

Legal 500

Country Comparative Guides 2026

Ireland

Artificial Intelligence

Contributor

Maples Group



Claire Morrissey

Partner and head of Data, Commercial and Technology |
claire.morrissey@maples.com

Sarah Lydon

Data, Commercial and Technology Associate | sarah.lydon@maples.com

This country-specific Q&A provides an overview of artificial intelligence laws and regulations applicable in Ireland.

For a full list of jurisdictional Q&As visit legal500.com/guides

Ireland: Artificial Intelligence

1. What is the legal definition of "artificial intelligence" in your jurisdiction, if any? If no definition exists, how do regulators or courts typically describe artificial intelligence?

Ireland has no standalone domestic AI definition.

The Regulation of Artificial Intelligence Bill 2026 (the "AI Bill"), expected to be enacted in mid-July 2026, does not introduce an independent Irish AI definition but relies on the EU AI Act definition of an "AI system". S.I. No. 366/2025 European Union (Artificial Intelligence) (Designation) Regulations 2025 ("Designation Regulations") also incorporates the EU AI Act definitions by reference. The EU AI Act applies directly in Ireland, so its definition of an "AI system" – broadly, a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness, and that infers from inputs to generate outputs such as predictions, content, recommendations, or decisions – is the operative definition in Irish law.

The Department of Public Expenditure, Infrastructure, Public Service Reform and Digitalisation "Guidelines for the Responsible Use of Artificial Intelligence in the Public Service" (the "Public Service AI Guidelines") refer to the EU AI Act definition while noting that AI definitions remain debated.

The Data Protection Commission ("DPC") does not adopt a formal definition of AI but describes its functionality – particularly generative AI chatbots powered by Large Language Models that use Natural Language Processing "to learn and mimic how human speech is naturally used," trained on publicly accessible internet data.

The Central Bank of Ireland ("CBI") describes AI as the concept of creating computer systems able to perform tasks that would normally require human intelligence.

The Courts Service defines AI practically as "computer systems that can perform tasks that normally require human intelligence" with generative AI being "a type of AI that can create new content, such as text, images, audio or video."

2. Has your country developed a national

strategy for artificial intelligence? If yes, what progress has been made in its implementation? Are there plans for updates or revisions?

Ireland has developed and updated a national AI strategy on multiple occasions.

Original National AI Strategy (2021)

Ireland launched "AI – Here for Good: A National Artificial Intelligence Strategy for Ireland" in July 2021, a whole-of-government roadmap to make Ireland an international leader in AI, grounded in a people-centred and ethical approach.

Implementation Progress

A formal progress report was published in 2023, documenting implementation activity under the strategy's various strands. Reported milestones included:

- Appointment of Ireland's AI Ambassador.
- Establishment of the Enterprise Digital Advisory Forum.
- Designation of CeADAR as the National AI Hub, allowing it to act as a one-stop-shop for businesses starting their AI journey.
- Publication of the Expert Group on Future Skills AI Skills report.
- Delivery of the National Youth Assembly on AI in October 2022.

2024 AI Strategy Refresh

Ireland issued a **National AI Strategy Refresh 2024**, prompted by the rapid emergence of generative AI following ChatGPT's 2022 launch and the EU AI Act's publication in 2024. The refresh sharpened priorities around balancing innovation with proportionate regulation, including leadership in EU AI Act implementation, participation in the EU AI Board, and rollout of AI standards and certification.

National Digital & AI Strategy 2030 (February 2026)

In February 2026, Ireland published a National Digital & AI Strategy 2030 (the "Digital & AI Strategy"), entitled "*Digital Ireland – Connecting our People, Securing our Future.*" This supersedes the earlier standalone AI strategy into a wider policy framework running to 2030, aiming to

reinforce Ireland's position as a digital leader and global hub for Applied AI.

The strategy contains **90 deliverables**, including:

- 100% of key public services digitalised by 2030, with 90% consumed online.
- A new AI Advisory Unit for the public service.
- A National AI Fellowship programme for the public sector.
- A GovTech 2026 Challenge.
- Implementation of "Digital for Care 2030" and a new "AI for Care" strategy.

Implementation emphasises central government oversight, regular progress tracking, and reporting to the Cabinet Committee on the Economy, Trade and Competitiveness.

3. Has your jurisdiction adopted any AI-specific laws, regulations, voluntary standards, or ethical guidelines? If so, please provide a brief overview. If not, which existing laws could be/are applied to artificial intelligence and the use of artificial intelligence, what are the main interpretive challenges, and are there any pending artificial intelligence legislative initiatives?

AI Bill and EU AI Act

Ireland has not yet enacted standalone domestic AI legislation, though the AI Bill is progressing through the legislature. As an EU Member State, Ireland is subject to the EU AI Act which establishes a risk-based framework classifying AI systems from unacceptable-risk (prohibited) through high-risk (subject to conformity assessments) to limited and minimal risk categories. The Designation Regulations 2025 designate the Minister for Enterprise, Tourism and Employment as a national competent authority and specify market surveillance authorities for enforcement.

The Workplace Relations Commission ("WRC") has published dedicated guidance on the use of AI tools to prepare material for WRC submissions. The Irish Court of Appeal also addressed the use of AI in litigation in *Guerin v O'Doherty* [2026] IECA 48.

Existing Laws Applied to Artificial Intelligence

Beyond the EU AI Act, several existing laws apply to AI systems. The GDPR and Data Protection Act 2018 govern personal data processing in AI contexts. The DPC has been particularly active, commencing a cross-border

inquiry into Google Ireland regarding use of EU/EEA personal data for training its PaLM 2 AI model and engaging with Meta on proposed use of public social media content for LLM training. It has published guidance titled "AI, Large Language Models and Data Protection" (the "DPC AI Guidance") and welcomed the EDPB's December 2024 opinion on personal data use in AI model development.

Other applicable frameworks include the Employment Equality Acts 1998–2015 (the "Employment Equality Acts") and Equal Status Acts 2000–2018 (the "Equal Status Acts") (addressing discrimination), the Copyright and Related Rights Act 2000 (the "CRRA") (relevant to AI-generated content and training data), the Liability for Defective Products Act 1991 (product liability for AI-embedded products), tort law and consumer protection legislation enforced by the Competition and Consumer Protection Commission ("CCPC").

Main Interpretive Challenges

Key interpretive challenges include satisfying GDPR transparency and explainability requirements for opaque models such as deep neural networks; allocating legal responsibility across the AI value chain from developers to end users; managing regulatory overlap between the EU AI Act and pre-existing sectoral regulation; and keeping pace with rapid technological development.

Voluntary Standards and Ethical Guidelines

The Digital & AI Strategy sets out a national vision for digital transformation and AI adoption. The Digital Regulators Group – comprising the CCPC, Coimisiún na Meán, the DPC, and ComReg – supports coordinated regulatory oversight.

The Public Service AI Guidelines set out seven principles for responsible AI with practical tools including a Decision Framework, Responsible AI Canvas Tool, and AI Lifecycle Guidance Tool. The NCSC has published "Securing AI Adoption in the Public Sector" (the "NCSC AI Guidelines") as the cyber security companion.

Both the Courts Service and the WRC have published guidance on AI tools for preparing submissions, emphasising that AI is not legal advice, parties remain responsible for accuracy regardless of AI assistance, and users must protect confidential information. The Court of Appeal's decision in *Guerin v O'Doherty* [2026] IECA 48 further underscores judicial engagement with AI in litigation.

Internationally, Ireland is party to the Bletchley Declaration (November 2023) and the Paris AI Action

Summit Statement (February 2025). The DPC has also signed a joint declaration with counterparts from Australia, Korea, France, and the United Kingdom on privacy-protective AI governance frameworks.

4. Are there legal requirements for artificial intelligence transparency, explainability, or audits? Are there obligations to disclose the use of artificial intelligence to customers/clients?

There is no standalone domestic Irish AI transparency statute. The EU AI Act imposes graduated transparency, explainability, and disclosure obligations depending on risk classification – including informing individuals of AI interactions, marking synthetic content, disclosing use of high-risk AI in decision-making, and providing meaningful explanations to affected individuals. The GDPR separately requires transparency about automated decision-making (Articles 13 and 14), gives individuals rights under Article 22, and requires DPIAs for high-risk processing (Article 35). The DPC has applied these requirements, commencing an inquiry into whether Google Ireland was required to undertake a DPIA for its PaLM 2 AI model.

As regards audits, the EU AI Act's conformity assessment, notified body, and market surveillance authority regimes apply in Ireland as in all Member States. The AI Bill expands these regulatory audit powers domestically, empowering authorised officers to enter and inspect premises, require records, and acquire product samples – including under cover – and enabling a fundamental rights authority to request that a market surveillance authority organise technical testing of a high-risk AI system.

In financial services, the Central Bank of Ireland has highlighted AI as a consumer protection and market conduct issue, with supervisory focus on fairness, explainability, governance, and trust in AI-driven processes. The Public Service AI Guidelines advise that end users be notified when interacting with an AI system. Beyond these specific obligations, there is no general requirement to disclose AI use to all customers in all contexts, though consumer protection law may require disclosure where failure to inform a customer would amount to a misleading commercial practice.

5. Are there legal requirements or best practice expectations for human oversight and human-in-the-loop in artificial intelligence systems?

There is no standalone domestic Irish statute on human

oversight or human-in-the-loop requirements. The EU AI Act requires high-risk AI systems to be designed for effective human oversight, enabling assigned individuals to understand the system's capabilities and limitations, monitor operation, and intervene where necessary. The GDPR requires that where solely automated decision-making with legal or similarly significant effects is permitted, data controllers must implement suitable safeguards, including human intervention, the right to express a point of view, and the right to contest decisions (Article 22).

The Public Service AI Guidelines require public sector bodies to maintain human oversight when deploying AI, with principles including accountability and governance requirements supporting meaningful human control. The NCSC AI Guidelines reiterate human oversight as a key principle.

6. Are there specific legal or regulatory requirements addressing algorithmic bias, discrimination, or fairness in AI systems (including gender bias)?

There is no Irish statute that specifically addresses algorithmic bias, discrimination, or fairness in AI systems. However, obligations arise under a combination of EU and domestic law.

The EU AI Act addresses bias through its risk-based framework. Certain AI practices exploiting vulnerabilities or manipulating individuals are prohibited outright. High-risk AI systems – including those used in employment, credit, insurance, education, and public services – must be designed to minimise risks of biased outputs, with appropriate data governance practices for training datasets. The government has appointed nine fundamental rights bodies to ensure AI systems respect fundamental rights.

Under Irish equality legislation, the Employment Equality Acts prohibit discrimination in employment on nine protected grounds, and the Equal Status Acts extend similar protections to goods, services, accommodation, and education. Neither Act refers to AI, but both cover discrimination regardless of whether caused by human or automated decision-making. Where an AI system produces outcomes that disproportionately disadvantage individuals on a protected ground, an indirect discrimination claim could arise.

The Public Service AI Guidelines advise public sector bodies to undertake bias detection and implement mitigation strategies where required.

7. What legal frameworks apply to AI-related harm and defective artificial intelligence systems? Who can be held liable (developer, deployer, victim of the damage, others), how is liability allocated, and what burden of proof applies to victims?

There is no AI-specific liability statute in Ireland. Claims arising from AI-related harm are governed by a combination of existing product liability legislation, the common law of negligence and contract, and forthcoming EU reforms that will significantly reshape the landscape.

Product liability

The Liability for Defective Products Act 1991, transposing the original EU Product Liability Directive (85/374/EEC), establishes strict liability under which a producer is liable for damage caused by a defect without the injured party proving fault. The injured party must prove the damage, defect, and causal relationship. However, whether standalone AI software qualifies as a “product” under the 1991 Act is debatable and unresolved.

Under the 1991 Act, the producer (manufacturer) is the primary liable party. Importers into the EU and suppliers who fail to identify the producer may also be liable.

The revised EU Product Liability Directive (Directive (EU) 2024/2853) must be transposed into Irish law by 8 December 2026. The revised Directive makes three AI-relevant changes:

- explicitly includes software (and within that AI systems) and digital manufacturing files within the definition of “product”;
- broadens the range of economic operators potentially liable to include authorised representatives, providers of a related service, fulfilment service providers, parties making substantial modifications to products and online platform providers. It extends liability to defects emerging after placing on the market where a product remains under the economic operator's control and it relates to software, including updates or lack thereof, a related service or a substantial modification; and
- eases the burden of proof for claimants by introducing rebuttable presumptions of defectiveness and causation in defined circumstances, including where technical complexity would otherwise prevent proof. Heads of damage are also expanded to cover psychological harm and data.

Negligence and contract

Alongside the statutory regime, the common law of negligence provides a basis for claims against any party in the AI value chain who owed a duty of care and whose breach caused harm. The burden of proof lies on the claimant to establish duty, breach, causation, and damage on the balance of probabilities. Contractual claims may also arise under the terms of supply, licensing, or service agreements governing the AI system, where the claimant must prove, again on the balance of probabilities, that a term of the contract was breached and that the breach caused the loss claimed.

Data Protection

Defects in AI systems may result in breaches of the GDPR which may lead to regulatory fines and/or claims from data subjects.

Equality

Where an AI system generates outcomes that are discriminatory in nature, individuals may take a claim under the Employment Equality Acts or Equal Status Acts (see Q6 for further detail on algorithmic bias and discrimination).

AI Liability Directive

The European Commission's proposed AI Liability Directive, which would have introduced specific rules on the burden of proof in AI-related damage claims, was formally withdrawn in October 2025 due to the absence of a foreseeable agreement among the EU institutions.

8. What cybersecurity obligations apply to AI systems?

There is no standalone Irish statute imposing cybersecurity obligations specific to AI systems. Obligations arise from a combination of directly applicable EU regulations, EU directives requiring transposition, and domestic guidance.

The EU AI Act requires that high-risk AI systems be designed and developed to achieve an appropriate level of accuracy, robustness, and cybersecurity, and to perform consistently in those respects throughout their lifecycle. The Digital Omnibus on AI, which received final Council approval on 29 June 2026, defers the application date for high-risk AI obligations – including these cybersecurity requirements – from 2 August 2026 to a later date linked to the availability of harmonised standards, with a longstop of 2 December 2027 for Annex

III systems and 2 August 2028 for Annex I systems embedded in regulated products. The AI Act's cybersecurity requirements interact with several other EU cybersecurity instruments.

High-risk AI systems certified under a cybersecurity scheme pursuant to the Cybersecurity Act (Regulation (EU) 2019/881) are presumed to comply with the AI Act's cybersecurity requirements insofar as the certificate covers those requirements. Similarly, the Cyber Resilience Act (Regulation (EU) 2024/2847) sets cybersecurity-by-design requirements for products with digital elements; where AI systems fall within its scope, compliance with its essential cybersecurity requirements may also demonstrate compliance with the AI Act.

The NIS2 Directive (Directive (EU) 2022/2555) imposes cybersecurity risk management and incident reporting obligations on essential and important entities across 18 critical sectors, including healthcare, energy, transport, and finance. AI developers and deployers operating in these sectors may need to align their cybersecurity practices with NIS2, particularly where their AI systems qualify as high-risk or support critical infrastructure. Ireland has not yet transposed NIS2 into national law – the transposition deadline of 17 October 2024 was missed, and the European Commission has referred Ireland to the CJEU for failure to transpose. The National Cyber Security Bill, which is the proposed transposition vehicle, remains at legislative scrutiny stage. In the interim, the NCSC has published draft Risk Management Measures guidance and launched Ireland's participation in the CyberFundamentals (CyFun) framework to help in-scope entities prepare for compliance.

In financial services, the Digital Operational Resilience Act ("DORA") imposes specific cybersecurity and ICT risk management obligations on financial entities, including requirements to assess third-party ICT service providers such as AI providers.

9. Is the use of artificial intelligence insured and/or insurable in your jurisdiction, including with cyber policies? Are there market trends, or limitations?

Existing insurance policies may respond to AI-related losses even without explicit AI wording, though coverage depends on specific policy terms and gaps remain. Relevant lines include cyber liability (digital threats, privacy breaches), technology errors and omissions (algorithmic bias, system failures), product liability (defective or malfunctioning AI), intellectual property (copyright or trademark issues), employment practices

liability (discriminatory AI decisions), media liability (defamatory AI-generated content), property/business interruption and workers' compensation policies, and sector-specific covers such as medical malpractice for healthcare AI errors.

Chubb, active in the Irish market, has flagged the "silent AI risk," describing AI as a "multiplier" across existing perils-cyber, crime, Tech E&O/PI, media, D&O and general liability-rather than a standalone risk category. A single AI-related event can therefore trigger multiple policies at once, raising questions of coverage clarity, programme design, and governance accountability. Internationally, some insurers have moved beyond silent coverage to dedicated AI products: Munich Re's aiSure™, for instance, offers cover for AI performance errors, spanning contractual liabilities, third-party damages, financial losses, and legal liabilities, for both AI developers and corporate deployers.

10. Can artificial intelligence be named as an inventor in a patent application filed in your jurisdiction? If not, what is the current legal position?

Section 2 of the Patents Act 1992 defines "inventor" as "the actual deviser of an invention". While the Act does not expressly state that the inventor must be a natural person, the concept of "devising" presupposes a human act of conception. There is no Irish court or Patent Office decision holding that a machine or AI system can be classified as an inventor under the Act.

Ireland is a party to the European Patent Convention, and EPO jurisprudence is persuasive. The EPO Guidelines for Examination state that an inventor must be a natural person and that it will verify this. The EPO Technical Board of Appeal in T 0528/25 (5 February 2026) confirmed that AI-assisted inventions remain patentable, but a human being must be named as the inventor.

11. Do images or works generated by and/or with artificial intelligence benefit from copyright protection in your jurisdiction? If so, who is the authorship attributed to, and under what conditions?

Yes. Under section 21 of the CRRA, the author of a computer-generated work is deemed to be "the person by whom the arrangements necessary for the creation of the work are undertaken". Authorship is not attributed to the AI system itself, but to the natural or legal person who

made the necessary arrangements for the work's creation – which could, depending on the facts, be the user who prompted the AI, the developer of the AI system, the platform operator, or an employer. The general rule under section 23 of the CRRA is that the author is the first owner of the copyright, subject to statutory exceptions such as works created in the course of employment.

The key condition for copyright protection is that the work must be "original" within the meaning of the CRRA. The question of what level of human creative input is required for a computer-generated work to qualify as original has not been tested in the Irish courts and remains an open interpretive issue – particularly in the context of modern generative AI systems where the human contribution may be limited to a brief text prompt.

A further practical difficulty is identifying, on the facts, who undertook the "arrangements necessary" for the creation of a particular AI-generated work. Section 21 provides the attribution formula, but its application to complex AI workflows – where multiple parties may contribute at different stages of development, training, and deployment – is untested and may give rise to disputes.

12. What are the main issues to consider when using artificial intelligence systems in the workplace? Have any new regulations, or guidelines, been introduced regarding AI-driven hiring, performance assessment, or employee monitoring?

The main issues Irish employers should consider when deploying AI in the workplace arise under three overlapping legal frameworks: the GDPR, the Employment Equality Acts, and the EU AI Act. Each of these frameworks is discussed elsewhere in this guide (see Q4 for transparency and human oversight, Q6 for bias and discrimination, and Q13 for data protection), and specific employment-related considerations are set out below.

1. Human Oversight of Significant Decisions

Employees have the right not to be subject to a decision based solely on automated processing where it produces legal effects or similarly significantly affects them. This directly applies to AI tools used for CV screening, candidate shortlisting, interview assessment, performance scoring, promotion decisions, and termination. Meaningful human review must be embedded before any consequential employment decision is taken.

2. Transparency and Explainability

Employers must provide information about the logic underpinning any automated process and the consequences of decisions arrived at through automated means (see Q4 for the underlying transparency obligations). This obligation is reinforced by the Employment Equality Acts: once a *prima facie* discrimination case is established, the burden of proof shifts to the employer. AI systems that cannot explain their outputs make it very difficult to discharge that burden.

3. Discrimination and Bias

The Employment Equality Acts prohibit discrimination on nine protected grounds (gender, civil status, family status, sexual orientation, religion, age, disability, race, and Traveller community membership) in recruitment, employment conditions, promotion, and dismissal – whether the decision is made by a human or an algorithm (see Q6 for further detail on bias and discrimination). AI tools trained on historical data risk embedding or amplifying existing biases, exposing employers to indirect discrimination claims. Automated assessment tools such as video interview analysis may also disadvantage candidates with disabilities, engaging the duty of reasonable accommodation. Use of a third-party AI vendor does not relieve the employer of liability before the WRC.

4. Proportionality and Purpose Limitation in Monitoring

AI-enabled monitoring can give rise to concerns of unreasonable intrusion and excessive surveillance. Employers must define a clear, lawful purpose for any AI monitoring, consider less intrusive alternatives, and bring monitoring policies to employees' attention.

5. Risk Assessment and Documentation

Employers should conduct bias audits and DPIAs before deployment and maintain documentation sufficient to demonstrate compliance and defend any equality or data protection complaint.

6. EU AI Act – High-Risk Employment Categories

Ireland has not yet introduced any new regulations regarding AI-driven hiring, performance assessment or employee monitoring but the EU AI Act introduced specific provisions addressing AI in the workplace. It prohibits:

- AI systems that infer emotions of an individual

in the workplace unless this is for medical or safety reasons; and

- biometric categorisation systems that categorise individuals based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation.

It also classifies the following employment-related AI uses as **high-risk**:

- **Recruitment and selection**– AI used for placing targeted job advertisements, screening or filtering applications, and evaluating candidates in interviews or tests.
- **Decisions affecting terms of employment**– AI used for promotion, termination, task allocation based on individual behaviour or personal characteristics, and contract decisions.
- **Performance and behaviour monitoring**– AI used to monitor and evaluate worker performance and conduct.

These high-risk systems will be subject to conformity assessments, transparency and information obligations, human oversight requirements, data governance standards, and record-keeping duties as the relevant provisions phase in. The DPC has been actively engaging with the EDPB on the use of personal data in AI to gain European-wide regulatory clarity, and its 2025 Annual Report noted a 45% increase in complaints, many involving the use of AI by complainants.

Irish employers should treat these converging frameworks as a single compliance agenda: ensuring lawful processing, meaningful human oversight, transparency, non-discrimination, proportionality, and thorough documentation across all AI-driven employment tools.

13. What are the main privacy/data protection issues arising from artificial intelligence development and use (including training data)? Have data protection authorities issued guidelines or rulings on artificial intelligence, and what are the key takeaways?

Key Privacy and Data Protection Issues

The development and use of AI raise several issues under the GDPR. The EU AI Act's transparency, human oversight, and conformity assessment obligations are

addressed in Q4 and Q5; the discussion below focuses on data protection considerations specific to AI development and deployment.

- **Lawful basis for processing:** AI systems often require large datasets that include personal data. Organisations must identify and document an appropriate lawful basis (e.g. legitimate interests, contractual necessity), which is particularly challenging when existing data is repurposed for AI training.
- **Transparency and explainability:** The GDPR requires that data subjects are informed about how their data is used, including, where automated decision-making is involved, the logic underpinning the process and any consequences of decisions reached through automated means. The complexity of AI models – particularly generative models – can make it difficult to provide clear explanations, hindering compliance with Articles 13 and 14 of the GDPR.
- **Data minimisation and purpose limitation:** Only data necessary for a specific, explicit purpose should be collected and processed. AI development carries a risk of collecting excessive data or using it beyond the original intent, breaching these principles.
- **Data subject rights:** The GDPR grants individuals rights of access, rectification, erasure, restriction, and portability. Fulfilling these rights can be challenging where personal data is embedded in training data or where outputs make it difficult to trace or delete specific data points.
- **Automated decision-making and profiling:** Article 22 of the GDPR gives individuals the right not to be subject to decisions based solely on automated processing, including profiling, which significantly affects them. AI systems that make or inform such decisions in a fully automated way raise concerns about fairness, bias, and contestability.
- **Data security and anonymisation risks:** AI systems can be vulnerable to data breaches, model inversion attacks, or unintended data leakage – particularly where generative models reproduce personal data from training sets. While anonymisation is a common mitigation strategy, AI models can sometimes “memorise” and regenerate personal data, undermining anonymisation efforts and creating re-identification risks.
- **International data transfers:** AI development

often involves cross-border data flows. The GDPR imposes strict requirements on transferring personal data outside the European Economic Area ("EEA"), and compliance can be complex when using cloud-based AI services or collaborating with international partners.

Regulatory Guidance

The DPC has not issued formal binding guidelines on AI but has been increasingly active in this area. In July 2024, the DPC published the DPC AI Guidance, setting out key considerations for organisations. These include: assessing whether new AI processing falls within the scope of an existing lawful basis; conducting DPIAs; meeting the principle of storage limitation; addressing risks of inaccurate or biased outputs relied upon without human intervention; securing personal data held by third parties; complying with data subject rights; and maintaining appropriate data governance, design, and decision-making controls.

In September 2024, the DPC requested a formal opinion from the European Data Protection Board ("EDPB") under Article 64(2) GDPR to achieve Europe-wide regulatory clarity on AI. EDPB Opinion 28/2024 is indicative of the approach European supervisory authorities, including the DPC, are likely to take. The key points are:

- **Anonymity of AI models:** An AI model will only be considered anonymous after a thorough evaluation concluding that the likelihood of extracting personal data is insignificant. Adequate documentation of processing operations at both development and deployment stages is required to ensure accountability under the GDPR.
- **Legitimate interests:** Legitimate interest may serve as a lawful basis for AI model development and deployment, provided three cumulative conditions are met: (i) the controller or a third party pursues a legitimate interest; (ii) the processing is necessary to pursue that interest; and (iii) the interest is not overridden by the data subjects' fundamental rights and freedoms. Less intrusive alternatives should be considered, and mitigating measures adopted to address any negative impacts.
- **Consequences of unlawful processing:** Unlawful processing at the development stage can affect the lawfulness of subsequent processing. Where separate controllers are involved at different stages, each controller's

due diligence will be assessed. However, where an AI model is effectively anonymised, the GDPR will not apply to subsequent processing.

DPC Enforcement Actions

- **X / Grok:** In August 2024, the DPC brought urgent High Court proceedings under section 134 of the Data Protection Act 2018 after X processed personal data from public posts of EU/EEA users to train Grok. X agreed to suspend the relevant processing, and the proceedings were struck out in September 2024. In April 2025, the DPC commenced a formal inquiry into X's use of publicly accessible EU/EEA user posts to train Grok, examining compliance with GDPR requirements including lawfulness and transparency. In February 2026, the DPC opened a further inquiry concerning the apparent creation and publication on X of potentially harmful, non-consensual intimate and/or sexualised images using Grok, examining compliance with Articles 5, 6, 25, and 35 of the GDPR.
- **Meta:** Meta notified the DPC in March 2024 of plans to train its LLM using public content shared by adults on Facebook and Instagram across the EU/EEA. Following DPC intervention, Meta paused training in June 2024. After the EDPB opinion and further engagement, Meta implemented significant improvements – including updated transparency notices, an easier objection process, de-identification measures, and output filters – before resuming training.
- **LinkedIn:** In March 2025, LinkedIn informed the DPC of plans to train generative AI models using EU/EEA members' personal data. Following DPC review, LinkedIn improved its transparency notices, narrowed the scope of personal data processed, strengthened user protections including improving measures to exclude under-18 users' data, and provided more detailed legitimate interest assessments and DPIAs.

14. How is data scraping regulated in your jurisdiction from an IP, privacy and competition perspective? Are there recent precedents addressing the legality of data scraping for

training of artificial intelligence systems?

IP

The European Union (Copyright and Related Rights in the Digital Single Market) Regulations 2021 (S.I. No. 567/2021) transposed the EU DSM Directive into Irish law, providing copyright exemptions for text and data mining ("TDM"). Under these provisions, research organisations and cultural heritage institutions may carry out TDM for scientific research purposes, provided they have lawful access to the works. A broader exemption permits TDM by any person with lawful access, but rightholders may expressly reserve their rights, in which case the exemption does not apply.

The EU AI Act requires providers of general-purpose AI (GPAI) models to comply with EU copyright law, including authors' reservations of rights, and to draw up and make publicly available a sufficiently detailed summary of the content used for training, in accordance with a template provided by the AI Office.

A pending case before the Court of Justice of the European Union, *Like Company v Google Ireland* (C-250/25), will examine the legality of Google scraping copyrighted articles to train its Gemini AI system, which reportedly produced wording closely resembling the original published content. The Advocate General's opinion is anticipated in September 2026 and the case is expected to be a significant development in the treatment of scraping for AI training from an IP perspective.

Data Protection

Where scraped data includes personal data, the full suite of GDPR obligations applies, including the requirement to have a lawful basis for processing and compliance with principles of transparency, purpose limitation, data minimisation, accuracy, and storage limitation.

As noted above, the DPC has taken a particularly active role in this area (see Q13 for details of DPC enforcement actions regarding AI training data), including launching an inquiry into X scraping users' publicly accessible posts to train its Grok AI system and engaging with Meta and LinkedIn on their use of scraped user data.

Competition

The Irish Competition Act 2002 (as amended) and Articles 101-106 TFEU apply to such activities.

15. To what extent is the prohibition of data

scraping in the terms of use of a website enforceable?

In order for prohibitions on data scraping contained in website terms to be enforceable in Ireland, the prohibition must be clear and form part of legally binding terms entered into between the parties which were accepted by the user including via a click-wrap or browse-wrap mechanism. This has been reflected at an EU level and also at a national level in a series of cases taken by Ryanair (*Ryanair Ltd v Bravofly* and *Travelfusion Ltd, Ryanair Ltd v Billigfluege* and *Ryanair Ltd v SC Vola.Ro Srl*) in which the Irish High Court enforced provisions of the Ryanair website terms prohibiting data scraping of their website.

16. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence? What are its powers and enforcement tools?

Ireland does not yet have a single dedicated AI regulator, but the regulatory architecture is taking shape through the AI Bill, which proposes to establish the AI Office of Ireland as an independent statutory body serving as Ireland's single point of contact under the EU AI Act. The AI Office will facilitate consistent enforcement of the Act, enable cooperation between competent authorities, promote technical expertise, and advance AI innovation and AI literacy.

Competent Authorities

The Irish government has appointed fifteen public authorities as competent authorities (either market surveillance authorities or notifying authorities) responsible for the implementation and enforcement of the EU AI Act within their respective sectors. These include the Central Bank of Ireland, Coimisiún na Meán, the Commission for Communications Regulation, the Commission for Railway Regulation, the Commission for Regulation of Utilities, the Competition and Consumer Protection Commission, the Data Protection Commission, the Health and Safety Authority, the Health Products Regulatory Authority, the Health Services Executive, the Marine Survey Office of the Department of Transport, the Minister for Enterprise, Tourism and Employment, the Minister for Transport, the National Transport Authority, and the Workplace Relations Commission.

The enforcement powers available to each competent authority under the EU AI Act and the AI Bill will differ depending on whether the authority is designated as a

market surveillance authority or a notifying authority. Market surveillance authorities will have broader investigative and enforcement powers, including the ability to assess AI systems for compliance, require corrective action, and impose penalties.

Fundamental Rights Authorities

The Irish government has also appointed nine fundamental rights authorities to supervise and enforce EU laws on the protection of fundamental rights in the context of AI. These are An Coimisiún Toghcháin, Coimisiún na Meán, the Data Protection Commission, the Environmental Protection Authority, the Financial Services and Pensions Ombudsman, the Irish Human Rights and Equality Commission, the Ombudsman, the Ombudsman for Children's Office, and the Ombudsman for the Defence Forces.

Fundamental rights authorities have the power to request and access documentation created or maintained under the Act where necessary for the exercise of their mandates. They may also raise concerns to a market surveillance authority, which must then take steps to assess the AI system in question.

17. How widespread is the adoption of artificial intelligence in businesses in your jurisdiction, and which sectors are leading?

AI adoption in Ireland is growing steadily. According to the Irish Central Statistics Office in February 2026, 20.2% of all enterprises indicated the use of AI in some capacity in 2025. There is a significant gap by enterprise size: 57.7% of large enterprises used AI, compared with 28.6% of medium-sized and 17.2% of small-sized enterprises. Data mining was identified as the most common use, followed by natural language generation and automation of workflows.

The AI Economy in Ireland AI Adoption Index 2026 report by Trinity College Dublin in association with Microsoft Ireland found that 43% of private sector organisations report AI tools in active use, compared with 36% in the public sector. The report further states that over 80% of employees use AI tools quite frequently (more than once a month).

In terms of sectoral adoption, the technology, science, and media sectors have seen the most rapid uptake, according to a 2024 report by Trinity College Dublin and Microsoft Ireland. AI has also been increasingly adopted in manufacturing (for process automation, predictive maintenance, and production optimisation), financial

services (for fraud detection, anti-money laundering, risk management, and customer analytics), and the retail and marketing sector (for customer insights, personalised marketing, and sales optimisation).

18. How is artificial intelligence used in the legal sector, by lawyers and/or in-house counsels? Are AI-driven legal tools widely adopted, and what are the main regulatory concerns?

AI adoption in the Irish legal sector has grown significantly in recent years, with generative AI and AI-powered assistants now in widespread use. According to the Clio UK & Ireland Legal Insights Report 2026, 89% of legal professionals use AI tools. The most common categories are generic non-legal AI tools (59%), document drafting or automation tools (46%), and legal research platforms (44%). However, adoption remains uneven: only 27% of law firms have embedded AI widely across the firm.

Main Regulatory Concerns

Beyond the broader data protection and EU AI Act issues discussed elsewhere in this guide (see Q3, Q4, and Q13), the legal profession faces several profession-specific regulatory concerns.

- **Confidentiality, privilege, and data protection:** Submitting client information to AI tools risks breaching confidentiality obligations and may constitute voluntary disclosure of privileged material to a third party, potentially waiving legal professional privilege. Law firms are also data controllers under the GDPR, and the sensitivity of legal data – which may include special category data – heightens the need for appropriate lawful bases, DPIAs, and data processing agreements with AI vendors.
- **Accuracy and supervision:** AI tools can generate fabricated outputs, including non-existent case law. Solicitors remain professionally responsible for all work product regardless of AI assistance, and reliance on unverified AI output could breach the duty of competence and the duty not to mislead the court.
- **Bias and liability:** AI tools used in case assessment or risk scoring may embed training data biases, raising equality law and professional ethics concerns. Professional indemnity coverage disputes may also arise where incorrect AI output causes client loss and the firm's AI governance is considered

inadequate.

The Law Society of Ireland has published non-binding "Guidelines for the Use of Generative Artificial Intelligence by the Legal Profession in Ireland". As the EU AI Act takes effect alongside GDPR and professional conduct obligations, firms face the challenge of navigating multiple evolving frameworks without a single consolidated regulatory position on AI in legal practice.

19. What are the 5 key challenges and the 5 key opportunities raised by artificial intelligence for lawyers in your jurisdiction?

Key Challenges:

1. **Confidentiality and privilege risk:** Submitting client information to AI tools creates a risk that confidential data may be used to train models or reproduced in outputs, potentially breaching solicitors' confidentiality obligations. Inputting privileged material into third-party platforms also raises a risk of waiver of legal professional privilege, as it may be treated as voluntary disclosure to a third party.
2. **Accuracy and professional liability:** AI tools can generate fabricated outputs, including non-existent case law, legislation, or precedent. Solicitors remain professionally responsible for all work product and reliance on unverified AI output could breach the duty of competence and the duty not to mislead the court. Professional indemnity coverage disputes may also arise where AI-generated errors cause client loss.
3. **Regulatory complexity:** Irish lawyers must navigate multiple overlapping frameworks – the GDPR, the EU AI Act, professional conduct rules, and the Employment Equality Acts – when advising clients on AI or deploying AI tools in their own practices. The regulatory landscape is evolving rapidly, with key obligations phasing in across 2026–2028, and no single consolidated regulatory position.
4. **Bias and ethical concerns:** AI tools used in legal analysis, case assessment, or risk scoring may embed biases from training data, potentially leading to unfair outcomes. This engages both equality law concerns and professional ethics obligations, requiring lawyers to exercise critical judgment over AI outputs rather than treating them as authoritative.
5. **Skills and adaptation:** Effective use of AI

requires lawyers to develop new competencies in areas such as prompt engineering, AI governance, data protection compliance, and critical evaluation of AI outputs. The pace of technological change creates a risk that practitioners who do not adapt will fall behind, while firms face the challenge of training staff and embedding AI governance frameworks without clear regulatory benchmarks for adequate supervision of AI-assisted work.

Key Opportunities:

1. **Efficiency and productivity:** AI tools can significantly accelerate routine legal tasks – including document review, due diligence, contract analysis, legal research, and first-draft preparation – enabling lawyers to handle larger volumes of work and focus their time on higher-value advisory and strategic tasks.
2. **Access to justice and new service models:** AI-powered tools have the potential to reduce the cost of legal services, making legal advice more accessible to individuals and SMEs who might otherwise be unable to afford representation.
3. **Enhanced legal research and analysis:** AI research platforms can search across large volumes of legislation, case law, and regulatory material far more quickly than manual methods, identifying relevant authorities, patterns, and connections that might otherwise be missed. This can improve the quality and comprehensiveness of legal analysis.
4. **New areas of practice:** The rapid development of AI regulation in Ireland is creating significant demand for specialist legal advice on AI governance, compliance, procurement, and risk management. Lawyers with expertise in AI-related regulatory frameworks are well positioned to advise clients across sectors on conformity assessments, DPIAs, AI policies, and the intersection of AI with data protection, employment, and intellectual property law.
5. **Client relationship and competitive advantage:** Firms that adopt AI effectively can offer faster turnaround times, more competitive pricing, and data-driven insights that enhance the quality of client service.

20. Where do you see the most significant legal developments in artificial intelligence in your

jurisdiction in the next 12 months? Are there any ongoing initiatives that could reshape AI governance?

- **Enactment of the AI Bill and establishment of the AI Office of Ireland:** The AI Bill once enacted will give full domestic effect to the EU AI Act and establish the AI Office of Ireland as an independent statutory body and Ireland's central coordinating authority. The AI Office must be operational by 1 August 2026. It will coordinate enforcement across all fifteen competent authorities, serve as the EU AI Act single point of contact, provide technical expertise to sectoral regulators, and operate the national AI regulatory sandbox.
- **Distributed regulatory model:** Ireland has adopted a distributed model of implementation, confirmed by Government Decisions of 4 March 2025 and 22 July 2025, leveraging existing sectoral regulatory authorities rather than creating a single centralised AI regulator. The fifteen competent authorities and nine fundamental rights authorities will need to develop sector-specific guidance and supervision programmes ahead of the high-risk obligations taking effect.
- **EU AI Act phased implementation:** The Digital Omnibus on AI, which was given final Council approval on 29 June 2026, defers the application date for standalone high-risk AI systems (Annex III) from 2 August 2026 to 2 December 2027 and for high-risk AI embedded in regulated products to 2 August 2028.

However, several obligations will take effect within the next 12 months. Transparency obligations under Article 50 – including informing users that they are interacting with an AI system – apply from 2 August 2026 as originally scheduled. Watermarking obligations for AI-generated content apply from the same date for new systems, with a grace period until 2 December 2026 for systems already on the market. A new prohibition on AI systems used to generate non-consensual intimate imagery or child sexual abuse material takes effect on 2 December 2026.

- **DPC enforcement and guidance on AI:** The DPC's ongoing inquiries into X (concerning the use of publicly accessible posts to train Grok and the generation of non-consensual intimate images) are expected to yield decisions that will set important precedents on the lawfulness and transparency of AI training using personal data. Coimisiún na Meán has also been engaging with the European Commission regarding xAI's Grok and the protection of minors.
- **CJEU ruling in *Like Company v Google Ireland*:** The Advocate General's opinion in Case C-250/25, expected in September 2026, will address the legality of scraping copyrighted content for AI training. A preliminary ruling from the CJEU would have significant implications for the scope of the text and data mining exceptions under the DSM Directive and could reshape how AI developers source training data across the EU.

Contributors

Claire Morrissey

Partner and head of Data, Commercial and Technology

claire.morrissey@maples.com



Sarah Lydon

Data, Commercial and Technology Associate

sarah.lydon@maples.com

