



MAPLES
GROUP

AI Act

An Overview of its Key Provisions


August 2024

[maples.com](https://www.maples.com)



Contents

Introduction	1
AI Act - Background and Key Principles	2
Scope	3
Risk Categories	5
Obligations	8
Harmonised Standards and Codes	13
Key Supports for SMEs	14
Enforcement	17
Fines	18
Liability	18
Timeframe for Implementation	18
Contacts	19



Introduction to the AI Act

Introduction

This article seeks to provide an overview of the EU Artificial Intelligence Act (“AI Act”) by setting out the key concepts and framework of the AI Act. It also examines potential impact on the small and medium enterprise (“SME”) sector.

In this article, we examine:

- AI Act - Background and Key Principles;
- Scope;
- Risk categories;
- Obligations;
- Harmonised standards and codes;
- Key supports for SMEs;
- Enforcement;
- Fines;
- Liability; and
- Timeframe for implementation.



AI Act - Background and Key Principles

The AI Act is the culmination of several years of work among the European institutions which started in March 2018 as part of the EU's initiative "Europe for the Digital Decade". The AI Act creates harmonised rules for the placing on the market, putting into service and use of AI systems. It aims to balance innovation with a high level of protection for public interests such as health and safety, the protection of fundamental rights including democracy, the rule of law and environmental protection. It defines an "AI system" as "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" (emphasis added).

The AI Act sets out six general principles ("General Principles") which underpin the Regulation, with the aim of encouraging the design of "coherent, trustworthy and human-centric" AI. The principle of accountability is also expressed in a more general way throughout the AI Act. The six key principles are:

1. Human agency and oversight;
2. Technical robustness and safety;
3. Transparency;
4. Privacy and data governance;
5. Diversity, non-discrimination and fairness; and
6. Social and environmental well-being.



Scope

Who does the AI Act apply to?

AI Actors	
Operator	Umbrella term covering all of the below.
Provider	Any person, entity, public authority or body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.
Deployer	Any person or entity, public authority or body which uses an AI system under its authority in the course of a professional activity.
Importer	Any person or entity located or established in the EU which puts an AI product on the market where that product is trademarked by a person or entity who is outside the EU.
Distributor	Any person or entity (other than a Provider / Importer) in the supply chain which makes an AI system available on the EU market.
Authorised Representative	Any person or entity established in the EU who is performing obligations and procedures established under the AI Act on behalf of a Provider of an AI system or General Purpose AI system.

Where does the AI Act apply?

The AI Act has extra-territorial scope meaning that it applies to entities established in the EU and entities established outside the EU which put AI on, or into service on, the EU market. It will also apply where AI outputs generated outside the EU are used within the EU.

Entities providing AI systems which are established outside the EU but which are within the scope of the Act, must appoint an Authorised Representative who is established in the EU.

What does the AI Act not apply to?

The AI Act will not apply where an AI system is used in the following contexts:

- a. National security;
- b. Military and defence;
- c. Public authorities in 3rd country for law enforcement and judicial cooperation;
- d. Scientific research and development where this is AI's sole purpose;
- e. Research, testing and development prior to being placed on the market or put into service;
- f. Natural persons use of AI in a personal non-professional capacity; and
- g. Free and open-source licences (unless the AI system is prohibited or high-risk).

Risk Categories

The AI Act takes a risk-based approach to AI wherein the level of regulation applicable to an AI system will be based on the severity of harm it poses to fundamental rights and the likelihood of those harms materialising.

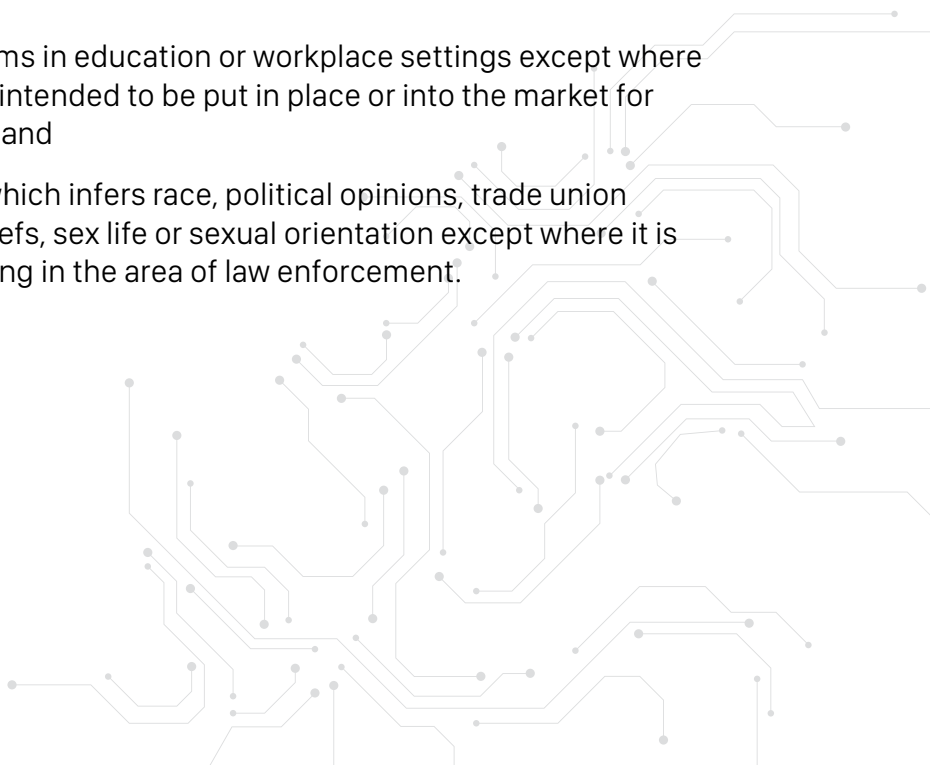
Under the AI Act, unacceptable risk AI is prohibited, high-risk AI (“HRAI”) is restricted and limited risk AI is subject to transparency requirements. General Purpose AI which incorporates generative AI is subject to specific provisions.

The AI Act creates four categories of risk for AI systems:

Prohibited AI

AI systems which carry an unacceptable level of risk to safety, security and fundamental rights are prohibited. This applies to AI systems which involve:

- i. behavioural manipulation based on subliminal, purposively manipulative / deceptive systems to impair decision making;
- ii. social scoring;
- iii. certain applications of predictive policing;
- iv. exploitation of vulnerabilities due to age, disability or social or economic circumstances which cause significant harm;
- v. real-time remote biometric identification which leads to detrimental or disproportionate treatment in other contexts, or which are not justified;
- vi. creation of facial recognition databases through indiscriminate scraping from CCTV or the internet;
- vii. emotion recognition systems in education or workplace settings except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons; and
- viii. biometric categorisation which infers race, political opinions, trade union membership, religious beliefs, sex life or sexual orientation except where it is lawful for labelling or filtering in the area of law enforcement.



High-Risk AI

AI systems which pose a high risk to health, safety, environment and fundamental rights are subject to restrictions. There are two categories of HRAI:

AI Systems as Products or Safety Component of Products

An AI system will be classified as a high-risk system if that system is:

- intended to be used as a safety component of a product, or if it is itself a product, covered by EU harmonisation legislation (which is listed in Annex II of the AI Act). Examples of such products include machinery, toys, marine equipment, medical devices and motor vehicles .

Standalone AI Systems

Standalone systems in the following areas:

- biometric systems not classified as prohibited AI;
- safety components in critical infrastructure systems including digital infrastructure;
- systems related to access to, and/or evaluating, education and vocational training;
- systems related to employee recruitment and/or performance management;
- certain systems related to essential private and public services/benefits such as healthcare, benefits, creditworthiness checks and life and healthcare insurance risk assessment and pricing;
- certain systems related to law enforcement such as risk assessment/ profiling, predictive policing, facial recognition and evidence analysis;
- certain systems related to migration, asylum and border control such as polygraphs, risk assessments, and asylum applications and
- certain systems related to administration of justice and democratic processes such as systems used by a judicial authority in applying the law and systems affecting voter decisions.

HRAI Carve-Outs

The AI Act includes carve outs for HRAI. An AI system will not be considered high-risk if it does not pose a significant harm to the health, safety or fundamental rights of persons, including by not materially influencing the outcome of decision-making. This will be the case where an AI system is intended to fulfil one or more of the following:

- perform narrow procedural tasks;
- improve the result of an activity previously completed by a human;
- detect decision-making patterns among humans but is not intended to influence or replace the human assessment; or
- perform a preparatory task to an assessment. However, in such cases, the Provider must be able to document the assessment it conducted prior to placing that product on the market which shows that the product is not high-risk. National authorities can request that copies of the risk assessment be furnished to them.

General Purpose AI

General Purpose AI (“GPAI”) models are those which are:

- trained with a **large amount of data** using self-supervision at scale;
- that displays **significant generality**;
- capable to competently perform a **wide range of distinct tasks**;
- can be **integrated** into a variety of downstream systems or applications.

GPAI models with systemic risk are subject to additional regulation. A GPAI model has systemic risk if:

- it has high impact capabilities (this is presumed where the cumulative amount of computation used for its training measured in floating point operations is greater than **10^(^25)**;
- the European Commission (the “Commission”) designates the system as being high-risk.

Limited Risk AI

This category applies to AI systems intended to interact directly with natural persons such as chat bots and AI systems which generate synthetic audio, image, video or text.

Obligations

This section provides an overview of the key compliance obligations under the AI Act based on the applicable operator and risk category.

AI Literacy

AI literacy is an overarching obligation that applies to all Providers and Deployers. They are required to take measures to ensure, to the best of their extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf. In taking such measures, factors such as: (i) an individual's technical knowledge, experience, education and training; (ii) the context the AI systems are used in; and (iii) the type of person on whom the AI systems will be used can be taken into account.

HRAI – Providers

Article	Requirement
8	Comply with the requirements laid down for HRAI, taking into account their intended purpose as well as the generally acknowledged state of the art on AI and AI-related technologies
9	Establish, implement, document, and maintain a risk management system
10	Develop AI systems using data which meets qualitative standards and engage in robust data governance
11	Draw up technical documentation prior to placing HRAI on the market and keep the documentation up-to-date
12	System must have automated record keeping
13	Ensure transparency and the provision of information to Deployers
14	Design system so that it can be effectively overseen by humans
15	Design system to ensure accuracy, robustness, cybersecurity and consistent performance throughout its life cycle

16, 49	Indicate on the system (or its packaging / documentation) the provider's name, registered trade name / trademark, and address
16, 17	Put in place a quality management system
16, 18	Retain documentation for 10 years after the HRAI system has been placed on the market
16, 19	Retain automatically generated logs to the extent such logs are under the Provider's control for the period appropriate to the purpose but for at least six months unless otherwise provided for in law. Financial institutions will retain logs automatically generated in accordance with financial services law
16, 43	Ensure that the HRAI system undergoes the relevant conformity assessment procedure before placing it on the market
16, 47	Draw up an EU declaration of conformity
16, 48	Affix CE mark to the system / packaging / documentation
16, 49	Providers must register themselves and their high-risk system with the EU HRAI database
16, 20	Where a high-risk system does not comply with the AI Act, take corrective measures and inform relevant authorities and other stakeholders
16	Where required, demonstrate compliance with the above requirements
16	Ensure that the HRAI system complies with accessibility requirements
21	Upon reasoned request, provide the competent authority all the information and documentation and automatically generated logs necessary to demonstrate the conformity of the high-risk AI system with the AI Act

HRAI - Deployer

Article	Requirement
26(1)	Implement technical and organisational measures to ensure use of high-risk complies with the instructions for use
26(2)	Assign human oversight to persons who have the necessary competence, training and authority, as well as the necessary support
26(4)	To the extent the deployer controls input data, ensure data is relevant and sufficiently representative in view of the intended purpose of the HRAI system
26(5)	Monitor the operation of the HRAI system on the basis of the instructions for use and, where relevant, update providers in accordance with post market monitoring requirements
26(6)	Retain automatically generated logs produced by the AI system for at least six months unless specified otherwise in other applicable national or EU law
26(7)	Inform employees if they will be subject to the use of a HRAI system
26(8)	Deployers who are public authorities using certain AI systems must register themselves and the system on the EU database
26(9)	Where relevant, conduct a data protection impact assessment in line with EU General Data Protection Regulation 2016/679 ("GDPR")
26(10)	Seek authorisation for use of HRAI for biometric identification where use is in the context of identifying a suspected / convicted criminal in targeted searches
26(11)	Inform individuals if a HRAI system is used to make decisions affecting them
26(12)	Cooperate with the relevant competent authorities in any action those authorities take in relation to the HRAI system

GPAI – Providers

GPAI providers will be subject to the same transparency requirements as apply to Limited Risk AI as described below. However, they are also subject to a number of GPAI specific requirements.

Article	Requirement
53(1a)	Draw up and keep up-to-date the technical documentation of the model (not applicable to certain free, open source models)
53(1b)	Draw up, keep up-to-date and make available information and documentation to providers of AI systems who intend to integrate the GPAI model into their AI systems (not applicable to certain free, open source models)
53(1c)	Put in place a policy to comply with EU law on copyright and related rights.
53(1d)	Draw up and make publicly available a sufficiently detailed summary about the content used for training the GPAI
53(3)	Cooperate as necessary with the Commission and the national competent authorities

Providers of GPAI which has systemic risk is also subject to an additional layer of regulation:

Article	Requirement
56(1a)	Perform model evaluation in accordance with standardised protocols and tools
56(1b)	Assess and mitigate possible systemic risks at EU level, including their sources, that may stem from the development, the placing on the market, or the use of general-purpose AI models with systemic risk
56(1c)	Track, document and report without undue delay to the AI Office and, as appropriate, national competent authorities, information about serious incidents and possible corrective measure
56(1d)	Ensure an adequate level of cybersecurity

Limited Risk AI - Providers and Deployers

Providers and users of certain AI systems where there is limited risk and GPAI systems are subject to transparency requirements. The legislative focus of the AI Act in relation to this category of AI systems is to ensure that AI generated content is clearly identifiable as such, and that users are made aware when they are interacting with AI.

Providers must comply with the following:

Article	Requirement
50(1)	Where AI systems are intended to interact with individuals, designing systems so that the individual is made aware that they are interacting with AI unless this is obvious
50(2)	Where AI systems are used to generate audio, image, video or text content, the content must have a watermark denoting that it is AI generated. Technical solutions must be effective, interoperable, robust and reliable

Deployers must comply with the following:

Article	Requirement
50(3)	Where AI is used for emotion recognition or biometric identification, inform the individual that this is so and process personal data in compliance with the GDPR
50(4)	Where AI systems are used to produce deepfakes or text which is published for the purposes of informing the public of matters of public interest, disclose that the content is AI generated

Harmonised Standards and Codes

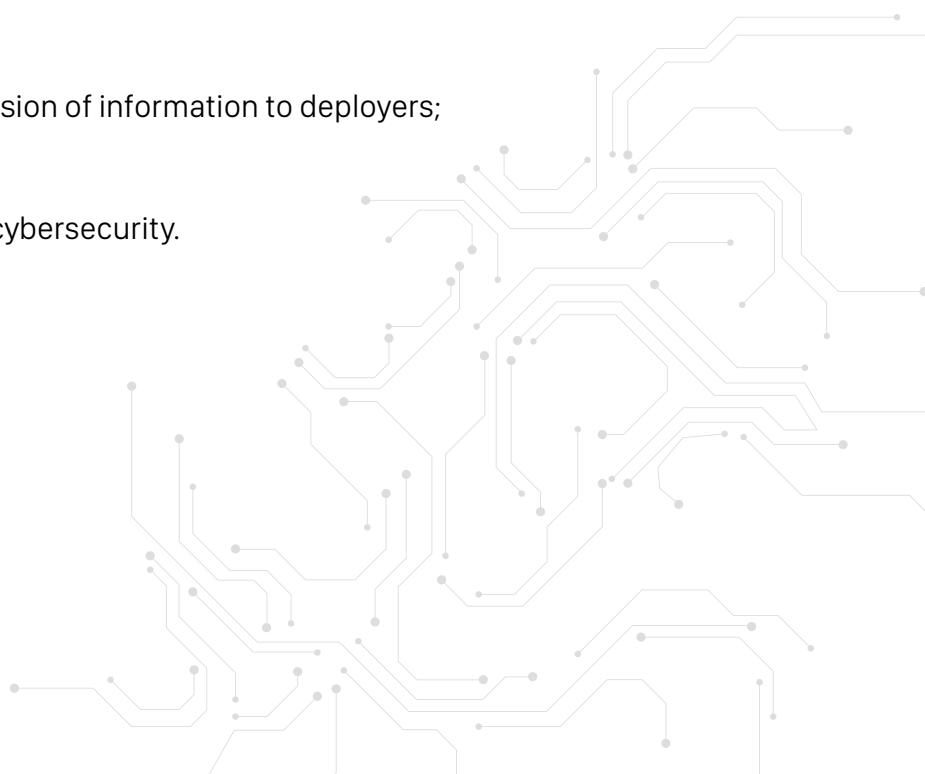
Harmonised Standards (Article 40): Under the AI Act, the Commission must request European standardisation organisations to draft a harmonised European standard to cover the core requirements applicable to GPAI and HRAI systems. When preparing the request, the Commission is required to consult with the EU AI Board (discussed below) and relevant stakeholders. Once developed, HRAI and GPAI which conform with the harmonised standards will be presumed to conform with the requirements of the AI Act to the extent that those standards cover those requirements.

Codes of Practice (Article 56): The AI Office will facilitate the development of codes of practice (“CoP”) by providers and national competent authorities (discussed below) which, at minimum, cover the obligations of providers of GPAI and GPAI with systemic risk.

The AI Office will assess the adequacy of CoPs and ifs CoPs are not drawn up within nine months of the AI Act coming into force, or are deemed inadequate by the Commission, the Commission may issue common rules for the implementation of the obligations of providers of GPAI and GPAI with systemic risk. The Commission may approve CoPs thereby giving them general validity within the EU.

Codes of Conduct (Article 95): The AI Office and EU Member States (“Member States”) will encourage and facilitate the development of Codes of Conduct (“CoC”) including voluntary adherence by AI systems other than HRAI to a subset of HRAI obligations. These obligations relate to:

- a. Risk management systems;
- b. Data and data governance;
- c. Technical documentation;
- d. Record keeping;
- e. Transparency and the provision of information to deployers;
- f. Human oversight; and
- g. Accuracy, robustness and cybersecurity.



Key Supports for SMEs

The AI Act contains specific provisions to promote and protect innovation, particularly within the SME¹ sector.

AI Regulatory Sandboxes

AI Regulatory Sandboxes (“Sandboxes”) are controlled environments within which AI systems can safely be developed and tested before they are put on the market. Each Member State will have at least one Sandbox.

Article	Support
58(2d)	SMEs will have access to the Sandboxes free of charge without prejudice to exceptional costs
58(2g)	Procedures, processes and administrative requirements for application, selection, participation and exiting the AI regulatory sandbox will be simple, easily intelligible, and clearly communicated in order to facilitate the participation of SMEs
58(3)	SMEs will be directed to pre-deployment services including guidance on the implementation of the AI Act and services such as assistance with documentation, certification testing and experimentation facilities, European Digital Innovation Hubs and centres of excellence
62(1a)	SMEs will have priority access to Sandboxes

¹ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF> - SME is defined as follows:

Medium Enterprise: 250 staff or less, annual turnover of €50 million or less, and / or annual balance sheet of €43 million or less

Small Enterprise: 50 staff or less, annual turnover and/or annual balance sheet of €10 million or less

Micro Enterprise: 10 staff or less, annual turnover and/or annual balance sheet of €2 million or less

Technical Documentation and Administration

Article	Support
11	SMEs may provide a simplified version of the technical documentation which is required for HRAI systems before they are placed on the market. The Commission will establish a simplified technical documentation form targeted at small and micro-enterprises. Simplified forms will be accepted for the purposes of conformity assessments
62(3a)	AI Office will provide standardised templates for documents required under the AI Act
62(3b)	AI Office will develop and maintain a single information platform providing easy to use information in relation to the AI Act
62(3c)	AI Office will organise public information campaigns to raise awareness about the obligations arising from the AI Act

Penalties

Article	Support
99(1)	When determining the level of fines to be issued for non-compliance with the AI Act by an SME, national authorities must take into account the interests and economic viability of the SME
99(6)	When fining an SME for non-compliance with the AI Act, the maximum fine will be the lower of the applicable percentage or amount, in contrast with non-SMEs which will be fined the higher of the applicable percentage or amount

Supports from National Authorities & the Commission

Article	Support
62(1b)	Organisation of specific awareness raising and training activities on the application of the AI Act tailored to the needs of SMEs
62(1c)	Use of dedicated channels for communicating with SMEs and local public authorities to advise on the application of the AI Act including in relation to Sandboxes
62(1d)	Facilitation SME participation in the development of standardisation
62(2)	Consideration of the needs of SME providers when setting fees for conformity assessments including reducing fees proportionate to the size of the entity
70(8)	Provide guidance and advice on the implementation of this Regulation
95(4)	Consideration of the interests and needs of SMEs when encouraging and facilitating the drawing up of the CoC
96(1)	Consideration of the needs of SMEs into account when issuing guidelines on the practical implementation of the AI Act



Enforcement

There will be a range of bodies and mechanisms put in place to enforce the AI Act.

At EU level, the AI Office will regulate the implementation of the AI Act across the Member States. The AI Board will comprise of one representative per Member State and the European Data Protection Supervisor and the EU AI Office will observe their meetings but cannot vote. The AI Board will oversee the application of the AI Act and act as an advisory body to the Commission. The Commission will also have powers to implement delegated legislation under the AI Act.

Ireland is obliged to establish or designate as independent national competent authorities (“NCA”) at least one:

1. notifying authority (“NA”) which will be responsible for assessing, notifying and monitoring conformity assessment bodies that can certify high-risk AI systems; and
2. market surveillance authority (“MSA”) which will be responsible for monitoring and enforcing the compliance of high-risk AI systems on the market, as well as cooperating with other authorities and the Commission.

Ireland must ensure that its NCAs have adequate technical, financial, and human resources, and infrastructure to fulfil their tasks effectively under the AI Act. They must have enough qualified personnel with in-depth knowledge of AI technologies, data and data computing, personal data protection, cybersecurity, fundamental rights, health and safety risks, and existing standards and legal requirements. Ireland will be obliged assess and update their NCAs competence and resource requirements annually. Ireland must designate, and notify the Commission of, a MSA which will be Ireland’s single point of contact for the AI Act.

NCAs may provide guidance and advice on the implementation of the AI Act, particularly to SMEs, including startups. If the advice relates to areas covered by EU law, the NCAs under the relevant EU law must be consulted.



Fines

The AI Act provides for significant fines for infringements.

- i. Breach of provisions relating to prohibited AI will see fines of up to the greater of €35 million or 7% annual global turnover.
- ii. Fines for breach of other provisions will see fines of up to the greater of €15 million or 3% of annual global turnover.

As discussed above, fines for infringement of the AI Act by SMEs will take into account the interests of the SME including their economic viability and where fines are applied to SMEs, it will be up to the lower of percentages or the amounts referred to above.

Liability

The AI Act is part of the Commission's three-pronged legal approach to regulating AI. In addition to the AI Act, the following directives have been proposed:

- a. AI Liability Directive² – sets down procedural rules for civil claims concerning AI; and
- b. Product Liability Directive³ – addresses harm caused by defective AI systems and provide for compensation.

Timeframe for Implementation

The provisions of the AI Act are expected to begin to apply from 1 August 2026 with certain exceptions:

- 1 November 2024 – National public authority protecting fundamental rights must be identified and notified to the Commission.
- 1 February 2025 – Provisions on scope, definitions and prohibited AI systems apply.
- 1 August 2025 – Provisions on GPAI, penalties and EU governance apply.
- 1 August 2027 – Provisions on safety components / specific products considered high risk per Annex I apply.

This document is intended to provide an overview of the AI Act.

This document does not purport to be comprehensive or to render legal advice.

² Progress on this Directive has stalled - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496>

³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495>

Contacts

For further information on our services, please contact:



Claire Morrissey
Partner and Group Head
+353 1 619 2113
claire.morrissey@maples.com



Stephen Carty
Partner
+353 1 619 2023
stephen.carty@maples.com



Lorna Smith
Partner
+353 1 619 2125
lorna.smith@maples.com



Philip Keegan
Partner
+353 1 619 2122
philip.keegan@maples.com



Colm Rafferty
Partner
+353 1 619 2058
colm.rafferty@maples.com

