts on our TechReg Connect portal, so that you can stay up-to-date with the latest developments in the technology regulatory landscape.


AI

1.1 EU ARTIFICIAL INTELLIGENCE ACT (AI Act)



IMPACT RATING 4

What is it?

The AI Act imposes certain obligations regarding the use of AI in the European Union, depending on the level of risk associated with that use and the nature of the business' relationship with the AI system (e.g. developer, user, etc).

Who does it apply to?

The AI Act regulates the development and deployment of certain AI systems by requiring certain actions from businesses at all stages of the AI lifecycle. The AI Act applies to providers, deployers, importers, distributors, and authorised representatives of AI systems.

- **Who is a Provider?** Organisations that develop an AI system or general-purpose AI model, or that have an AI system or general purpose AI model developed, and places it on the market or puts it into service.
- **Who is a Deployer?** Anyone using an AI system.
- **Who is an Importer?** A natural or legal person located or established in the EU that places on the EU market an AI system that bears the name of a business established outside the EU.
- **Who is a Distributor?** A natural or legal person in the supply chain, other than a provider or the importer, that makes an AI system available in the EU.

What is an AI system, a general-purpose AI model, and a general-purpose AI system?

The AI Act defines these terms as follows:

'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

'general-purpose AI model' means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market.

'general-purpose AI system' means an AI system which is based on a general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems.

Key obligations

- The AI Act follows a risk-based approach, differentiating between uses of AI that create;
    i. an unacceptable risk;
    ii. a high-risk;
    iii. a low or minimal risk; or
    iv. a minimal risk (and which are not subject to any obligations under the AI Act).
- Since 2 February 2025, AI practices which are considered to create an unacceptable risk by contravening EU values (e.g. by infringing fundamental rights) are prohibited. These prohibited AI practices include the following:

Manipulative or Deceptive AI Systems	**AI systems that exploit vulnerabilities**
Social Scoring	**Predictive Policing Based on Profiling**
Untargeted Facial Recognition Databases	**Emotion Recognition in Workplaces and Educational Institutions**
Biometric Categorisation	**Real-Time Remote Biometric Identification for Law Enforcement**

- High-risk AI systems are categorised under two main Annexes in the AI Act. Under Annex I, An AI system is considered high-risk if it is used as a safety component of a product, or is itself a product covered by specific EU harmonisation legislation. Additionally, these products or AI systems require a third-party conformity assessment before market placement or service initiation. These rules will be effective from 2 August 2027.
- In contrast, high-risk AI systems under Annex III will be subjected to strict obligations from 2 August 2026. When evaluating whether an AI system is within the high-risk category, the purpose for which the AI system was deployed is of critical importance. The high-risk category requires an objective evaluation of any potential significant risk of harm to the health and safety or the fundamental rights of persons in light of the intended purpose. Annex III covers the following areas:

Remote Biometric Identification, Biometric Categorisation, and Emotion Recognition systems	**Safety components in Critical Infrastructure**
Education and Vocational Training	**Employment, Workers' Management and Access to Self-Employment**
Essential Private Services and Essential Public Services and Benefits	**Law Enforcement**
Migration, Asylum And Border Control Management	**Administration of Justice and Democratic Processes**

- Developers of high-risk AI systems will have to conduct a conformity assessment before being released on the EU market. The emphasis of the conformity assessment is on transparency and traceability of results with certain obligations in relation to security, human oversight and the implementation of internal controls. Deployers will also be required to carry out a fundamental rights impact assessment when using of certain high-risk AI systems.
- AI models and systems which otherwise only cause limited risks (e.g. simple customer service chatbots) face fewer obligations under the AI Act (e.g., transparency).
- The primary obligation on **all** AI systems, general-purpose AI models and general-purpose AI systems is that they must adhere to transparency requirements (e.g. by informing a natural person that they are communicating with an AI system). This may extend further to transparency regarding the decision-making process and any human oversight of the AI system (where applicable).
- Importantly, providers and deployers of **all** AI systems are also required to ensure their staff and other individuals involved in AI operations possess adequate AI literacy since 2 February 2025. This includes understanding the technical aspects of AI systems, proper application during development and deployment, and interpreting AI outputs correctly.
- Providers of general-purpose AI models will need to draw up and maintain technical documentation on the model's training, make documents and information available to downstream providers, and publish a summary of the content used for training the model.
- Additionally, providers of generative AI models will need to put policies in place to ensure compliance with EU law on copyright and related rights, in particular complying with any reservation of rights expressed by rightsholders against text and data mining. Providers will be able to show compliance with these obligations by signing up to approved Codes of Practice. The General-Purpose AI Code of Practice is currently in draft format and expected to be finalised in mid-2025.
- Providers of AI systems must register themselves and the system in an EU database.
- Importantly for organisations planning to deploy AI at the workplace, before putting into service or using a high-risk AI system, deployers who are employers must inform affected workers that they will be subject to the system.

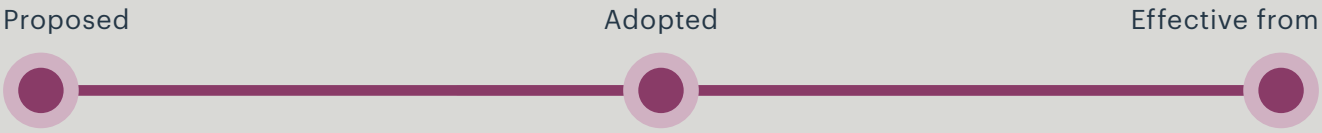
Business Impact

The AI Act has a broad application and applies to those developing, deploying or professionally using AI in the EU or for an EU audience. Impacted businesses should be aware that the 'prohibited practices' provisions in the AI Act are already in force with the vast majority of the remaining provisions, including obligations for high-risk AI systems, becoming effective from 2 August 2026.

The AI Act allows for the imposition of financial penalties for non-compliance with its provisions with fines up to €35,000,000 or 7% of worldwide annual turnover.

Content

2.1 DIGITAL SERVICES ACT (DSA)



IMPACT RATING 3

What is it?

The DSA aims to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses. The DSA will provide a common set of rules on intermediaries' obligations and accountability which will result in a high level of protection to users across the EU.

Who does it apply to?

The DSA imposes new and revised obligations on businesses that provide the following in the European Union:

(a) hosting, caching or mere conduit services, e.g. internet service providers, cloud service providers and other domain name service providers;

(b) online platforms e.g. social media services, online marketplaces; and

(c) online search engines.

Key obligations

The DSA gives users of the services more control over the content they engage with online and imposes new obligations on those entities that come within the DSA's scope:

(a) **Benefits for users of the services**

- Users will gain clearer insights into why specific content is recommended to them and will have the option to choose settings that do not include profiling.
- Targeted advertising directed at minors is not prohibited, and the use of sensitive data, such as sexual orientation, religion or ethnicity, is restricted.
- The new rules also enhance user protection against harmful and illegal content, significantly improving the speed and efficiency of removing such content.
- It aims to address harmful content, including political or health-related disinformation, even if it is not be illegal, while introducing rules to protect freedom of speech.
- The DSA also ensures that products sold online are safe and meet the highest EU standards

and that users have the ability to gain better knowledge of the actual sellers of the products they purchase online.

(b) **New obligations imposed on businesses:**

- Depending on what type of provider the business is, the DSA has a tiered structure of what obligations apply to that business. More obligations apply to providers that are Online Platforms or Online Search Engines; lesser obligations apply to those that are simply hosting content, caching or are mere conduits.
- Hosting providers are required to inform users when content is removed and provide an option for users to appeal the decision.
- Entities involved in hosting, caching, or acting as mere conduits will face new obligations, such as appointing a single point of contact and submitting annual reports on content removal.
- For Online Platforms a range of significant new obligations apply such as a prohibition on "dark patterns", transparency obligations in relation to ads, and recommender systems.
- Very large online platforms and search engines will have additional responsibilities, including establishing an internal compliance function and performing risk assessments.

Business Impact

The DSA has a significant impact on businesses that come within its scope requiring investment of resources to effect compliance. Such resourcing includes requiring significant time and incurring costs to achieve the necessary legal and technical changes. The key obligations imposed on providers are far reaching and cumbersome. If a business is found to be non-compliant, it can face fines of up to 6% of the preceding year's worldwide turnover. Furthermore, in a similar way to the GDPR, users can seek compensation for damage/loss due to an infringement of the DSA.

The Irish Digital Services Act 2024 implements the DSA and includes derogations in relation to investigation and enforcement. It does not alter or amend the DSA which has direct legal effect in all Member States of the EU and does not require any implementing measures in national law.

2.2 ONLINE SAFETY AND MEDIA REGULATION ACT (OSMRA)

IMPACT RATING 3

What is it?

The OSMRA marks the introduction of a first-of-its-kind media regulation regime. It established "Coimisiún na Meán" as a new regulator, the transposition of the revised Audiovisual Media Services Directive (**AVMSD**), and the creation of a robust regulatory framework to tackle the spread of harmful content online. The OSMRA amends the Broadcasting Act 2009 (as amended).

Who does it apply to?

- Providers of broadcasting services;
- Audiovisual on-demand media services; and
- Any 'relevant online service' (including video sharing platform services and other information society services on which user-generated content is made available) designated by the Commission as being subject to online safety codes.

Key obligations

Obligations arising from the implementation of the revised AVMSD include:

- Registration with the regulator established under the OSMRA, "Coimisiún na Meán" (the Irish Media Commission).
- An obligation to pay industry levies to fund the Coimisiún na Meán.
- Reporting requirements and Content Requirements -
    - Broadcasters and on-demand audio-visual media service providers must ensure they do not make available content that causes undue harm/offence or that incites violence/crime.
    - Relevant online services must not make available content that deals with criminal acts, or content that deals with suicide, self-harm, eating disorders, humiliation/bullying AND which poses a risk of death or reasonably foreseeable physical/mental harm to users.
    - Sound broadcasters must ensure at least 20% of the broadcasting time is dedicated to news and current affairs.
- Privacy Requirement - Programmes, and the means of making such programmes, must not

unreasonably encroach upon the privacy of any individuals.

- News and current affairs - News and current affairs content must be objective and impartial, and give due regard to all sides on a contentious matter of public interest.
- Advertisements - Political, industrial dispute or religious advertisements of a proselytising nature should not be made available. Sound broadcasters must ensure broadcasting time of advertisements does not exceed 15% of total broadcasting time.
- Programme material - Copies of programme material must be retained for a duration specified by the Commission.

New obligations with respect to online safety include:

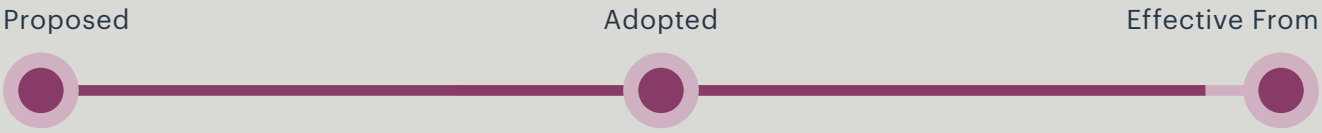
- Measures must be implemented to minimise the dissemination of "harmful online content" (as defined in the OSMRA) on designated online services.
- Compliance with binding online safety codes applicable to the providers of relevant online services designated as being subject to these codes, as issued by Coimisiún na Meán.
- Abidance by non-binding online safety guidance materials and advisory notes published by Coimisiún na Meán.

Business Impact

Administrative financial sanctions of up to €20,000,000 or 10% of turnover for the preceding financial year may be imposed, as well as the possibility of various enforcement orders being made by CoimisiCan na Meán or the Irish Courts.

As mentioned above, to regulate the availability of harmful online content, the providers of designated relevant online services will be required to comply with online safety codes. In October 2024, as part of its Online Safety Framework, Coimisiún na Meán published an Online Safety Code which mandates video-sharing platform services to implement measures protecting children and the general public from harmful and illegal content. These measures include content rating, age assurance, parental controls, and a user-friendly reporting system.

2.3 European Accessibility Act (EAA)



IMPACT RATING 3

What is it?

The EAA introduces harmonised accessibility standards across the EU for a wide range of in-scope products and services in the private sector. The core aim of the EAA is to remove barriers for people with disabilities, ensuring they have equal access to in-scope products and services. The EAA streamlines regulations, making it easier for businesses to comply with a single set of rules across the EU.

Who does it apply to?

The EAA applies to a wide range of economic operators involved in the production, distribution and provision of the in-scope products and services within the EU. A high-level summary of the roles as prescribed by the EAA are as follows:

- **Product Manufacturers:** are those that manufacture a product, or that have a product designed or manufactured, and market it under their name or trade mark.
- **Service Providers:** are those that provide a service on the EU market or make offers to provide such a service to consumers in the EU.
- **Importers:** are those that are established in the EU, and that place a product originating in a third country on the EU market.
- **Distributors:** are those in the supply chain, other than the manufacturer or the importer, that make a product available on the EU market.

The level of obligations imposed on a given economic operator will depend on (i) which of the above roles it fulfils in the supply chain and (i) the exact nature of the in-scope products and/or services it supplies (which are detailed further below). We have been providing guidance to clients across a diverse range of industries, such as retail, financial services, gaming, and e-commerce.

What products and services are in-scope of the EAA?

The EEA covers a wide range of products and services to ensure that they are accessible to people with disabilities, a non-exhaustive summary of which is outlined below. We recommend evaluating these categories in relation to your business's range of offerings to determine if any fall within the scope of the EAA. By doing so, you can ensure compliance and enhance accessibility for individuals with disabilities, aligning your products and services with the EAA's standards.

Products:

1. **Consumer General Purpose Computer Hardware and Operating Systems:** including personal computers, in particular desktops, notebooks, smartphones and tablets, and software which, among other things, handles the interface to hardware, schedules tasks, and allocates storage.
2. **Self-Service Terminals:** including automated teller machines (ATMs), ticketing machines, check-in machines, and interactive self-service terminals providing information.
3. **Consumer Terminal Equipment with interactive computing capability, used for Electronic Communications:** this category includes devices such as smartphones (which support voice calls, text messaging, and various communication apps), tablets (capable of video calls, messaging, and email through apps or web browsers), laptops and desktops (providing voice and video conferencing, email, and instant messaging), smart speaker devices (allowing users to make calls or send messages via voice commands), and webcams (used with computers or tablets for video communication).
4. **Consumer Terminal Equipment for Audiovisual Media Services:** including smart TVs, streaming devices, boxes provided by cable or satellite companies that allow users to access TV channels, game consoles that offer streaming services as well as gaming capabilities, and mobile devices used to access apps for streaming content.
5. **E-Readers:** this category includes specialised devices, both hardware and software, designed for accessing, navigating, reading, and using e-book files.

Services:

1. **Electronic Communications Services:** including services that involve communication between people or systems provided via the internet, such as email, messaging, and video calls.
2. **Audiovisual Media Services:** including any service that provides or facilitates viewing of visual and audio media, like streaming platforms, digital TV services, and on-demand content.
3. **Transport Services: several aspects of air, bus, rail, and water passenger transport services are covered by the EAA, namely:** websites, mobile apps, electronic tickets and ticking services, and delivery of real-time travel information, and interactive self-service terminals (except those built into vehicles used for transporting passengers).
4. **Consumer Banking Services:** including credit agreements, payment services , services linked to a payment account and electronic money.
5. **E-Books and Dedicated Software:** including services that provide digital book files, which can be accessed, navigated, read, and used. This includes software and mobile apps designed for these purposes.
6. **E-Commerce:** including services provided at a distance through websites and mobile device-based services by electronic means and at the individual request of a consumer with a view to concluding a contract, for example online shopping.

There are several exceptions to the EAA scope coverage which economic operators should explore when analysing the extent to which the products and/or services it provides are caught within the EAA's remit.

Key obligations

The EAA outlines broad design requirements to ensure that products and services are accessible to those individuals with disabilities. As an economic operator involved in the supply chain of same, you are required to:

- In-scope products are:
    - Design and produce products to maximise their use by people with disabilities.
    - Adhere to detailed rules regarding information and instructions, user interface and functionality design, support services and packaging.
- When providing in-scope services, that:
    - Provide consumers with information about the service, its accessibility features, and facilities.
    - Ensure websites and mobile devices are easily accessible.
    - Offer support systems, such as help desks, call centres, and training, in an accessible manner.
    - Implement practices, policies, and procedures to address the needs of people with disabilities.

Additionally, the EAA imposes specific requirements on manufacturers, service providers and importers, including document keeping obligations, conformity assessments and packaging requirements.

Business Impact

As the EAA becomes enforceable on 28 June 2025, businesses should use this lead-in time to take proactive steps to ensure compliance and enhance accessibility for individuals with disabilities. Initially, we recommend analysing the products and services offered by the business to identify those that fall within the scope of the EAA. Following this, a review of the business's role concerning the identified in-scope products and services is essential. Assessing current compliance measures is beneficial to determine if any exemptions might apply, thereby streamlining EAA compliance requirements. Finally, businesses should develop a comprehensive plan to ensure all products and services meet the accessibility standards prescribed by the EAA. This plan should outline timelines, responsible parties, and specific actions to be taken. All elements should be documented in a manner that is presentable to a regulator, should such a request arise. Non-compliance with the EAA may result in fines of up to €60,000 and/or imprisonment of up to 18 months, with both companies and their officers potentially liable.

If your business has not yet considered how the EAA might affect it yet, our Technology Team at William Fry has been helping clients from various industries with this and would be happy to assist with a detailed analysis.

2.4 Other Regulations and Acts

Terrorist Content Online Regulation (TCOR)

The Terrorist Content Online Regulation (**TCOR**) is an EU-wide law designed to counteract the dissemination of terrorist content online and ensure its swift removal by hosting service providers. Enacted to enhance online safety, TCOR mandates that hosting service providers take proactive measures to prevent their platforms from being used to spread terrorist content, which includes incitement, solicitation, threats, or instructions for terrorist activities.

In Ireland, the implementation of TCOR is overseen by Coimisiún na Meán which has established a detailed decision-making framework to identify hosting service providers exposed to terrorist content and enforce compliance with TCOR. If a hosting service provider is found to be repeatedly hosting terrorist content, it must undertake specific measures to protect its services and report these actions to Coimisiún na Meán. Additionally, An Garda Síochána, Ireland's national police service, is authorised to issue removal orders for terrorist content, ensuring rapid response and coordination with the regulatory framework.

Child Sexual Abuse Material Regulation

The proposed EU Regulation on Child Sexual Abuse Material (**CSAM**) aims to create a framework to combat online child sexual abuse across member states. It imposes obligations on service providers to implement robust child protection measures. While the goal of protecting children is widely supported, the proposal gives rise to concerns about privacy and data protection. Stakeholders stress the need for alignment with existing laws like the GDPR and the preservation of end-to-end encryption. Due to these conflicting views, negotiations on this new law have stalled. In April 2024, the European Parliament extended the current e-Privacy derogation, allowing voluntary CSAM detection by internet platforms until April 2026, so that an agreement on the long-term legal framework to prevent and combat child sexual abuse online can be reached.

Political Advertising Regulation

The new Regulation (EU) 2024/900 on the transparency and targeting of political advertising, adopted in March 2024, seeks to improve transparency and accountability in political advertising across member states. It mandates stringent requirements for service providers, such as clear labelling of political ads and disclosure of funding sources. Although the regulation is now in force, most of its provisions will take effect in all member states starting from 10 October 2025.

European Media Freedom Act

The European Media Freedom Act (**EMFA**), which came into force on May 7, 2024, aims to protect media pluralism and independence across the EU. The new rules will apply fully as of 8 August 2025. In Ireland, the implementation of EMFA is facilitated through the European Union (Media Freedom Act) Regulations 2025, which came into operation on February 8, 2025. These regulations designate Coimisiún na Meán as the National Regulatory Authority responsible for ensuring compliance with EMFA's provisions. The EMFA introduces measures to safeguard editorial independence, protect journalistic sources, and enhance transparency in media ownership and state advertising.

PLATFORM

3.1 DIGITAL MARKETS ACT (DMA)

IMPACT RATING 5

What is it?

The DMA aims to ensure that large online platforms which act as "gatekeepers" act in a fair manner online. Gatekeeper platforms are digital platforms with a systemic role in the internal market that function as bottlenecks between businesses and consumers for important digital services, some of whom are also regulated by the DSA. The DMA establishes narrowly defined objective criteria for qualifying as a "gatekeeper" under the DMA, allowing it to target issues as regards large, systemic online platforms.

Who does it apply to?

The DMA establishes the criteria for qualifying a large online platform as a "gatekeeper". The criteria will be met if a company:

- has a strong economic position;
- significant impact on the internal market; and
- is active in multiple EU countries with a strong intermediation position, meaning that it links a large user base to a large number of businesses, has (or is about to have) an entrenched and durable position in the market, meaning that it is stable over time if the company met the other two criteria in each of the last three financial years.

Key obligations

Gatekeepers must not:

- process the data of end users using services of third parties that make use of core platform services of the Gatekeeper;
- combine or cross use personal data obtained from different core platforms offered by the Gatekeeper or third party operators;
- sign end users to other services of the Gatekeeper to combine personal data;
- prohibit business users from offering the same products or services through other platforms or channels at prices or conditions that are different from those offered through the online intermediation services of the Gatekeeper;

- limit end users / businesses using the gatekeepers core platform to a specific identification service, web browser engine or a payment service etc.;
- treat their own services more favourably, in ranking and related indexing and crawling; or
- restrict technically or otherwise the ability of end users to switch between, and subscribe to, different software applications and services that are accessed using the core platform services of the Gatekeeper.

Gatekeepers must:

- allow business users, to communicate freely and promote offers to end users via the Gatekeeper core platform service or other channels and conclude contracts with those end users, regardless of whether, for that purpose, they use the core platform services of the Gatekeeper;
- provide each advertiser availing of advertising services with information on a daily basis free of charge, concerning each advertisement placed by the advertiser;
- allow end users to access and use, through its core platform services, content, subscriptions, features or other items, by using the software application of a business user, including where those end users acquired such items from the relevant business user without using the core platform services of the Gatekeeper; and
- technically enable end users to easily un-install any software applications or change default settings or enable the installation of third-party software on the operating system of the Gatekeeper.

Gatekeepers should provide:

- end users and authorised third parties with effective portability of data relevant to the end user in the context of the use of the relevant core platform service;
- access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on its online search engines to third parties using the platform; and
- general conditions of access, including an alternative dispute settlement mechanism.

Gatekeepers should not:

- have general conditions for terminating the provision of a core platform service that are disproportionate.

Business Impact

If a Gatekeeper does not comply with the rules, the Commission can impose fines of up to 10% of the company's total worldwide annual turnover or 20% in the event of repeated infringements and periodic penalty payments of up to 5% of the company's total worldwide daily turnover. In case of systematic infringements, the Commission can impose additional measures. Where necessary to achieve compliance, and where no alternative, equally effective measures are available. These can include structural remedies, such as obliging a gatekeeper to sell a business, or parts of it (e.g. selling

business divisions, assets, intellectual property rights or brands), or banning a gatekeeper from acquiring any company that provides services in the digital sector or services enabling the collection of data affected by the systematic non-compliance.

To date the EU Commission has designated several gatekeepers under the DMA and identified a range of core platforms services provided by these gatekeepers. Such services cover well-known search engines, app stores, messenger services, and online intermediaries.

3.2 General Product Safety Regulation

IMPACT RATING 2

What is it?

The GPSR replaces the current General Product Safety Directive and Food Imitating Product Directive. It modernises the EU general product safety framework as applies to all products and aims to address new challenges posed to product safety due to advancements in technology. The GPSR requires that all consumer products on the EU markets are safe and established specific obligations for business to ensure this.

Who does it apply to?

The GPSR applies to several key players, most notably ***Economic Operators*** and ***Providers of an Online Marketplace***.

Economic Operator:
The GPSR defines an economic operator as including: manufacturers, authorised representatives, importers, distributors, fulfilment service providers and any other person who is subject to obligations in relation to the manufacture of products or making them available within the EU.

Provider of an Online Marketplace:
Providers of an Online marketplace are defined as providers of an intermediary service using an online interface, which allows consumers to conclude distance contracts with traders for the sale of products.

Key obligations

All economic operators must:

- Only place/make available safe products on the market;
- Ensure they have internal processes in place to enable for product safety so that that can comply with the GSPR; and
- Various information obligations in relation to specific products.

In addition to the general obligations above, a company's obligations under the GPSR will depend on their specific category within framework. Specifically, Providers of an Online Marketplace must:

- Establish a single point of contact enabling direct communication with consumers and market surveillance authorities in relation to product safety issues;

- Remove and disable access to dangerous content when ordered by the relevant market surveillance authority; and
- Design their online interface in a way that enables traders to provide and display certain minimum information requirements on the product.

Business Impact

The GSPR requires economic operators and providers of online marketplaces to take a number of steps to ensure the safety of products placed on the EU market and modernise their practices to reflect the large-scale digitalisation of commerce. The GPSR was implemented into Irish law pursuant to the Irish General Product Safety Regulations 2024. It provides that committing an offence can result in a summary conviction with a fine of up to €5,000 and/or imprisonment for up to 6 months. On indictment, the penalties increase to a fine of up to €500,000 and/or imprisonment for up to 2 years. Additionally, individuals may be held personally liable if the offence was committed with their consent, connivance, or due to their neglect.


DATA

4.1 EU DATA ACT

Effective from

11 January 2024

Obligations Applicable From

12 September 2025

IMPACT RATING 3

What is it?

The Data Act is a blueprint for the free flow of data and innovation in the digital space. It allows access to data generated by providers and manufacturers of connected devices and smart objects in certain instances. For end-users (both B2C and B2B), the Data Act will reinforce the GDPR's right to data portability as it will permit end-users to switch providers and facilitate the transfer of data gathered through smart objects and connected devices from one provider to another. The Data Act is part of a broader package of legislation (including the DGA and the EHDSR) aimed at clarifying who can create value from data and under which conditions.

Who does it apply to?

The Data Act applies to manufacturers, providers of connected products and related services, digital service providers, as well as public authorities in the EU. It also applies to various types of data which are generated by these providers and their users.

Key obligations

Organisations within scope of the Data Act are obliged to ensure:

- **Data Access:** Provide relevant data to a user, on request, without undue delay or charge, subject to certain restrictions regarding disclosure of trade secrets and personal data.
- **Data Sharing on Request:** Provide relevant data to third parties upon request by a user (including potentially to a competitor business).
- **Fair, Reasonable and Non-Discriminatory Terms:** Ensure that when obliged to make data available to a data recipient, it is done on fair, reasonable and non-discriminatory terms and in a transparent manner, pursuant to unfair contract restrictions and reasonable compensation (in the case of SME organisations which are data recipients, subject to a cap at the cost of making the data available).
- **Data Sharing with Public-Bodies:** Make data available without undue delay to public bodies in the EU where there is an exceptional need to use the requested data. This can include, for example, circumstances where the data recipient is responding to, preventing or recovering from a public emergency.

- **Data Switching:** Enable customers to switch easily to another data processing service provider (such as an IaaS, PaaS or SaaS provider). The Data Act will require in-scope providers to ensure interoperability for customer switching.

Business Impact

Echoing similarities to the GDPR, Member States must lay down the rules on penalties for infringements of the Data Act that are "effective proportionate and dissuasive". We await implementing legislation in Ireland that will provide specific details in relation to penalties.

In relation to certain infringements of the data access and data sharing provisions, the Data Protection Commission of Ireland may impose fines within its scope of competence as provided for in the GDPR, up to €20 million euro of 4% of global turnover.

4.2 EU DATA GOVERNANCE ACT (DGA)

Effective from

23 June 2022

Applicable from

24 September 2023

IMPACT RATING 3

What is it?

The DGA aims to strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data. The DGA will support the set-up and development of European data spaces in strategic domains, involving both private and public players, in sectors such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills. It will make more data available and facilitate data sharing across sectors and EU countries in order to use data for the benefit of European citizens and businesses.

Who does it apply to?

The DGA applies to both personal and non-personal data, and imposes obligations on public sector bodies, including new types of organisations introduced by the DGA:

- **Data Intermediaries:** These are providers of data intermediary services, who provide infrastructure for data to be hosted, accessed, shared and exchanged. Data intermediaries need to notify the competent authority of their intention to provide these services.
- **Data Altruism Organisations:** Organisations which qualify as data altruism organisations are those which are encouraged to share personal or non-personal data on a voluntary basis for the public good.

Key obligations

- **Transparency:** The DGA requires data intermediaries to ensure access to their service is fair, transparent and non-discriminatory. Data altruism organisations must keep accurate records of processing of data held by them, such as information on entities or individuals who have given data access, and the date, duration and purposes of processing.
- **Consent Tools:** Data altruism organisations must provide tools for obtaining consent from data subjects or permission to process data from data users. These tools must also provide for the easy withdrawal of this consent and permission.
- **Maintain Neutrality:** The DGA sets strict neutrality requirements. Data altruism organisations must avoid conflicts of interest by separating their data altruism function from all other structures, while data intermediaries must only use data for the purpose of providing it to data users.

- **Data Exchange:** Data intermediaries are required to take measures to ensure interoperability with one another by using commonly used open standards in the sector in which they operate.
- **Anonymisation / Pseudonymisation & Security:** The DGA sets out strict requirements in relation to anonymisation / pseudonymisation techniques and secure storage and processing environments to ensure an appropriate level of protection of data in scope of the DGA.

Other Features

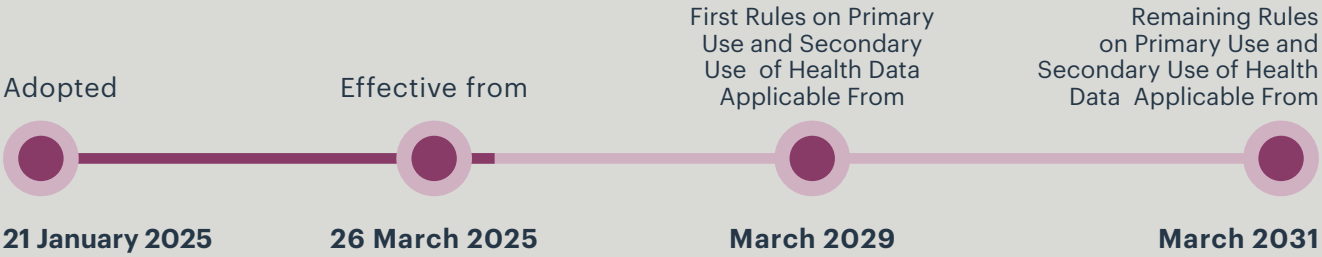
- **Data Pools:** Under the DGA, organisations can avail of 'data pools' to receive and hold data in a controlled environment as a result of businesses combining, exchanging and sharing such data for defined purposes, such as research and innovation;
- **European Data Innovation Board:** The DGA established a European Data Innovation Board (EDIB) by the European Commission. The EDIB comprises various stakeholders from EU bodies, who ensure the sharing of data occurs in line with best practices.

Business Impact

The DGA does not explicitly provide for sanctions, pointing to the role of member states to establish provisions for penalties applicable to violations of obligations, as well as to take all necessary measures to ensure their enforcement.

Member states were given a date of 24 September 2023 to notify the EC of the said provisions and measures.

4.3 EUROPEAN HEALTH DATA SPACE REGULATION (EHDSR)



IMPACT RATING **1-2**

What is it?

The EHDSR aims to improve the 'primary use' of health data by empowering individuals to access, control and share their own health data. The EHDSR also enables the sharing of health data to support a number of 'second use' activities carried out across the EU including for research, innovation, policy-making and regulatory purposes. The EHDSR supports the use of health data for better healthcare delivery and enables the EU to make use of the potential offered by a safe and secure exchange, use and reuse of health data.

Who does it apply to?

The EHDSR applies to any "health data holder", defined widely to include any entity in the healthcare or care sector, and any entity developing products or services intended for the health, healthcare or care sectors, who has either: (i) the right or obligation as a controller to process health data; or (ii) the ability to make non-personal health data available through the control of the technical design of a product or related service. This includes most hospitals, public health bodies, pharmaceutical and MedTech companies and is particularly applicable to entities operating in the Life Sciences sector.

Key obligations

- **Data Access:** Individuals must be granted access to their personal electronic health records free of charge and in a user-friendly format.
- **Data Permits:** Health data holders are required to share certain health data with health data users who receive a data permit from designated health data access bodies.
- **Interoperability:** Manufacturers of health record systems must certify compliance with interoperability and data security mandatory requirements by using a new European electronic health record exchange format.

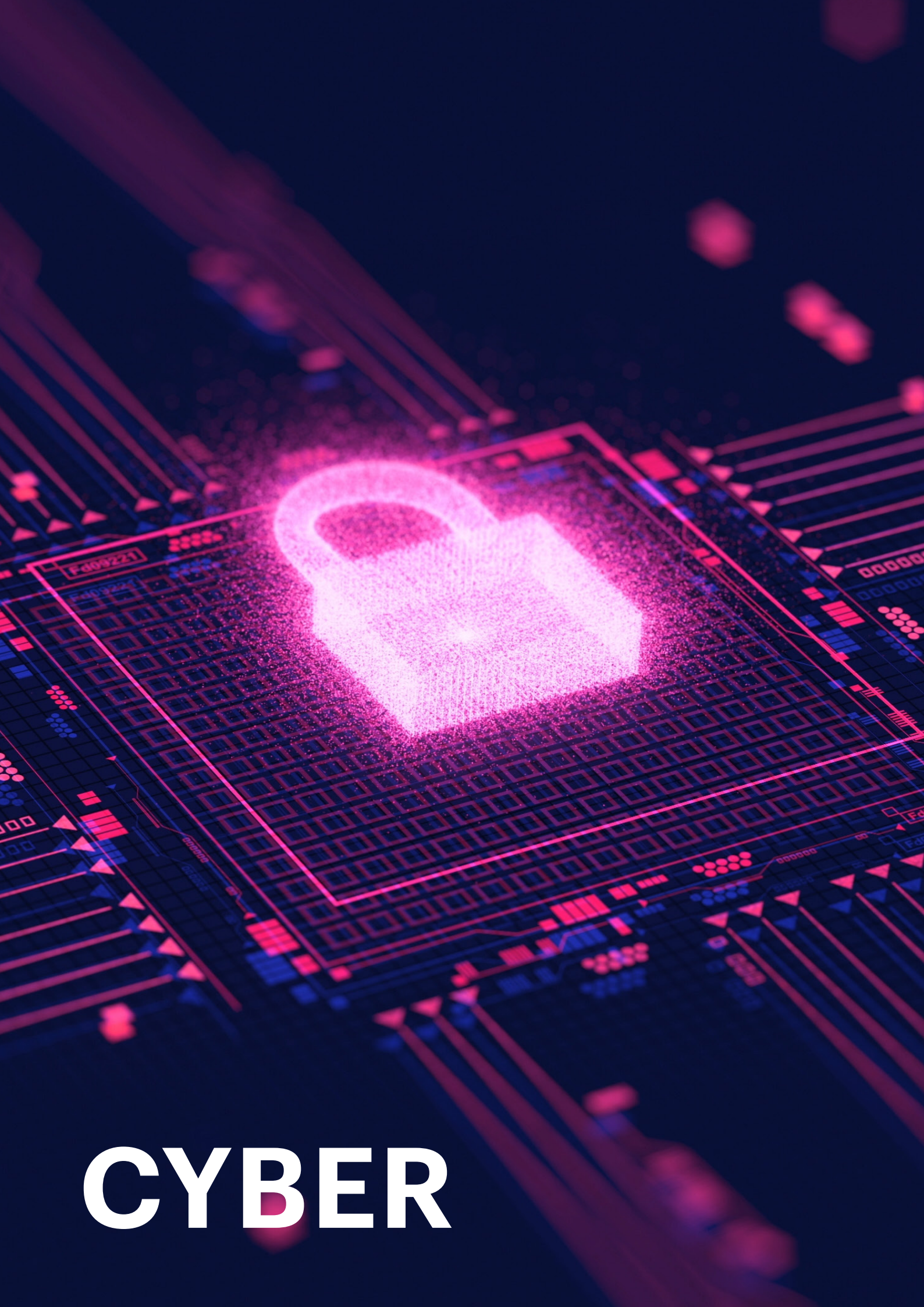
Other Features

By 2027, each EU country must establish a Digital Health Authority, a Health Data Access Body, and Market Surveillance Authority to supervise and enforce the provisions of the EHDSR relating to health data. In particular, they must ensure the rights of individuals are protected and obligations of health data holders are applied in practice.

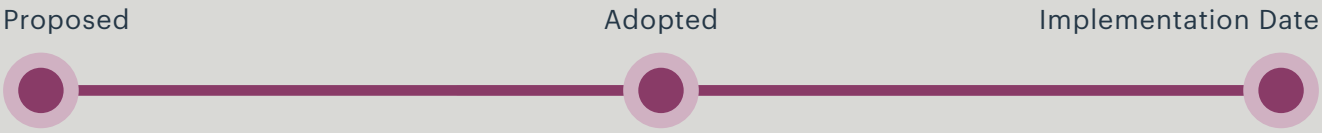
Business Impact

Digital Health Authorities will be responsible for enforcing the provisions of the EHDSR at EU Member State level. These authorities will have significant enforcement powers including the ability to impose fines from anywhere between €10,000,000 and €20,000,000 or from 2% to 4% of global turnover in the preceding financial year for non-compliance.

Ireland's implementation of the EHDSR is in its early stages – the Health Information Bill 2024 is part of a proposed suite of upcoming legislative measures aimed at implementing the EHDSR.


CYBER

5.1 NIS2 DIRECTIVE (NIS2D)



IMPACT RATING 4

What is it?

Ireland missed the transposition deadline of 17 October 2024 for the NIS2D. The predecessor of NIS2 (NIS1) remains in full effect and covers the most critical operators within the State on an interim basis until NIS2D is transposed into national law. Ireland's implementing legislation has been given priority drafting status by the Irish government.

The European Union Agency for Cybersecurity plays a crucial role in supporting the implementation of the NIS2D. This includes developing a European vulnerability registry, organising peer reviews, and maintaining a registry for entities providing cross-border services.

Who does it apply to?

NIS2D introduces new rules to determine which entities come within its scope. Entities in the following sectors will be subject to the NIS2D if they meet certain threshold criteria (micro and small businesses are excluded from its scope):

(a) **Essential Entities are those in the following sectors:** energy; transport; banking; financial markets infrastructure; health; drinking water and wastewater; digital infrastructure; public administration; space.

(b) **Important Entities being those in the following sectors:** postal and courier services; waste management; the manufacture, production and distribution of chemicals; food production, processing and distribution; manufacturing; digital providers (such as providers of online marketplaces, online search engines and social networking services platforms).

Key obligations

- Risk Management Measures: NIS2D will impose direct and ongoing obligations on "management bodies" concerning implementation and supervision of an organisation's compliance with the legislation. Notably, NIS2D specifically provides that C-Suite must follow "specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to assess cybersecurity risks and management practices and their impact on the operations of the entity" and approve cyber policies and programs.

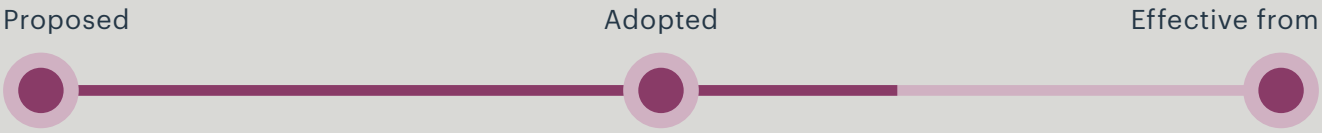
- Enhanced Security Requirements: Those within scope must implement and maintain cyber risk management measures that are "appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services."
- Incident Reporting Requirements: NIS2D imposes notification obligations in phases, including an initial notification within 24 hours of becoming aware of any incidents having a significant impact on the provision of a company's services or any significant cyber threat which those companies identify that could have potentially resulted in a significant incident. Previously, the NIS Directive required notification without "undue delay". Following the initial notification, entities in scope are required to meet "intermediate" and "final" reporting obligations.

Business Impact

Personal Liability: As well as imposing tight deadlines and reporting obligations, NIS2D adds an additional burden for directors of entities within scope, as it includes personal liability for non-compliance.

Fines and penalties: Member States are granted discretion to set out effective, proportionate and dissuasive penalties for breaches of NIS2D, such as fines and temporary suspensions from discharging managerial functions including at C-suite level. Further penalties may include administrative fines for certain breaches of up to €10,000,000 or 2% of total worldwide turnover (whichever is higher).

5.2 EU CYBER RESILIENCE ACT (CRA)



IMPACT RATING 3

What is it?

The CRA strengthens cybersecurity rules to ensure more secure hardware and software products. It aims to protect consumers and businesses buying or using products or software with a digital component. The CRA introduces mandatory cybersecurity requirements for manufacturers and retailers of such products, with this protection extending throughout the product lifecycle. This will ensure that hardware and software products are placed on the market with fewer vulnerabilities. The CRA will enable users to take cybersecurity into account when selecting and using products with a digital element.

Who does it apply to?

The CRA establishes new rules and obligations for **manufacturers, importers, and distributors** (as defined in the CRA) of digital products. A product with digital elements is defined as meaning *"any software or hardware product and its remote data processing solutions including software or hardware components placed on the market separately"*. Examples of products with digital elements include connected devices (e.g. consumer and industrial IoT), firewalls, operating systems and non-embedded software. The CRA also applies to AI systems, including the cybersecurity of products with digital elements that are classified as high-risk AI systems. There are certain exemptions to the above (for example, services including SaaS) unless they are part of integral remote data processing solutions for a product with digital elements.

Key obligations

The key obligations for manufacturers under the CRA can be categorised as follows:

- **Cyber Security by Design:** manufacturers are required to factor cybersecurity into the design, development, and production of products, undertake conformity assessments and provide ongoing security support for: (i) the expected lifetime of the product; or (ii) 5 years, (whichever is shorter).
- **Vulnerability Management:** manufacturers have to ensure that digital products are delivered without any known exploitable vulnerabilities and put in place appropriate policies and procedures for disclosure of identified vulnerabilities. Once a digital product is placed on the market, manufacturers must deploy regular vulnerability testing and remediate identified vulnerabilities by providing free updates and patches.

- **Market Surveillance:** manufacturers are required to provide information on compliance with the CRA to their market surveillance authority in their Member State of the EU (the relevant Irish authority has not yet been named). Any actively exploited vulnerabilities and security incidents must be reported to ENISA (the EU Cyber Security Agency) within 24 hours.

The CRA divides products with digital elements into two main categories based on their level of risk: (i) **default non-critical products**; and (ii) **critical products** (listed under Annex III), which are further divided into two sub-categories. Based on their level of risk, products with digital elements will be subject to less or more stringent conformity assessment procedures to demonstrate compliance with cybersecurity obligations.

Distributors and Importers also have obligations under the CRA including:

- (for importers), only placing products on the EU market that comply with the cybersecurity standards laid down by the CRA;
- informing the manufacturer without undue delay where a vulnerability is identified. Where a product with digital elements presents a significant cybersecurity risk, immediately informing the market surveillance authority;
- ensuring that the product is accompanied with appropriate instructions and information, verifying that the product with digital elements bears the CE mark, and that all conformity assessment procedures have been carried out.

Business Impact

Non-compliance by manufacturers with obligations set out in Annex I and Articles 10 and 11 carries fines of up to €15,000,000 or up to 2.5% of total worldwide annual turnover for the preceding financial year, whichever is higher. Non-compliance with any other obligations under the CRA carries fines of up to €10,000,000 or up to 2% of total worldwide annual turnover for the preceding financial year, whichever is higher.

The supply of incorrect, incomplete, or misleading information to notified bodies and market surveillance authorities after a disclosure is requested will incur a fine of €5,000,000 or up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

5.3 Digital Operational Resilience Act (DORA)

IMPACT RATING 3

What is it?

DORA aims to consolidate and upgrade ICT risk requirements in the EU financial sector, to guard against cyber-attacks and ensure that in-scope financial entities such as banks, insurance companies and investment firms are subject to uniform rules mitigating ICT-related operational risk. DORA sets out requirements for financial entities relating to governance structures, systems and controls. The management of in-scope financial entities will be required to define, approve, oversee and be accountable for the their ICT risk management framework.

Who does it apply to?

Subject to some exemptions, DORA applies to regulated financial services firm operating within the European Union defined under the Act as "financial entities". This covers a broad range of businesses from credit institutions to electronic money institutions, investment firms, insurance and reinsurance undertakings, insurance intermediaries, and many more.

Key obligations

(a) **Governance and Organisation:** DORA sets out requirements for entities in scope relating to governance structures, systems and controls.

(b) **ICT Risk Management Framework:** An ICT risk management framework is required which must be sound, comprehensive and well-documented.

(c) **Protection, Prevention and Detection:** ICT security must be monitored and reviewed frequently.

(d) **Response and Recovery:** Entities must have in place a comprehensive ICT business continuity policy, backup policies and procedures and restoration and recovery procedures and methods.

(e) **Learning and Communication:** Entities must have in place capabilities and staff to gather information on vulnerabilities, cyber-threats, ICT-related incidents and cyber-attacks and analyse the impact they have on their digital operational resilience.

(f) **ICT Incident Management, Classification and Reporting:** Financial entities must define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.

(g) **Testing:** DORA requires comprehensive digital operational resilience testing of ICT tools, systems, methodologies, practices and processes.

(h) **ICT Third-Party Risk Management:** Financial entities must adopt a strategy on ICT third-party risk and maintain a register of information relating to all contractual arrangements on the use of ICT services. New contractual arrangements must be reported to competent authorities on a yearly basis.

(i) **Critical ICT Third-Party Service Providers:** ICT third-party service providers designated as "critical" by the European Supervisory Authorities will be subject to oversight by a "Lead Overseer" (i.e., the relevant European Supervisory Authority appointed).

Business Impact

- Many of the obligations mandated under DORA will be familiar to financial entities in scope as there is significant overlap with existing EU and domestic laws and regulation, and guidance from the Central Bank of Ireland.
- DORA introduces mandatory contractual provisions which must be included in all contracts for ICT services, including both contracts for critical or important functions and for those that are not.
- ICT third-party service providers designated as "critical" by the European Supervisory Authorities will be subject to a new oversight framework led by the Lead Overseer appointed to them.
- DORA also introduces broad enforcement powers for competent authorities such as the Central Bank of Ireland including powers of investigation, inspection and requiring corrective and remedial measures for breaches of DORA to be put in place.

Why choose William Fry?

Trusted Expertise:

Our team comprises highly experienced and dedicated professionals. We have a long-standing track record advising leading global businesses in relation to technology regulations, offering you unparalleled insights and guidance.

Tailored Solutions:

We understand that every business is unique. Our approach is not one-size-fits-all. We craft strategies that are tailored to your specific needs, ensuring efficient and effective compliance strategies.

Innovation Embraced:

Our mission goes beyond compliance; it is about embracing the power of innovation. We help you leverage technology to drive growth and success while meeting regulatory requirements. We use bespoke designed systems and customised technology to drive efficiencies in providing this offering to you.

Client-Centric Approach:

Your success is our success. We work closely with you, providing ongoing support, education, and guidance throughout your compliance journey.

Ready to Thrive in the Digital Era? Contact Us Today

Key Contacts

Leo Moore
PARTNER
Head of Technology
+353 1 639 5152
leo.moore@williamfry.com

David Cullen
PARTNER
Technology
+353 1 639 5202
david.cullen@williamfry.com

Barry Scannell
PARTNER
Technology
+353 1 639 5393
barry.scannell@williamfry.com

Rachel Hayes
PARTNER
Technology
+353 1 639 5218
rachel.hayes@williamfry.com

WILLIAM FRY

DUBLIN | CORK | LONDON | NEW YORK | SAN FRANCISCO

WILLIAM FRY LLP | **T:** +353 1 639 5000 | **E:** info@williamfry.com

williamfry.com