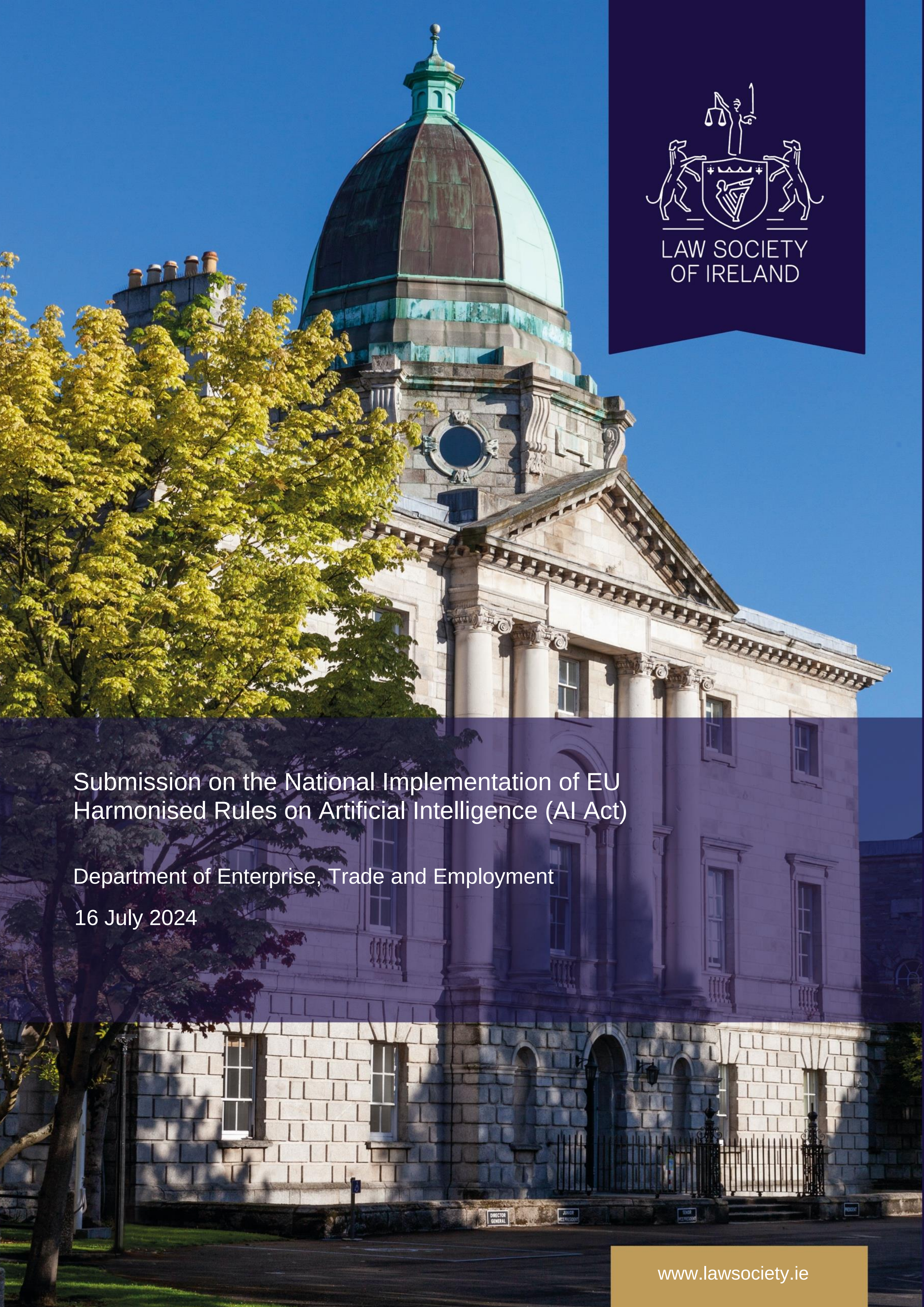

LAW SOCIETY
OF IRELAND

Submission on the National Implementation of EU Harmonised Rules on Artificial Intelligence (AI Act)

Department of Enterprise, Trade and Employment

16 July 2024

www.lawsociety.ie

Submission on the National Implementation of EU Harmonised Rules on Artificial Intelligence (AI Act)

Introduction

The Law Society of Ireland (the **Law Society**) is the educational, representative and regulatory body of the solicitors' profession in Ireland. The Law Society delivers high-quality legal education and training and also places significant emphasis on civic engagement, supporting local community initiatives and driving diversity and inclusion.

The Law Society appreciates the opportunity to provide views on what considerations should be taken into account by the Government when implementing the European Union Harmonised Rules on Artificial Intelligence Act (the **AI Act**) at a national level.

The Law Society is optimistic about the future of AI in Irish society and is particularly interested in the implications of this technology for fundamental rights and the continued development of the legal industry. A survey of members conducted by the Law Society in 2023 found that AI and data protection topped the list of areas that the surveyed legal profession felt were most likely to experience substantial growth. As a prolific educator of solicitors, the Law Society is also particularly interested in how the safe use of AI can be encouraged among the legal profession from an educational standpoint.

A 2023 LexisNexis International Legal Generative AI Report that polled over 8000 respondents (including 3,700 lawyers) in the US, UK, France and Canada noted that 47% of respondents thought that AI tools (specifically generative AI) would have a 'significant or transformative' impact on the legal profession. At the same time, the survey found that almost 90% of lawyer respondents had at least some concerns about the ethical implications of generative AI (with almost a third saying that these implications will be 'significant or fundamental' in nature).

Taking into account the substantial contemporary relevance of AI in society, it is clear that it provides substantial opportunities but also substantial risks. Misuse of AI, either intentional or accidental, can have severe repercussions beyond a mere 'product safety' commercial standpoint: fundamental rights of data privacy or reputation can be at risk if AI is not correctly regulated.

For example, deepfakes can ruin a person's reputation, private sensitive information can be leaked to bad actors by generative AI tools and so on. It is also acknowledged that there are substantial environmental considerations about the use of AI, concerns that must be allayed by effective and robust regulation that nevertheless encourages, rather than stifles, technological innovation.

This public consultation was opened by the Department of Enterprise, Trade and Employment (the **Department**) on 21 May 2024. The initial consultation was divided into four specific questions and this submission aims to address each of these in-turn. The Law Society is available to meet in order to discuss these issues further. It is also willing to provide any further expertise or assistance on the national implementation of the AI Act, particularly in the drafting of any regulations that may arise as a result of this implementation, including via its membership.

Key Takeaways

a) The Law Society recognises that centralised or distributed models of AI regulation have their own distinct advantages and disadvantages. Despite this, centralised and distributed models are not mutually exclusive. Both can be drawn from by the Government in creating an AI regulatory ecosystem. The Government should seek to construct AI regulation that eases the leveraging of EU financial aid and expertise. Extensive cross-border collaboration with EU organisations on AI should be encouraged in both the economy and in Government agencies.

b) When constructing a new national AI regulatory framework, the Government should prioritise:

- Maximising the efficiency of sectoral expertise and encouraging robust stakeholder engagement,
- Ensuring that any national competent authorities are well resourced,
- Facilitating communication and coordination between national competent authorities, and
- Improving access to justice.

c) The Government should be aware of the potential synergies between the AI Act, the General Data Protection Regulation and the Digital Services Act prior to national implementation of the AI Act. In particular, the Data Protection Commission could be well-positioned to adopt an enforcement or co-enforcement role given its expertise and resources.

d) Ireland is very well-resourced to position itself at the forefront of AI provided it takes advantage of regulatory sandboxes and develops AI in an environmentally sustainable manner. There is a possibility for AI to enhance the provision of legal aid provided there is effective human oversight. Support for small and medium enterprises should be prioritised by the Government, including the deployment of targeted supports for these enterprises.

e) Excellence in Irish AI regulation would emphasise:

- Certainty and flexibility,
- Strong support for innovation and development, and
- Environmental and energy sustainability.

f) Finally: under the National AI Strategy, Irish AI regulation should prioritise the public interest by leveraging AI for economic and social benefit alike. The Law Society argues that economic benefit and ethical regulation are not mutually exclusive and that both can be pursued to the benefit of the Irish public. Being highly invested in education, the Law Society suggests that the utility of AI for improving education should be seriously explored by the Government.

Question 1: For national implementation of the Act, different approaches to the designation of competent authorities could be considered, ranging from a centralised model to a more distributed, sector-based approach. Selecting an approach will likely involve trade-offs. For example, a distributed approach may provide better access to sectoral expertise but may pose coordination challenges.

What considerations should the Department have regard to when devising the configuration of national competent authorities for implementation?

Answer:

Background

Article 59 of the EU AI Act allows a Member State to establish or designate a 'national competent authority' or authorities which have the responsibility of overseeing the application and implementation of the AI Act.

Under Article 70, a Member State is required to have at least one notifying authority and at least one market surveillance authority (**MSA**). These authorities, referred to collectively in Article 3 of the Act as 'national competent authorities', have substantially different responsibilities. MSAs are required to enforce the rules in the AI Act, investigate complaints and impose penalties for violations of the Act. Notifying authorities establish and maintain procedures for the assessment, designation of notification of conformity assessment bodies. Notified conformity assessment bodies perform third party conformity assessment activities on AI.

Both MSAs and notifying authorities collectively will be referred to as national competent authorities in this submission.

Generally, these national competent authorities must:

- operate as independent entities and be free of bias,
- have suitable expertise in AI, personal data protection, cybersecurity, fundamental rights, health/safety risks and knowledge of existing standards and legal requirements,
- comply with confidentiality requirements under Article 78,
- be provided with adequate technical, financial and human resources by the Member State.

Although the AI Act gives substantial leeway to Member States on how to approach the national implementation of the Act, Article 70 of the Act does require Member States to designate a MSA as a 'single point of contact.' A Member State must then notify the European Commission of the identity of this single point of contact, which the Commission then adds to a publicly-available list.

The AI Act also establishes the AI Office at EU level. This Office implements and supervises AI systems (and particularly General Purpose AI systems[1]). A separate AI Board will fulfil an advisory role to this AI Office and will be composed of representatives from the Member States.

Centralised and Distributed Approaches

[1] **GPAI**, as defined under Article 3, are AI models trained with a large amount of data that display substantial generality (i.e. are able to perform a wide variety of different tasks).

The Act gives flexibility to Member States as it does not explicitly require them to establish a new regulatory authority dedicated to AI. Ireland could approach the national implementation of the Act in a number of different ways:

A. Ireland could establish or designate a single, centralised national competent authority that would have primary or sole responsibility for the regulation and development of AI. There are already precedents for this approach in both Spain[2] and France,[3] which may serve as useful models if the Government takes this route.
B. Ireland could designate or establish a basket of national competent authorities governing various areas of the economy,[4] with responsibilities corresponding to their existing areas of expertise.[5]
C. Finally, Ireland could take a combined approach of having multiple market surveillance authorities in crucial areas reporting to a centralised authority. Centralised or distributed approaches are not necessarily mutually exclusive.
    - As in example B, the CBI could regulate the use of AI in finance, the Department of Justice could regulate the use of AI in law enforcement, and so on.
    - This would be combined with a central, primary market surveillance/notifying authority that would cooperate with the various market surveillance authorities and (a) enhance their interoperability, (b) engage in training and information sharing and (c) offer a cohesive single point of contact.
    - Ireland may also place responsibility for AI regulation on a body such as the Data Protection Commission (the **DPC**), while leaving an option for the DPC to delegate market supervisory authority where needed to the nearest sector or domain-specific supervisor, as has been recently recommended by the Dutch Data Protection Authority (the **AP**).

As noted earlier, the Law Society acknowledges that the current leeway given to Member States for the regulation of AI is a relatively recent change to the AI Act: the European Parliament's earlier draft, adopted on 14 June 2023,[6] had proposed to centralise AI oversight in a single national surveillance authority in each Member State.[7]

[2] Spain established the Spanish Agency for the Supervision of Artificial Intelligence (**AESIA**) in September 2023, prior to the EU AI Act, for this exact purpose. It may be worth noting that AESIA does not supersede the Spanish data protection authority (AEPD) but it complements and collaborates with it as a co-enforcer of data protection/AI regulation.

[3] France appointed the national data protection authority as the central authority for the regulation of AI in the State. In France, this role is filled by the National Commission on Informatics and Liberty (**CNIL**) which has already created a department dedicated solely to AI. For an example of the grade of work that the CNIL carries out, please see its recent recommendations on the development of AI systems. Available at: https://cnil.fr/en/ai-cnil-publishes-its-first-recommendations-development-artificial-intelligence-systems

[4] For example, the Central Bank of Ireland (CBI) could regulate AI used in financial transactions. Article 74 of the AI Act does require that, under certain circumstances, the national competent authority for financial institutions should be the relevant national authority responsible for the supervision of those institutions in the first place, i.e. the CBI. There is a derogation from this allowing for another relevant authority to be designated by a Member State as an MSA supervising the financial sector, where there are proper coordination measures in place (Article 74, para. 6).

[5] Although outside of the EU, the UK has taken a similar approach to this by establishing the Digital Regulation Cooperation Forum composed of four separate digital regulators that are seeking to coordinate their efforts on AI (and other areas such as online platforms and digital services).

[6] Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

[7] This would have been, in contrast, a departure from the final text of the General Data Protection Regulation (the **GDPR**) which allowed Member States to establish one or more independent public authorities for monitoring the application of the GDPR. The Parliament's proposal differed from the

The EU's approach to the regulation of the AI Act closely follows the principle of subsidiarity by assigning essential roles to both the Member States and the Commission alike.[8] Considering this leeway given by the Act there is a clear opportunity to identify the considerations that should be taken into account prior to pursuing a 'centralised' versus a 'distributed' approach towards national implementation of the Act. Ireland is completely free to adopt a stance of its own choosing so long as it is within the framework established by the AI Act requiring a minimum of one market surveillance authority, one notifying authority, and one single point of contact.

The Law Society recognises that it is not necessarily an either/or question when it comes to centralised or distributed forms of governance. A centralised regulatory system, for example, can be complemented with a distribution of oversight activities drawn from groups across society.[9]

The Law Society notes that the Department consultation specifically asks for considerations that should be taken into account when planning this national implementation of the Act and the Law Society aims to fully detail any considerations that it believes relevant.

Main Considerations

When implementing the provisions of the EU AI Act at a national level by configuring the new AI regulatory landscape, the Department should prioritise the following considerations:

A. Maximising the efficiency of sectoral expertise and encouraging robust stakeholder engagement

The Department should, in considering a suitable means of national implementation, seek to leverage and maximise pre-existing and future sectoral expertise. In addition, the model that ends up being implemented by the Department should itself facilitate ongoing stakeholder engagement.

Distributed model

In this regard, the Law Society notes that a 'distributed' model of national implementation would have an advantage over a more 'centralised' approach. If a centralised market surveillance authority were to be established, it might lack easily-accessible expertise in AI as applied to financial contexts, legal contexts, healthcare contexts and so on. This would necessitate extensive cooperation between the centralised authority and various financial, legal and healthcare institutions, which may be less efficient than a more decentralised model where each of these institutions have bespoke remit over AI in their respective areas (such as the CBI for AI in finance, the Department of Justice over law enforcement, the Department of Health over healthcare and so on).[10]

Council and Commission proposals which aimed to give more freedom for Member States to designate and establish market surveillance authorities.

[8] Manuel Wörsdörfer, 'The E.U.'s Artificial Intelligence Act: An Ordoliberal Assessment' (AI Ethics, 2023), p. 8.

[9] Joan Lopez Solano and others, 'Governing data and artificial intelligence for all: models for sustainable and just data governance' (European Parliamentary Research Service, 2022).

[10] For example, the AI Now Institute has previously argued (in the US context) that domains like health, education, criminal justice and welfare all have their own contextual backgrounds and regulatory frameworks: therefore, a national AI safety body will struggle to meet the sectoral expertise minimum standards needed for regulation that is nuanced and well-rounded. They also gave (non-AI)

On the other hand, a distributed model may also have issues pooling expertise and knowledge as each market surveillance authority is segregated in its own area, making coordination difficult.

Centralised model

Although the above considerations are relevant, a centralised model,[11] if implemented correctly, could avoid these pitfalls and be able to effectively harness sectoral expertise while also benefiting from the various advantages that a centralised model could bring. The Data Protection Commission, although it is a centralised authority responsible for data protection in Ireland, regularly consults with experts from various sectors when drafting its guidance notes. It has also committed to increased stakeholder and sectoral expertise engagement in its strategy,[12] which was well received by those parties.[13] A centralised authority could emulate these models in order to maximise: (a) its utility of sectoral expertise, and (b) stakeholder engagement.

Democratising oversight within a centralised system can lead to better outcomes than a fully distributed system in that accountability is more representative of society. This approach fits into a reflexive system of governance which gives voice to all sectors of society.[14]

Further considerations

Any national regulatory model introduced by the Department should have a strong focus on engaging with stakeholders such as researchers from academia, expert organisations and consumer advocacy organisations. In addition, the Law Society recognises that the general public are also important stakeholders in the development of safe, effective, well-regulated AI systems. The Department might also consider creating a regulatory framework that is particularly aware of the needs of the public. For example, national competent authorities might be required to have an online feedback and complaints portal aimed at the public.

As noted by the International Association of Privacy Professionals (IAPP), AI is not a static product and its regulation requires continuous adaptation. Accordingly, the AI Act and its provisions need to be flexible: it is a framework that will be continually built upon and expanded by the EU (see answer to Question 3). In this sense, the Irish stance on the Act should remain agile. Maintaining a continued dialogue with sectoral expertise and stakeholders is particularly important given the fact that AI is an emerging and rapidly developing technology. The Law Society wishes to emphasise that, together with its Intellectual Property & Data Protection and Technology Committees, it is happy to offer expertise, feedback and support on any national implementation measures being devised by the Department in the coming years.

Finally, Recitals 105 to 109 of the AI Act require that the providers of GPAI models put in place policies to comply with the requirements of EU copyright and related rights law. In particular,

examples of this in the US, such as the US Federal Aviation Administration – see the AI Now Report 2018 (AI Now Institute, December 2018) at page 4. The same is true in Ireland, with a variety of different organisations possessing expertise in their own respective areas.

[11] Like with the AESIA in Spain, or CNIL in France.

[12] Draft Regulatory Strategy for 2021-2026 (Data Protection Commission).

[13] Regulatory Strategy: Consultation Feedback Report, pgs 9-10. Available at: https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Regulatory%20Strategy_Final%20Consultation%20Report.pdf

[14] Labhaoise Ní Fhaoláin, Vivek Nallur and Colin Scott, ‘Promoting Social Justice through the Reflexive Governance of AI’ in Karine Gentelet (eds), *Considering Artificial Intelligence Through the Lens of Social Justice* (Presses de l’Université Laval 2023).

the consent of rights holders is required to the text and data mining of copyright works, unless the exception under Article 4 of the Copyright Directive EU (2019/790) applies and the rights holders have not reserved their rights in the appropriate manner including in machine readable form for online content under the provisions of Article 4(3) of that Directive.

These matters are of great concern to Irish creative industries which rely extensively on the integrity of copyright and related rights law to protect their products and services. Any regulation of AI in Ireland needs to ensure that the transparency requirements in the AI Act related to text and data mining and the provisions of Articles 3 and 4 of the Copyright Directive are fully reflected in the regulatory regime.

B. Ensuring that any national competent authorities are well resourced

It is made explicit under the AI Act that all national competent authorities should have access to the suitable expertise in AI, personal data protection, cybersecurity, fundamental rights, health/safety risks and knowledge of existing standards and legal requirements. They must also be provided with adequate technical, financial and human resources by Member States. These authorities must also ensure an adequate level of cybersecurity.

Accordingly, there is a positive obligation contained in the AI Act for a Member State to keep any national competent authorities well-resourced including with technical know-how. This might pose a particular set of challenges as a solution is not as simple as shifting resources to authorities. Technical capabilities are often concentrated in a small number of private sector organisations that pay large salaries compared to those offered in regulatory bodies (regulatory bodies being the primary candidates for Ireland's future national competent authorities). The AI Act also requires agents involved in product safety regulation to assess risks to fundamental rights.[15]

Regulating product safety is substantially different than the assessment of risks to fundamental rights, and this difference will necessitate the contracting of external expertise or internal staff training. Both of these outcomes are very resource-intensive and will likely necessitate the procurement of external assistance. It is also acknowledged that the resource issue is exacerbated by the introduction of, among other instruments, the Digital Services Act which imposes additional burdens on regulators that cannot be easily rectified by increased funding.[16] This is despite the fact that there are potential synergies between the AI Act and the Digital Services Act (see answer to Question 2).

The Department should take into account the above concerns when considering how to implement the AI Act. The Department should prioritise the public interest by protecting fundamental rights above all else, ensuring that the development of AI is transparent and ethical. The Law Society would caution that an overreliance on private sector actors could increase the risk of regulatory capture whereby AI is regulated in a manner that benefits and protects deployers and providers of AI systems, rather than the general public who are most at risk of having their private information mishandled or reputations damaged by AI misuse.

Resourcing issues should therefore be carefully considered by the Department. It is not simply a financing issue that can be solved with additional funding: the Department should put a strategic focus on supplying a future regulatory infrastructure with the right knowledge and expertise. All future regulatory bodies should be aided directly by the Department in the sense

[15] Marco Almada and Nicolas Petit, 'The EU AI Act: A Medley of Product Safety and Fundamental Rights?' (European University Institute - Robert Schuman Centre for Advanced Studies, 2023), pgs 22-23.

[16] Ibid.

of providing not just funding, but also the means of acquiring, hiring and retaining talent in the form of AI specialists and researchers.

The Law Society recognises this is a challenge and it would take a substantial amount of time and effort to build up this infrastructure. The Department might look to the DPC as a useful model as the DPC possesses a substantial amount of expertise while being the sole data protection authority in Ireland. The DPC also works effectively with third parties from a wide range of backgrounds to rectify any areas in which it might lack expertise or knowledge. The DPC's substantial bank of expertise and experience makes it a good candidate to be the main enforcer or co-enforcer of the Act's provisions, depending on the final approach taken by the Department.

This being said, the Law Society also recognises the huge potential of AI when developed safely and used responsibly. The Law Society fully recognises the worth of 'regulatory sandboxes'[17] (which have been implemented in other jurisdictions[18]) for the development of groundbreaking AI systems. The AI Act requires Member States to set up regulatory sandboxes for the testing of AI innovations.[19] Accordingly, the Department should give strong consideration towards fully resourcing these initiatives with the necessary human capital and financial support.

The Law Society would also recommend that the Department, when implementing the AI Act, should seek to facilitate an interplay between academia and NGO resources to maintain this focus on the protection of fundamental rights in the public interest. Although AI regulation also has a product safety dimension, the ethos of the AI Act (like the GDPR) emphasises a rights-based approach focusing on individual rights to privacy and dignity. Accordingly, the Law Society would recommend that the Department strongly prioritise the protection of fundamental rights by robustly resourcing any future national competent authority or authorities and organising them in such a manner to vindicate the rights of the public.

C. Facilitating communication and coordination between national competent authorities

One potentially significant concern associated with a decentralised model is that it would make coordination and communication between national competent authorities difficult. Such issues would generally not be present in a centralised model as all the components of a central regulator would be able to easily exchange information and coordinate their efforts under a singular strategy.

At EU-level, the EU will coordinate the work of national supervisory authorities and the Commission via the European AI Board (**EAIB**).[20] If adopting a more distributed model of regulation, a system similar to this could be implemented by the Department whereby a national-level AI Board or Commission could coordinate various national competent authorities and enable the sharing of information from one organisation to another.

It may be worthwhile to note that the EU requires at least one notifying authority, one market surveillance authority, and one single point of contact. A model in which all of these authorities are separate might present communication and logistical challenges, and could lead to

[17] A testing ground for AI where regulatory restrictions have been loosened, within a controlled environment. See response to Question 3.

[18] See, for example Filippo Bagni, 'The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act' (Rivista italiana di informatica e diritto, 2023) pgs 205-207.

[19] Article 57.

[20] Article 65.

unnecessary bureaucracy and inefficiency. A centralised approach would certainly have an advantage in this sense, assuming that the centralised approach involved a singular notifying authority, market surveillance authority and single point of contact concentrated in one national competent authority. This would also facilitate the liaising of Ireland's AI regulatory landscape with the EAIB.

D. Improving access to justice

It is the view of the Law Society that any national implementation of the EU AI Act would be undermined if such an implementation did not adequately consider access to justice.

Under Article 85, the EU AI Act does contain provisions that allow individual members of the public to lodge a complaint directly with a market surveillance authority, without prejudice to other administrative or judicial remedies. The Law Society sees this as a very positive aspect of the AI Act. There are no restrictions placed on this right: an individual who makes a complaint might not necessarily have conventional legal standing.

The legal system ought not to be the sole means by which members of the public seek to lodge their complaints. The implementation of this guaranteed right to lodge a complaint, although positive, must be seriously considered by the Department when constructing the new regulatory framework around AI as certain modes of national implementation might interfere with the intended nature of this right making it difficult for an individual to make a complaint.[21] The process for making a complaint should be as streamlined as possible to make the process accessible for members of the public.[22] The Government might also consider providing an explicit right for civil society organisations to bring a complaint on behalf of an individual or group of individuals.

Having a single point of contact for the public would help with access to justice through the complaints mechanism, although the Department might also consider other alternative approaches for complaint-making. The Ada Lovelace Institute, for example, has proposed the piloting of an AI Ombudsman role in the UK.[23] This would allow complaints to be coalesced in one Office in the event the Department pursues a distributed model. In the event the Department pursues a centralised model, having an AI Ombudsman might help alleviate backlogs in complaints as well as allowing the Ombudsman to collaborate with Ombudsmen from other sectors of Irish economy and society. Related to this, Ireland has already implemented an Ombudsman mechanism across various areas.[24] It might be beneficial for the Department to investigate the possibility of such a position for AI as this role could enhance access to justice by creating a forward-facing and proactive Office dedicated solely to the investigation of complaints.

[21] In a distributed model of national implementation it may be unclear, depending on how such a model is implemented, where a person should make a complaint particularly where the alleged abuse of AI might span multiple areas (such as finance and health). In a centralised system, an individual would only need to make a formal complaint on misuse of AI to a single competent authority.
[22] For example and as mentioned before, the Department might require national competent authorities to implement an online complaints and feedback portal for the public and require them to regularly consult their users. Once the Department decides on a model regulatory framework, they might also invite feedback from the public and publish a roadmap for implementation so that the general public can view the progress on its implementation.
[23] Regulating AI in the UK (Ada Lovelace Institute, July 2023) pgs 29-30. Available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2023/09/ALI_Regulating-AI-in-the-UK_2023.pdf
[24] Including the Financial Services and Pensions Ombudsman, the Office of the Ombudsman (which investigates complaints against public service providers) and the Garda Síochána Ombudsman Commission (soon to be rebranded as Fiosrú – the Office of the Police Ombudsman) which deals with complaints against members of the Gardaí.

Question 2: The EU has adopted a series of Regulations in recent years designed to protect consumers, strengthen the internal market and ensure that the EU remains at the forefront of innovation and the adoption of advanced technologies.

Are there potential synergies between the implementation of the AI Act and the implementation of other EU Regulations applying to digital markets, services and infrastructure?

Answer:

There are potential synergies between the implementation of other EU Regulations (applying to digital markets, services, and infrastructure) and the AI Act.

- **The AI Act and the General Data Protection Regulation**

Potential synergies exist between the implementation of the AI Act and the General Data Protection Regulation (**GDPR**). While the two regulations address different entities — the GDPR outlines obligations for data controllers and processors, while the AI Act targets providers and users of AI systems—organisations must carefully map these concepts to determine which parties are subject to the requirements of the AI Act, GDPR or both. This is particularly important due to the overlapping aspects of the two regimes, especially regarding (1) bias and discrimination, (2) risk assessments, and (3) solely automated decision-making.[25]

For example, a company (A) that processes personal data to train a new AI system, functions both as a provider under the EU AI Act and as a controller under the GDPR. This dual role arises because the company is developing a new AI system and is making decisions about how to process personal data for the purpose of training it.[26] Following on from the first example, if a company (B) that purchases the AI system from company A (as described in Example 1) and uses it in a manner involving the processing of personal data (such as a chatbot for customer interactions or an automated recruitment tool) it will act as both a deployer under the EU AI Act and a controller under the GDPR for its own personal data processing. This means company B is not responsible for the personal data originally used to train the AI system but is responsible for any data it uses in conjunction with the AI.[27]

Clearly, organisations deploying AI systems will need to be well-versed in both the AI Act and the GDPR. Organisations may need to adopt more proactive measures to ensure compliance with the AI Act, such as conducting regular risk assessments and implementing robust data governance frameworks. This proactive stance will be critical to avoiding enforcement actions. When complying with both Acts, synergies in implementation will become apparent including in the following ways.

Data protection authorities and the implementation of the AI Act

Before the EU AI Act, EU data protection authorities (**DPAs**) were among the first regulatory bodies to take enforcement actions against the use of AI systems. These actions were based on various concerns, particularly the lack of a legal basis for processing personal data or special categories of personal data, lack of transparency, abuses in automated decision-

[25] See https://www.euaiact.com/key-issue/6

[26] See https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/#:~:text=Human%20oversight%20under%20the%20EU,legal%20or%20similarly%20significant%20effects.

[27] Ibid.

making, failure to fulfil data subject rights, and issues with data accuracy.[28] The introduction of the EU AI Act is likely to change the enforcement landscape for AI systems in several significant ways compared to the previous actions taken by DPAs.

- Specific Requirements for AI Systems: The EU AI Act introduces specific requirements for different categories of AI systems, such as high-risk AI. These requirements include risk management, data governance, transparency, and human oversight. This specificity will likely lead to more detailed and targeted enforcement actions by DPAs and authorities established under the AI Act. In addition, the AI Act places particular emphasis on high-risk AI systems, which are subject to stricter requirements. This focus means that enforcement actions will likely target these systems more rigorously, ensuring that they adhere to the highest standards of safety and accountability as required by EU regulations.
- Enhanced Transparency Obligations: The AI Act mandates higher levels of transparency from AI providers and deployers, requiring them to provide clear information about the operation and purpose of AI systems. This increased transparency will enable more effective monitoring and enforcement by regulatory bodies, including DPAs.
- Increased Penalties and Sanctions: The EU AI Act is expected to introduce stringent penalties for non-compliance, similar to the GDPR. These increased penalties can act as a stronger deterrent against violations and encourage organisations to prioritise compliance. Penalties under multiple EU regulations will create a synergistic deterrent effect whereby the risk of non-compliance with multiple regulations brought on by a single violation could mean heavy fines that not even the largest corporations can afford to ignore.
- Collaboration Between Authorities: The AI Act encourages collaboration between different regulatory bodies, including DPAs and those overseeing AI regulations. This collaborative approach can lead to more comprehensive and coordinated enforcement actions. Enforcement bodies will be able to collaborate on complex enforcement actions, bringing additional resources to bear on violators. Moreover, multiple agencies overseeing the sector will mean that less violations go unnoticed by regulators, and regulatory bodies can inform each other of violations that might not be solidly within their regulatory scope.

Furthermore, as DPAs develop their enforcement policies influenced by public concerns, and with the growing public awareness and interest in AI, it is likely that DPAs will increasingly focus on AI.[29] Overall, the EU AI Act is set to create a more structured and rigorous enforcement landscape for AI systems, addressing a broader array of concerns and ensuring higher standards of accountability and transparency that will benefit the implementation and enforcement of the GDPR and other EU regulations.

It has been noted previously in this submission that certain models of AI regulation could lead to DPAs being enforcers of the provisions of the AI Act. The EU AI Act mandates that each Member State designate one or more national competent authorities responsible for supervising the application and implementation of the Act. These authorities will also be tasked with conducting market surveillance activities to ensure compliance with the new regulations. The national competent authorities will receive support from the European Artificial Intelligence Board and the European AI Office. The European AI Office's most significant duty

[28] See https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/#:~:text=Human%20oversight%20under%20the%20EU,legal%20or%20similarly%20significant%20effects.

[29] Ibid.

is to enforce and supervise the new rules for general-purpose AI models, ensuring that these models adhere to the standards set out in the AI Act. The potential appointment of the Data Protection Commission (**DPC**) as the main enforcer or co-enforcer of the EU AI Act would reinforce the existing relationship between the EU GDPR and the EU AI Act. This would create a cohesive regulatory framework, leveraging the expertise of DPAs in handling data protection and privacy issues to oversee the responsible deployment and use of AI systems across the EU. It is noted that the Spanish AESIA, mentioned earlier in this submission, cooperates extensively in this manner with the Spanish data protection authority (AEPD) by sharing expertise and knowledge.

Conformity assessments and fundamental rights impact assessments under the AI Act and the data protection impact assessments under the GDPR

The AI Act requires conformity assessments to ensure that providers adhere to its requirements for the safe development of high-risk AI systems.[30] These conformity assessments are not risk assessments; instead, they serve as demonstrative tools to verify compliance with the EU AI Act's stipulations. Furthermore, the AI Act requires a fundamental rights impact assessment (**FRIA**). The purpose of a FRIA is to identify and mitigate risks to the fundamental rights of individuals arising from the deployment of an AI system. In addition to the above requirements, it is likely that AI systems will be subject to data protection impact assessments (**DPIAs**), as mandated by the GDPR, for high-risk personal data processing activities. According to Article 35 of the GDPR, data controllers must conduct DPIAs when processing activities are likely to pose a high risk to the rights and freedoms of individuals.[31]

AI providers may not always be able to predict all potential uses of a system. Even if a provider's initial assessment deems the system not high-risk under the AI Act, this does not preclude a subsequent data protection impact assessment by the user. Consequently, the same AI system might be subject to varying risk management requirements and classifications under different laws. In this way, providers of high-risk AI systems may also need to conduct a DPIA concerning the use of personal data during the development and training of the system. In this context, the technical documentation prepared for conformity assessments can help establish the factual basis for a DPIA. Similarly, this technical information can assist a deployer of the AI system who is required to conduct a DPIA related to its use.

The synergy between the GDPR and the EU AI Act lies in their complementary focus: while the GDPR emphasises the need for DPIAs to protect individual rights and freedoms, the EU AI Act mandates conformity assessments to ensure the safe development of AI systems. This dual framework ensures that AI systems are both compliant with safety standards and considerate of data protection principles, requiring AI providers and users to navigate and harmonise these overlapping regulatory landscapes effectively.

Some organisations, particularly so in the case of larger organisations, already have governance mechanisms in place that bring together legal, IT and business professionals for impact assessments like the DPIA.[32] In these organisations, those existing structures can also be utilised for conducting assessments mandated by the AI Act. Similar to a DPIA, the initial step in conducting an assessment under the AI Act is likely a pre-screening to identify the use

[30] AI Act, Title III, Chapter 2.

[31] See https://www.euaiact.com/key-issue/6

[32] Small and medium enterprises may not already have these governance mechanisms in place, necessitating Government aid and support. See the answer to Question 3 for further discussion on this.

of a high-risk AI system that falls within the scope.[33] In addition, if obligations related to fundamental rights impact assessments under the AI act are already addressed through the GDPR's data protection impact assessments), then these assessments should be conducted in parallel.[34] It is unlikely, however, that a DPIA will cover all the obligations required of FRIAs. FRIAs under the AI Act have a broader material scope because DPIAs typically focus on a single fundamental right: data privacy. In contrast, FRIAs must address a wide array of fundamental rights, which can be particularly challenging due to the inherent complexity of AI systems.[35]

- **Synergies between the implementation of the AI Act and the Digital Services Act package**

The Digital Services Act (**DSA**) and the AI Act fundamentally address different aspects of technology regulation. The AI Act primarily governs AI technology, while the DSA regulates intermediary services, including online platforms. While the development of the DSA occurred when Generative AI was still emerging and although the DSA and AI Act were enacted separately, the regulation of platforms and the use of AI systems are becoming increasingly interconnected as acknowledged in the AI Act's preamble. Determining the legal framework applicable to issues at the intersection of AI and platform regulation may require efforts to harmonise these two distinct but parallel pieces of legislation.

The DSA encompasses three broad categories of intermediary services: conduit, caching, and hosting. Generally, standalone AI services such as generative AI, which create new content based on user prompts, do not fall into these categories.[36] However, the distinction between standalone large language models performing exhaustive internet searches and traditional search engines has become increasingly blurred. For instance, Google's recent introduction of AI Overviews transforms its traditional services by providing users with AI-generated answers drawn from web information, aiming to directly present the sought-after information instead of just listing links.

Moreover, interpersonal communication services, like emails or private messaging services, fall outside the DSA's scope for hosting services and are subject to specific requirements only when operating through public groups or open channels.[37] Consequently, AI chatbots facilitating individual user interactions on online platforms are generally excluded from the DSA rules applicable to the main service. A more complex scenario arises when generative AI products are integrated into platforms subject to the DSA and offered as a specific service. These tools may prompt or assist in creating new content, such as text and images, involving some level of human intervention.

Synergistic regulation of systemic risks in the DSA and the AI Act

[33] See https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/#:~:text=Human%20oversight%20under%20the%20EU,legal%20or%20similarly%20significant%20effects.

[34] AI Act, Article 29a.

[35] See https://www.technologyslegaledge.com/2024/03/fundamental-rights-impact-assessments-under-the-eu-ai-act-who-what-and-how/?_gl=1*2kv90j*_ga*MTg3MjEwMzgzOC4xNzE4ODcyNjQ3*_ga_NF3H0849M0*MTcxOTIzNjEyNS4zLjEuMTcxOTIzNjEyOC42MC4wLjA.

[36] See https://www.techpolicy.press/the-digital-services-act-meets-the-ai-act-bridging-platform-and-ai-governance/

[37] Ibid.

A key area where the AI Act and the DSA intersect is in the obligation to assess and mitigate "systemic risks" as outlined in both laws.[38] This obligation requires both AI system providers and digital service intermediaries to conduct thorough risk assessments to identify potential harms that their technologies or services could pose to users and society at large. The aim is to implement measures that mitigate these risks, ensuring that their operations do not negatively impact areas such as user safety, public health, democratic processes or fundamental rights. The systemic risks include not only technical failures and security vulnerabilities but also broader societal impacts, such as the spread of misinformation, discrimination, and threats to freedom of expression. Consequently, both the AI Act and the DSA emphasise the importance of accountability and proactive risk management to create a safer and more transparent digital environment.

Once in effect, the AI Act will require providers of general-purpose AI models with systemic risks to assess and mitigate these risks. General-purpose AI models, which are trained on large datasets and capable of performing a wide range of tasks, are considered to have systemic risks if they possess high-impact capabilities. Industry experts have noted that this criterion will include many current models.[39]

The DSA, adopted in 2022 and fully applicable since February 2023, also mandates that Very Large Online Platforms (**VLOPs**) and Very Large Online Search Engines (**VLOSEs**) assess and mitigate "systemic risks." Although the definition of systemic risks in the AI Act and the DSA are not identical, they share many similarities.[40] The AI Act explicitly states that AI systems integrated into VLOPs or VLOSEs must adhere to the risk management framework of the DSA.[41] Furthermore, the AI Act stipulates that if AI models comply with the systemic risk obligations outlined in the DSA, they are also presumed to meet the requirements of the AI Act, provided no significant systemic risks not addressed by the DSA arise.

The recitals of the AI Act indicate that the authorities designated under the DSA should also serve as enforcement authorities for the AI Act's recommended system provisions.[42] Practically, for VLOPs, this implies that the DSA Compliance Officer may play a significant role in regulatory interactions concerning the AI Act.

[38] See https://www.techpolicy.press/the-digital-services-act-meets-the-ai-act-bridging-platform-and-ai-governance/

[39] See https://aibusiness.com/responsible-ai/eu-ai-act-would-scrutinize-many-general-ai-models-sxsw-2024

[40] See https://www.techpolicy.press/the-digital-services-act-meets-the-ai-act-bridging-platform-and-ai-governance/

[41] See https://legalbriefs.deloitte.com/post/102ierr/eu-ai-act-implications-for-vlops-and-digital-services-act

[42] Ibid.

Question 3: **Harnessing Digital – The Digital Ireland Framework** establishes the goal for Ireland to be a digital leader at the heart of European and global digital developments. In support of this goal, Ireland is a member of the D9+ Group, an informal alliance of Digital Ministers from the digital frontrunner EU Member States. It also calls for Ireland to be a "centre of regulatory excellence" in Europe. The AI Act will set out a requirement to promote innovation, having regard to SMEs, including start-ups, that are providers or deployers of AI systems.

How can Ireland's implementation of the AI Act bolster Ireland's position as a leading Digital Economy, increasing investment and accelerating innovation in AI? What would excellence in AI regulation look like?

Answer:

A. How can Ireland's implementation of the AI Act bolster Ireland's position as a leading Digital Economy, increasing investment and accelerating innovation in AI?

Regulatory sandboxes

Ireland is the only major English-speaking common law jurisdiction in the Eurozone. In addition to hosting large tech and pharmaceutical companies, Ireland also has a strong foundation of educational excellence particularly in the technological fields which forms the basis of a very effective supply chain of human capital. Irish third-level STEM graduates per 100,000 people are the highest in Europe. Ireland already possesses substantial financial incentive for R&D and has encouraged a strong industry cluster environment supporting collaboration between corporations and researchers. These offerings mean that Ireland is uniquely and strongly positioned to leverage investment and innovation in AI as a leading Digital Economy.[43]

Article 57 of the AI Act requires that Member States establish at least one regulatory sandbox at a national level. These regulatory sandboxes are permitted to be established jointly with the national competent authorities of other Member States. Article 57.2 allows Member States to establish additional regulatory sandboxes at regional or local levels on their own volition. These sandboxes may also be given technical support, advice and tools by the European Commission.

Regulatory sandboxes have the potential to increase investment and accelerate innovation in AI in Ireland. The Government could look at establishing collaborative initiatives with other Member States to pool resources and expertise, in order to maximise the effectiveness of these regulatory sandboxes. In addition, direct Commission support for these sandboxes could help alleviate existing concerns about access to resources and talent.

Under the Digital Ireland Framework the Government has committed to promoting the creation of testbeds and regulatory sandboxes for AI (and other digital technologies).[44] The AI Act imposes a requirement on Member States to establish at least one such sandbox. The Government could consider establishing a number of regulatory sandboxes allowing for innovation in particular narrow areas. For example, in the UK both the Financial Conduct Authority (**FCA**) and the Information Commissioner's Office (**ICO**) have established regulatory sandboxes relating to AI solutions in their respective areas. The FCA sandbox is fintech-

[43] The Law Society is actively involved in promoting Ireland's advantages as a venue for international legal work, emphasising its competitiveness and its attractiveness in relation to the rule of law, through its support for Ireland for Law. The Ireland for Law initiative is also supported by the IDA, the Bar of Ireland and the Department of Justice.
[44] Page 13.

focused but it also admits AI solutions with applications in the financial sector, whereas the ICO sandbox includes a focus on AI and privacy-related solutions. In France, the CNIL has established a personal data sandbox calling for projects in the field of health (which includes AI in that sphere). The German Government, in accordance with its AI strategy and via the coordinating office for Regulatory Sandboxes at the Federal Ministry for Economic Affairs and Climate Action, established and is planning to establish multiple regulatory sandboxes[45] (for particularly granular applications[46]). Numerous firms and colleges in Ireland have also independently started their own AI innovation programmes, including AI incubators which, although not the same as a formal regulatory sandbox, operate on similar principles.[47]

A tailored regulatory sandbox could be established specifically for the development and testing of AI to be used in legal contexts.

AI systems for Legal Aid efforts

The Law Society, having a strong interest in improving access to justice, notes that it has been previously argued that there is strong potential for AI to enhance the administration and provision of legal aid in Ireland, but that these efficiencies come with risks, especially if AI is used to make decisions that affect individual rights (i.e. whether to grant or deny requests for criminal legal aid) without human oversight,[48] meaning that testing AI tools designed to improve legal aid outcomes in the real world might be excessively risky.

A low-risk regulatory sandbox used for the express purpose of testing AI systems for use in the provision of legal aid would be an ideal method by which any shortcomings of such AI could be ironed out in advance of any deployment of such systems. These systems may be classified as high risk under the Act meaning that extensive testing and regulation is a must, although their potential utility to the streamlining of the legal aid process is evident. A regulatory sandbox like this, contained under a broader, law-related regulatory sandbox could be resourced by the Commission and could be conducted with cross-Member State cooperation.

*Supporting and nurturing small and medium enterprises (**SMEs**)*

Under Article 62, Member States are required to give priority access for SMEs and start-ups to any regulatory sandboxes established under the Act. Ireland is, according to a report by PwC, already a highly attractive jurisdiction for business. It seems likely that the correct implementation of AI regulation could improve Ireland's attractiveness even further.

If the Government were to introduce a dedicated regulatory sandbox for AI with legal applications, this would be an important aspect of the AI Act's implementation as, in

[45] Regulatory Sandboxes in Artificial Intelligence (OECD Digital Economy Papers, July 2023), pgs. 30-32. Available at: https://www.oecd-ilibrary.org/docserver/8f80a0e6-en.pdf?expires=1719389902&id=id&accname=guest&checksum=F7D7556BABEA846BAD579710869A799F

[46] Including (a) a regulatory sandbox, established in Hamburg, for the specific purpose of testing an autonomous delivery robot and (b) a regulatory sandbox focused specifically on automated driving.

[47] UCD, for example, has created an AI accelerator programme for start-ups and entrepreneurs aiming to support them in developing AI solutions in key sectors such as healthcare and finance. Intel created an AI incubator partnership with DCU at Talent Garden Dublin in 2018, aimed at providing technical support and guidance to AI innovators. Finally, Expleo (a global engineering, technology and consulting services provider) invested €1 million to launch an AI centre of excellence in 2024. This AI centre aims to gather more than 380 experts to help businesses adopt AI including generative AI and AI involved in fraud detection.

[48] See https://www.lawsociety.ie/gazette/top-stories/2024/may/human-oversight-key-to-fair-use-of-ai-in-legal-aid

comparison to smaller organisations, larger firms have easy access to resources and talent. In the future this would lead to a lopsided adoption of legal AI in Ireland, something that could prejudice smaller firms. Large law firms are already taking the initiative by extensively collaborating with AI providers (such as A&L Goodbody and McCann FitzGerald announcing partnerships with Harvey AI). The option of extensively cooperating with an AI provider is not available to small and medium firms meaning easy access to regulatory sandboxes would help to reduce the ever-widening AI gap in the legal industry. Smaller firms could maximise their engagement with these sandboxes through the medium of industry clusters encouraged by the Government for the exact purpose of facilitating the development of AI tools.

Small and medium firms in Ireland are extremely important, particularly in rural communities and in smaller towns where they are often the sole providers of legal services to the public. Maintaining the competitiveness of these firms is of particular importance. To this end, the Government might seek to leverage all relevant EU financial aid via the Digital Europe programme to support SMEs throughout the economy but particularly in the legal sphere. The legal profession in Ireland is well positioned to play a leading role in the use of ethical AI and this prospect can be enhanced through robust Government financial and technical support as well as funding at the EU level. Targeted supports for SMEs would be key to minimise the AI technology gap. The Government should strive to avoid the formation of a two-tier economy where some firms, due to an inherent advantage in financial resources or expertise, have a substantial advantage in leveraging new AI tools relative to smaller firms.

This access for small and medium firms would coincide with the Government's commitment in the Framework to develop a comprehensive programme of digitalisation across enterprise (with a particular focus on SMEs),[49] running from 2022 to 2026. The Law Society notes that the Government has also committed to funding this programme with the €85 million Digital Transition Fund and by leveraging the National Recovery and Resilience Plan to give particular attention to SMEs. The Law Society welcomes these initiatives and believes that it will coincide well with the AI Act's focus on aiding SMEs in adopting AI tools in the future.

B. What would excellence in AI regulation look like?

AI regulatory excellency is achievable in Ireland given the unique characteristics of our jurisdiction. From the perspective of the Law Society, regulatory excellence would possess the following characteristics:

Certainty and flexibility

The nature of AI technologies present a series of problems that make it difficult for a democratic society to regulate them. Namely, in order to maintain legal certainty laws need to be clear, precise and fixed to an extent: but in the case of the regulation of a rapidly-moving technology like AI, laws need to have a degree of flexibility to adapt to changing circumstances. This is often expressed as a 'pacing problem' i.e. a gap between the pace of regulation and technological advancement.[50] One common criticism has emphasised regulators' inadequate understanding of complex and rapidly-developing AI systems.[51]

[49] Page 9.
[50] Stefan Larsson, Jockum Hildén and Kasia Söderlund, 'Between Regulatory Fixity and Flexibility in the EU AI Act' (Lund University, 2024), pgs 1-2. Available at: https://portal.research.lu.se/en/publications/between-regulatory-fixity-and-flexibility-in-the-eu-ai-act
[51] Anu Bradford, 'The False Choice Between Digital Regulation and Innovation' (2024) 118(2) Northwestern University Law Review, p. 29.

AI is developing extremely rapidly with figures demonstrating that, since 2012, the amount of computing power used in the largest AI training runs has grown by more than 300,000 times.[52] Of course, this dramatic and rapid increase in the capability of AI tools opens the potential for AI to be used in almost every sphere of life including in health, law enforcement and finance, and this necessitates a regulatory response in kind.

The AI Act itself contains flexible and 'future-proof' language and provisions, often bordering on 'soft governance' or anticipatory regulation. For example, the definition of AI in Article 3 is very broad leaving room for future interpretation. Article 69 of the Act also provides for voluntary codes of conduct that will be encouraged by the AI Office and Member States. As another example, the AI Act aims to introduce harmonised standards, established by European standard setting organisations (such as the European Committee for Standardisation), the primary function of which is to provide an example of how the essential requirements in the Act are to be interpreted on a detailed and technical level. When in conformity with these standards, a high-risk AI possesses the presumption of conformity with the AI Act.[53]

If regulations on AI are too flexible, they lack certainty and if they are excessively rigid, they lack the agility to respond a rapidly changing technology. The ideal AI regulatory landscape would be one that strikes a careful balance between flexibility and certainty.

Having both effective regulation and strong support for innovation and development

The Law Society believes that regulatory excellence and innovation are not mutually exclusive. It is entirely possible to construct an AI regulatory ecosystem that protects and cultivates individual rights as well as innovation. There is a common perception that European digital regulatory approaches, including in AI, stifle economic and innovation relative to the United States (which takes a more laissez-faire approach to regulation), for example.[54] Certain types of regulation, however, actively promote innovation (such as intellectual property protection) and innovation offsets produced by regulations can exceed the compliance costs of said regulations as companies find new ways to meet the demands of new regulations. New regulations may also encourage companies to join the market that would otherwise remain on the sidelines.[55] With regards to AI regulation, any costs of compliance may be offset if regulators help companies (particularly SMEs) with their compliance efforts.

Finally, creating trustworthy AI through effective regulation will lead to economic benefits as consumers will adopt AI as a consequence of trusting AI technologies that meet regulatory standards.[56] This will in turn attract the developers of AI tools to Ireland, boosting their revenues and allowing them to commit more resources to innovation which benefits the Irish AI landscape. Ireland should maintain its competitive advantage in Europe by leading in the development of AI tools, but this goal should not be pursued at the expense of public safety or data protection hence the need to synergise AI regulation with the GDPR (see answer to Question 2).

[52] Hannah Ruschemeier, 'AI as a challenge for legal regulation – the scope of application of the artificial intelligence act proposal' (2023) 23 ERA Forum 361.
[53] Stefan Larsson, Jockum Hildén and Kasia Söderlund, 'Between Regulatory Fixity and Flexibility in the EU AI Act' (Lund University, 2024), p. 11. Available at: https://portal.research.lu.se/en/publications/between-regulatory-fixity-and-flexibility-in-the-eu-ai-act
[54] Anu Bradford, 'The False Choice Between Digital Regulation and Innovation' (2024) 118(2) Northwestern University Law Review, p. 12.
[55] Ibid, 20.
[56] Ibid, 30-31.

The Law Society has made several suggestions to improve and encourage innovation under regulations stemming from the AI Act, including giving easier access to regulatory sandboxes for SMEs. In relation to future-proofing regulations to provide for continuous strong protections of fundamental rights, the Government could also look towards international regulatory initiatives such as the US Algorithmic Accountability Act (which is more technology-neutral in principle than the AI Act) as inspiration. Aside from this, the implementation of the AI Act should provide for the involvement of civil society organisations in the monitoring of AI, particularly in view of their focus on the protection of fundamental rights.[57] In addition, market expertise (particularly from SMEs) is also crucial for making AI regulation supportive of innovation.

A strong focus on sustainability

One often overlooked aspect of AI training and usage is the cost to the environment. AI consumes large amounts of energy and water. By 2027, for example, it is estimated that the total energy consumption of AI is estimated to rival the energy demand of the Netherlands or Argentina. The creation of one single image using a leading image generation AI requires as much energy as charging a smartphone.[58] The Law Society strongly believes any future AI regulatory landscape must, in the public interest, emphasise the importance of environmental sustainability.

The Government could construct regulations in such a way that emphasises AI sustainability, for example, by requiring environmental impact statements and increased transparency in disclosing what resources are consumed by AI models. The Government could also consider introducing a dedicated AI sustainability regulation which places caps on the amount of power or water that AI tools consume. It could also complement this approach by encouraging the adoption of AI industry codes of conduct that have a strong emphasis on sustainability and particularly the minimisation of power usage for AI. These codes could be made semi-binding and could be very effective when used in conjunction with formal regulation.[59]

Finally, if Ireland is to attain a competitive advantage in the development, training and operation of AI tools, its energy infrastructure must be well equipped to meet the needs of the AI industry. The Law Society notes that recent reports have suggested that Ireland's electricity supply is already restricted by rising demand and that Eirgrid expects that electricity supply and demand will be constrained in the next ten years.[60] If Ireland wishes to improve its position in relation to the hosting and development of advanced AI tools (particularly generative models) and become a European leader in AI, steps will need to be taken by the Government to correspondingly increase energy production.

[57] Marinos Kalpakos, 'Defining the Future: The AI Act's Potential in Equitably Safeguarding Fundamental Rights and Promoting AI Innovation' (UFITA, 2024) p. 165. Available at: https://www.nomos-elibrary.de/10.5771/2568-9185-2023-1-128.pdf

[58] Philipp Hacker, 'Sustainable AI Regulation' (European New School of Digital Studies, 2023). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4467684

[59] Ibid, p. 21-22. Article 95 in fact allows Member States to draw up codes of conduct specifically aimed at minimising the environmental footprint of AI systems.

[60] 'Squeeze on electricity supply to last into 2030s, report finds' (Irish Times, January 2024). Available at: https://www.irishtimes.com/ireland/2024/01/13/squeezed-electricity-supplies-may-force-state-to-fall-back-on-older-fossil-burning-power-plants-eirgrid-report/

Question 4: AI – Here for Good: National Artificial Intelligence Strategy for Ireland sets out how Ireland can be an international leader in using AI to benefit our economy and society, through a people-centred, ethical approach to its development, adoption and use. In recognition of the wide-ranging effect AI will have on our lives, this Strategy considers AI from several perspectives: Building public trust in AI; Leveraging AI for economic and social benefit; and Enablers for AI.

How can Ireland's implementation of the AI Act drive support and accelerate progress from each of these perspectives while meeting our regulatory obligations?

Answer:

The Law Society believes that Ireland's future implementation of the AI Act offers significant opportunities to drive support and accelerate progress from each of the three perspectives under the National AI Strategy (the **Strategy**). Within these three broad headings there are eight 'strands' of progress.

A. Building public trust in AI

The Law Society notes that a substantial amount of progress has been made by the Government under this heading in the last few years, notably under Strand 1 – "AI and Society". This progress includes the appointment of an AI Ambassador in May 2022 and the establishment of the National Youth Assembly on AI in October 2022.

The freedom given to the Member States by the AI Act allows Ireland to introduce a comprehensive and robust regulatory AI ecosystem (Strand 2 – "A Governance Ecosystem that Promotes Trustworthy AI"). The Government should consider the factors mentioned previously in this submission[61] prior to introducing any regulatory framework. Ireland's implementation of the AI Act will allow Ireland to exercise its soft power influence in the 'multinational forum' of the EU[62] to advocate for an ethical, human-centred approach to AI (while also not sacrificing a commitment to innovation and technological progress) particularly if Ireland's implementation of the Act involves a strong focus on cross-border cooperation with other Member States. This might be aided through collaboration with the Department of Foreign Affairs or other Departments as necessary.

The Strategy[63] mentions that the Government will seek to examine and promote ways to help businesses self-asses the trustworthiness of their AI systems. This will include the development of case studies and toolkits for SMEs and could be undertaken by the Department in conjunction with Enterprise Ireland. The success of this goal will depend on how the Government aims to implement Chapter X of the AI Act, which concerns voluntary codes of conduct. The Government could progress this strategic goal by developing codes of conduct on AI trustworthiness that would then be applied to businesses.

These codes could be developed collaboratively with organisations. For example, the Law Society is already aiming to ensure trustworthiness in legal AI by working to provide guidance on the deployment of AI systems. This Law Society guidance is aimed at professionals, particularly those in small and medium law firms. The guidance also promotes an ethical and human rights-based approach to AI governance. The Law Society welcomes any future collaboration with the Government on legal industry codes of conduct on the use of AI.

[61] See answer to Question 1.
[62] Page 7 of the Strategy.
[63] Ibid.

The Law Society also notes that the Department of Children, Equality, Disability, Integration and Youth will consider the implications of AI as part of a planned review of equality legislation. AI, if misused, could have serious implications on equality particularly in the context of law enforcement (including discriminatory practices such as over policing that might be exacerbated by AI if not properly regulated). As noted in this submission's answer to Question 2, Article 27 of the Act requires that a fundamental rights assessment must be conducted by certain deployers of high-risk AI systems prior to any deployment to the market.

Finally, this submission has already advocated that regulatory sandboxes should, as a concept, be utilised in Ireland. This would coincide well with the Strategy's stated aims to investigate the utility of these sandboxes for promoting innovation. Regulatory sandboxes could be trialled and analysed for successes or failures. The Law Society believes that SME access to these sandboxes should be prioritised.

B. Leveraging AI for economic and social benefit

This strategic perspective is divided into Strand 3 ('Driving adoption of AI in Irish enterprise') and Strand 4 ('AI serving the public').

This submission has already mentioned extensively how the Government, in implementing the AI Act, could leverage AI for economic and social benefit. Namely, the Government could make effective use of regulatory sandboxes, encourage AI to be environmentally sustainable, and ensure the protection of fundamental rights by facilitating fundamental rights assessments. The Law Society notes a commitment in the Strategy that the GovTech Delivery Board will consider the adoption of AI by the Public Service (Page 9).[64] The definition of high-risk AI systems, as specified in Annex III of the Act, includes systems used for migration and law enforcement, both areas that are governed by the Public Service (specifically, the Department of Justice). While welcome, AI used in these contexts should be carefully regulated and subject to human oversight, particularly if applied to the granting and administration of legal aid[65] or the administration of justice. The Act's risk-based framework will provide crucial guardrails within which the Government can accelerate leveraging AI to improve efficiencies and outcomes in the Public Service.

Page 11 of the Strategy includes a commitment to assist employers to expand workplace-focused AI upskilling and reskilling. The Law Society welcomes this commitment and believes that the introduction of national competent authorities under the Act will assist the implementation of this commitment as these authorities will be equipped with the tools necessary to aid with the upskilling and reskilling of Ireland's economy towards AI.

C. Enablers for AI

There are four Strands under this heading. These are "A strong AI innovation ecosystem" (Strand 5), "AI education, skills and talent" (Strand 6), "A supportive and secure infrastructure for AI" (Strand 7) and "Implementing the Strategy" (Strand 8).

[64] Including:
(a) what appropriate safeguards are needed to ensure a secure system for AI development and use in the public service,
(b) The approach to developing and promulgating principles for trustworthy AI which will apply to all AI developed for and used by the Public Service,
(c) The development needs for AI talent in the Public Service,
(d) Opportunities for public procurement of AI, using public purchasing power to drive innovation and growth in the development of ethical and trustworthy AI.

[65] See https://www.lawsociety.ie/gazette/top-stories/2024/may/human-oversight-key-to-fair-use-of-ai-in-legal-aid

This submission has already discussed means by which the Government's implementation of the AI Act can boost a strong AI innovation ecosystem focusing on SMEs, including permitting SMEs access to regulatory sandboxes and aiding them in upskilling/reskilling. As noted before, the AI Act intends to enhance cross-border cooperation between Member States on AI. This international collaboration will greatly assist in the development of tools and methodologies to develop a framework for trustworthy AI governance (Page 19 of the Strategy). Ireland already has a good record of cooperating with other EU Member States, including on data protection matters and enforcement via the European Data Protection Board: this level of cooperation should be continued and expanded by the Government in the area of AI given its strong contemporary relevance and potential impacts on fundamental rights.

The Law Society notes that the Government has also committed to encouraging higher level education institutions to take a coordinated approach to delivering AI education and training.[66] As a leading provider of higher level legal education, the Law Society welcomes this commitment and looks forward to cooperating on this coordinated approach in the future. It is noted that the configuration of national competent authorities under the AI Act will be important for this goal as these will likely be the primary organisation(s) steering this coordinated approach.

It is important that any national competent authorities receive the necessary funding and access to expertise so that their efforts to provide for AI education at higher level are successful. It is also acknowledged that the Government is undertaking the drafting of guidelines for teachers and other educators outside of higher level education.[67] These guidelines are being informed through discussion with other Member States, a trend that should continue in all aspects of the implementation, enforcement and development of AI regulation giving the inherent benefits of pooling resources particularly with larger Member States.

The AI Act gives Ireland substantial leeway to figure out the ideal configuration of national competent authorities, meaning that Ireland has the freedom to pursue the ideal infrastructure for AI regulation. Part of this secure infrastructure is physical infrastructure. As the Strategy notes, it aims to provide "*sufficient computing power and storage capabilities*" for the development and operation of AI. As noted in the answer to Question 3, there are some concerns about the suitability of Ireland's energy infrastructure that may limit the capability of the jurisdiction to fully embrace its potential as a leader in AI technologies. Over time, it is likely that newer AI models will become more and more efficient and environmentally friendly but this will not occur without a strong focus on the part of the Government in regulating the energy and water usage of these technologies. Fortunately, the AI Act provides a toolset of environmental impact assessments that must be utilised by the Government to help adapt Ireland's infrastructure to this new, fast-growing technology.

[66] See https://www.gov.ie/en/press-release/87b43-minister-foley-pledges-commitment-to-establishing-guidelines-on-the-use-of-ai/

[67] See https://www.irishexaminer.com/news/arid-41365471.html

Conclusion

With this submission, the Law Society appreciates the opportunity to contribute towards the Department of Enterprise, Trade and Employment's consultation on the national implementation of the EU AI Act.

The national configuration of AI regulation is particularly important to both the interest of the legal profession and the public. Therefore, it is hoped that the Department takes into account the considerations and suggestions that are mentioned in this submission. The Law Society aims to be supportive of the considered implementation of AI into public life provided that this implementation is safe and revolves primarily around the protection of fundamental rights.

The Law Society remains available to assist the Department on any aspect of the future national implementation of the AI Act including the drafting of regulations on foot of the adoption of the Act. We are willing to meet in order to respond to any queries on the content of this submission and we will continue to make available AI in Law specialists to the Government.

For further information

Leo Twiggs
Policy Advisor
l.twiggs@lawsociety.ie

James Egleston
Policy Development Executive
j.egleston@lawsociety.ie

Blackhall Place, Dublin 7
t. 01 672 4800
e. general@lawsociety.ie