European AI Act

Ibec Priorities

Contents

Key Messages

Ibec support a proportionate, human-centred approach to the governance and regulation of AI development and adoption, based on evidence and risk. We broadly welcome the Commission intention to take a risk-based approach in the proposed AI Act.

Ibec encourage co-legislators to assess potential administrative and compliance burdens, particularly for SMEs and corporations deploying AI in a low risk setting or where AI is a minor or ancillary feature of a service offering or unwanted consequences in the proposed AI Act which could discourage investment in the development and deployment of AI systems that consequently hurt Europe's twinned Green and Digital transitions and its competitiveness.

Specifically:

- Ensure that the focus is where the most widespread and significant societal damage are likely to arise, particularly in proposals around the definition of AI systems, the allocation of responsibilities between different actors in the AI value chain, criteria for determining prohibited practices and the classification of high-risk systems.
- Use the definition proposed by the High-Level Expert Group on AI, focusing on AI systems that display intelligent behaviour and take actions with some degree of autonomy. The current proposed definition of "AI systems" is too broad.
- Refine the proposed classification rules for high-risk AI to ensure consistency with sectoral legislation in Annex II. The AIA should only regulate high-risk AI applications in areas where a clear regulatory gap has been demonstrated.
- Reassess and clarify responsibilities of different actors in the AI value chain to ensure obligations are allocated to the actors that can ensure compliance.
- Ensure the proposed compliance framework is proportionate and flexible.
- Ensure EU standardisation activity on AI is aligned with international efforts.
- Support and embed the use of sandbox schemes, with well-established criteria to ensure an effective access by businesses, particularly SMEs. Support controlled experimentation to assess (yet unforeseeable) risks and locate potential legal barriers and inconsistencies.
- Support and enable efficient co-operation between relevant regulators at national and EU level to prevent divergent opinions, interpretations, and decisions as well as fragmentation in the internal market.

Introduction

The shape of Europe's digital future matters. Ibec envisage a more competitive, smarter low carbon economy, with a sustainable enterprise base that provides quality jobs and enables a high quality of life. We envisage an outward looking, dynamic, and successful EU, that provides the conditions for organisations and individuals to adapt to technological change and reach their full potential. Under the right conditions, Artificial Intelligence (AI) represents a suite of transformative technologies or systems that can enable that vision. Developing a strong European data economy and ensuring excellence and trust are crucial to that success.

Ibec has engaged in EU and national consultative processes on AI policy and governance, including the European Commission White Paper on Artificial Intelligence (AI)[1] and the development of Ireland's recent National AI Strategy[2].

This paper presents initial Ibec comments to EU co-legislators on the further development of the European Commission's proposed legislative framework on Artificial Intelligence (AI), known as the 'AI Act (AIA)'[3].

General Comments on the proposal

Ibec support a proportionate, human-centred[4] approach to the governance and regulation of AI development and adoption, based on evidence and risk. We broadly welcome the Commission's intention to take a risk-based approach in the proposed AI Act. The heterogenous nature of AI and its applications means a one-size-fits-all approach would be problematic or risk stifling the desired opportunities. It is important to clearly define further appropriate safeguards needed for sensitive use cases whilst continuing to encourage innovation. While costs of high-risk AI should be considered, the cost of not enabling further AI innovation in addressing economic and societal challenges should also be considered.

[1] Implementing an open European digital future - Ibec response to the European Commission White Paper on Artificial Intelligence

[2] Smarter technology for a better future - Irish business priorities for a national AI strategy

[3] Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM (2021) 206 final

[4] Principled approach outlined by the European Commission's High-Level Expert Group on AI ('AI HLEG') and OECD that encourages beneficial outcomes from AI for both humans and the planet that sustains them. This approach encourages a respect for law, human rights, and democratic values as well as a consideration for the natural environment and sustainability.

There are already many regulations and legal codes that are technology neutral in nature, and thus already apply to AI[5], but it is important to evaluate if there are gaps in the context of specific demonstrable risk.

Any gaps identified should be addressed via practical, proportionate, principles-based rules which build on existing legislation, and address demonstrable high risk, to avoid creating overly complex or conflicting legal obligations. It is crucial to ensure consistency and synergy between this proposal and the broader EU legislative framework[6].

[5] For example, the framework provided by the General Data Protection Regulation (GDPR), the Product Liability Directive (PLD), and the General Product Safety Directive (GPSD).

[6] E.g., General Data Protection (GDPR) for all the data and record-keeping provisions, the EU Cybersecurity Act regarding cybersecurity measures and incident notifications from AI systems providers and ongoing discussions on the proposed General Product Safety and Machinery regulations.

Specific comments and recommendations on elements of the proposal

I. General Provisions

We agree that the AIA should focus on applications of AI systems which pose a demonstrable high risk of causing damage to humans or have a detrimental impact on fundamental human rights, based on objective, clear and unambiguous criteria.

Recommendations to co-legislators:

1. **Clarify the extraterritorial applicability of the AIA (Art. 2) and future EU collaboration with international partners regarding the global governance of AI**. We understand a desire to offer extra-territorial protection to EU citizens but believe there is a risk of uncertainty for firms operating internationally. Recital 11 states that '*certain AI systems should fall within the scope of this Regulation even when they are neither placed on the market, nor put into service, nor used in the Union'*.

2. **Ensure the AIA is focussed on high-risk AI systems. Further clarify its proposed definition of AI, the criteria for determining prohibited practices and the classification of high-risk AI systems, to focus on where most widespread and significant damage is likely to arise.**
    - Exclude simple supervised machine learning and focus on AI systems that can take actual decisions with a degree of autonomy.
    - Use the definition of AI suggested by the High-Level Expert Group on AI: *"Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals".*
        - The proposed definition of an "*Artificial Intelligence System*" in Article 3(1) and the list of techniques listed in Annex I of the AIA are too broad.
        - The proposed AIA definition of AI would likely include most contemporary software and applications that use pure statistical and knowledge-based approaches for conventional data analysis that have little impact on individuals, such as AI methods for internal modelling needs (e.g., Asset and Liability Management models for the banking sector), for corporate scoring or for industrial issues. This proposal would create legal uncertainty, if companies are required to assess if their software, which conventionally would not be considered an AI system, may still fall within this legislation's scope.

3. **Use an ordinary legislative procedure for proposed adjustments to the definition of AI**. Art 4 provides for the use of delegated acts in amending Annex I. Delegated acts typically enable the Commission to 'supplement or amend certain non-essential elements' of an EU legislative act[7]. We understand a desire to accommodate technical progress, however the definition of AI is fundamental to this proposal.

II. Prohibited AI Practices

Recommendation to co-legislators:

4. **Acknowledging the ambition to prohibit certain very high-risk AI applications that represent a demonstrable threat to human health and rights, provide further legal certainty**:
    - Clarify what is meant by '*deploying subliminal techniques', 'detrimental or unfavourable treatment' and "psychological harm".*

III. High-Risk AI Systems

Chapter 1: Classification of AI Systems as High-Risk

Recommendations to co-legislators:

5. **Enhance legal certainty and proportionality in the classification of high-risk AI systems**. Promote further AI adoption and innovation.
    - **Refine classification of high-risk AI to ensure consistency with sectoral legislation in Annex II. Focus where there are demonstrable regulatory gaps using a targeted risk-based approach.**
        - EU product harmonisation legislation in Annex II is effectively addressing risks linked to certain industrial AI applications.
        - We have a concern that the proposal regarding safety components of regulated products (Annex II) could:
            - Create conflicting requirements and uncertainty between a new AI framework and sector-based regulation. The proposed AIA modifies key concepts and definitions of the New Legislative Framework (NLF) for products (e.g., concepts of "*putting into service*").
            - Risk misalignment and duplication in the case of the Medical Devices Regulation (MDR) and In-vitro Diagnostics Regulation (IVDR).

[7] Art. 290(1) Treaty on the Functioning of the EU (TFEU)

- **Focus the scope of application of Annex III further, based on clear, evidence-based, and objective criteria.**
    - While acknowledging the need for specific requirements for certain standalone AI uses, we have a concern that the proposed scope of stand-alone high-risk AI applications (Annex III) is broad. Risk may depend on context and whether the AI system takes the final decision. A blanket approach undermines proportionality. The scope of application should be refined further according to the risks posed to fundamental rights and health and safety.
        - Avoid unintended inclusion of non-critical systems or ancillary use of AI systems which pose no safety risk. For example, Annex 3(2) on the "management and operation of critical infrastructure", could unintentionally include non-critical systems such as AI-supported office management solutions.
        - The very broad definition of AI used in "*employment, self-employment or workplace context*" will hinder the application of AI in human resources processes, where they can be used to enhance productivity, promote diversity, and augment human abilities, to the benefit of both employers and workers. If there are concerns about the use of AI in specific processes for example recruitment and termination, then the scope should be limited to those specific use cases[8].
        - The broad definition of "*AI systems used to evaluate the credit score or creditworthiness of natural persons"* could slow down the process for accessing small loans for individuals and small businesses and undermine competition from smaller entities providing financial services as auxiliary features.
    - **Clarify the criteria and specific triggers that would enable the European Commission to update the list of high-risk AI systems (Annex III) through delegated acts (Art. 7). Enhance legal and hence market certainty.**
        - For example, Article 7(b) could further clarify cases regarding *"adverse impact on fundamental rights*".
        - Introduce provisions for Member States and industry involvement in any future process for updating the list (e.g., by renewing the mandate of the High-Level Expert Group on AI).

[8] Note the European Social Partners' Autonomous Agreement on digitalisation (2020) already sets out some direction and principles of how and under which circumstances AI is introduced in the world of work.

Chapter 2: Requirements for High-Risk AI Systems

Recommendations to co-legislators:

6. **Take a principled approach to proposed requirements (i.e., market access conditions) for high-risk systems.** Requirements should:
   - Be risk-based and proportionate;
   - Be flexible to adapt to evolving knowledge and organisational models;
   - Ensure a level pitch by being non-exclusionary to SMEs and start-ups; and
   - Identify and allocate clear responsibilities in the AI value chain.

7. **Support the Commission's intention to provide guidance on how to implement risk management systems for high-risk AI systems in Article 9. Provide further focus.**
   - Align the AIA with the core New Legislative Framework (NLF) principles[9]. Focus on the desired outcome of risk assessment and management systems. Enable industry to design systems and adapt them to their internal operations and structure, through state-of-the-art standards.
   - Specify the type of risks providers should consider when assessing and taking steps to mitigate risks. While some Recitals (e.g., 27 and 43) indicate that the goal of the Regulation is to mitigate risks to *"health, safety and fundamental rights,"* Article 9 offers no guidance on what specific risks need to be considered by the risk management system.
   - Further clarify the interplay between the risk-management system and other requirements set in chapter 2.

8. **Enable impacted sectors to integrate the risk management for systems classified as high-risk AI into existing risk management processes to reduce regulatory burden**. Credit institutions are to be allowed[10] to integrate the required risk management system into risk management processes prescribed by the sector-specific legislation[11]. Expand this to other sectors.

9. **Support measures to enhance the quality of training data (Art.10).**
   - Ibec support enhanced data quality, availability, access, and collaboration to enable further digital transformation in addressing both societal and economic challenges across Europe. See separate Ibec papers on priorities for EU data governance[12].

[9] Aims to improve the internal market for goods by improving market surveillance and boosting the quality of conformity assessments.

[10] Art. 9(9)

[11]Directive 2013/36/EU

[12] Ibec priorities for the EU Data Governance Act (June 2021) and Ibec response to European Commission consultation on its European Strategy for Data (2020).

   - Focus on the general output and compliance of an AI system with legal requirements, rather than laying out the specifics of their technical realisation.
     - The proposal[13] states that "*training, validation and testing data sets shall be relevant, representative, free of errors and complete*", which would be unworkable in practice, given the degree of variance in data sets, and would prevent the use of real-life data.
     - Pursuing "zero-risk" circumstances is impractical and, given potential penalties in the event of non-compliance, will not foster innovation in European AI.
     - A pragmatic approach to data quality could be realised through 'best efforts', or the use of state-of-the-art standards[14] to preserve privacy and security in data management

10. **Ensure technical documentation requirements (Art. 11) are proportionate and appropriate to the use case**.
    - Technical specifications stipulated prior to market entry might not be relevant at later stages of an AI's lifecycle since operational environments of AI applications may vary based on context.
    - The information interests of the addressees of the technical documentation must be balanced carefully against the intellectual property protection needs of the company concerned. The contents of technical documentation specified in Annex IV are expansive. The detailed description of the "elements of the AI system" required under item 2 b), may constitute trade secrets.

11. **Determine record storage requirements based on risk, business needs, capabilities, and informational value**. We acknowledge the need to keep records, documentation, and where relevant datasets (Art. 12) in identified high-risk cases. However, record keeping requirements should avoid unnecessary regulatory burden, while enabling effective enforcement. For example, datasets used to generate a model collected in the early stages may not be pertinent when the damage occurs, since it will have been consequently altered, modified, or even removed in the interim. If a storage time is stipulated we propose that the retention periods should not exceed a maximum 10 fiscal years and is in conformity with established auditing standards and actual practices in each sector.

12. **Provide further clarity for providers and users on the criteria in Article 13 (transparency and information provision to users)**
    - Keep the information for use manageable and comprehensible in practice.

[13] Article 10(3)

[14] ISO/IEC 25024 "*Measurement of data quality*", ISO/IEC 25012 "*Data quality model*" and ISO/IEC 24745 "*Performance testing of biometric template protection schemes"*

- It is unclear if very detailed and technical information (e.g., regarding the test data used) offers practical information value for the users of a AI system.
- Limit requirements in Article 13 (3) to essential information (e.g., special risks in the event of non-intended use of the AI system).
- Focus on providing users with instructions on how they can test the accuracy of a system in a deployment setting, for instance by providers making tools available to users to help them assess their own outcomes and incorporating testing capabilities into the system. Much will depend on the quality of data input by users, the circumstances of its use, and the ways in which users operate the system.

13. **Ensure a proportionate and practical approach in enabling human oversight in Article 14**. The approach in determining the format and stage of human oversight should be outcome driven and dependent on the intended use and associated impacts.
    - Ibec support human-centric AI and acknowledge the need for an appropriate level of human oversight of high-risk systems. However, instructions to users and requirements to "*fully understand the capabilities*" of AI systems appear to set an overly high bar and may not be useful to the average user. The aim should be to have an appropriate understanding of the capabilities and limitations of the system.
    - Certain AI controlled machines (e.g., in a factory context) can provide higher safety and lower accident rates with built-in risk prevention measures compared to having human oversight.

14. **Clarify requirements for accuracy, robustness, and cybersecurity in Article 15**.
    - Further consider the evolving nature of AI and capacities to influence in the AI value chain.
        - We acknowledge that trust for certain AI may rely on ex-ante consideration of the risks they may generate.
        - But determining the entire potential of the AI’s lifecycle ex-ante doesn’t reflect AI which learns continuously. Many AI systems placed on the market learn from the end user, and most often the influence shifts from the business considering risks at the ex-ante phase to the end-user or operator.
    - Further clarify what constitutes an "*appropriate level*" of accuracy, robustness, and cybersecurity (Art. 15). Compliance with such requirements should be linked to the implementation of measures in accordance with the "state of the art" and context. Ensure coherence with cybersecurity requirements across EU legislation e.g. Regulation (EU) 2019/881.

Chapter 3: Obligations of Providers and Users of High-Risk AI Systems and Other Parties

Recommendations to co-legislators:

15. **Ensure a proportionate balance in responsibilities between actors in the AI value chain in Article 16,** especially in the provision of general-purpose tools and Application Programming Interface (APIs) and open-source AI models**.**
    - Proposed obligations on providers appear to extend beyond placing on the market throughout the entire life cycle of an AI system. This is a challenge where providers don't exercise control over systems throughout their lifetime and in the provision of general-purpose tools and Application Programming Interface (APIs) and open-source AI systems that are not intended for high-risk AI, but may be subsequently used by third parties in a way that may be considered in scope of AIA requirements as high-risk AI (e.g., open deep fake detection API that is used by law enforcement).
    - Clarify responsibilities of different actors in the AI value chain to ensure obligations are allocated to the actors that can ensure compliance.

16. **Enable impacted sectors to integrate quality management issues for systems classified as high-risk AI (proposed in Art. 17) into the robust risk management process (proposed in Art. 9) and existing quality management processes to reduce regulatory burden**.
    - Quality management is assumed with the proposed Article 9. Avoid duplication and unnecessary cost in inadvertently developing siloed risk and quality management processes. Enable all sectors as in Recommendation no. 8 of this paper above.

17. **Ensure balance between regulators' information requests and intellectual property and contractual protections.** Enable effective co-operation with competent authorities and enforcement (Art. 23).

18. **Exempt product manufacturers from certain obligations (Art. 24) in cases that can only be addressed by the provider of an installed AI system** e.g., provision of technical documentation (Art. 16).

19. **Clarify responsibilities of different actors in the AI value chain to ensure obligations are allocated to those that can ensure compliance (Art. 28)**. Enable the freedom for actors to use contractual freedom to allocate responsibilities.

Chapter 4: Notifying Authorities and Notified Bodies

Recommendation to co-legislators:

20. **Engage industry and regulators to ensure the requirements of the AIA are in line with the available testing capacities**. Sufficient testing capacities are key to rapid market access of AI systems.

Chapter 5: Standards, Conformity Assessment, Certificates, Registration

Recommendations to co-legislators:

21. **Ensure EU standardisation activity on AI is aligned with international efforts (Art. 40).**

22. **Prioritise the New Legislative Framework (NLF) of consensus-based, harmonised standards as well as international standards over technical specifications in implementing acts (Art. 41)**.
    - European and international standards are developed by experts where market demand and high-level knowledge for such standards exists. Their use can facilitate enhanced product safety and/or interoperability.
    - As proposed, the European Commission could adopt common specifications, through implementing acts, in respect of the requirements in Chapter 2. Such an approach should be exceptional and under conditions where standardisation is shown to be inappropriate. If adopted, relevant stakeholders should be engaged in the development of such common specifications.

23. **Provide further clarity and flexibility in conformity assessment (Art. 43)**.
    - Provide further flexibility and resources to take account of evolving expertise and infrastructure in the compliance assessment framework for AI. Avoid disparities in enforcement.
        - Conformity assessment based on internal control referred to in Article 43 is welcome.
        - The expertise in auditing standalone AI systems is evolving.
    - Further clarify the concept of "*substantial modification*" (Art. 43 (4)), under which a new conformity assessment is required as some AI systems may continue to learn after being placed on the market or put into service.

24. **Adapt CE marking to AI systems and its digital nature**. The proposed Article 49 (CE marking of conformity) appears to be based on traditional product safety requirements.

25. **Reconsider the proposed introduction of an obligation for registration of certain AI systems (Art. 51).**
    - Such an obligation is neither an element of conformity assessment under the NLF nor proportionate, considering the information that must be provided together with the registration according to Annex VIII.

IV. Transparency Obligations for Certain AI Systems

Recommendations to co-legislators:

26. **Ensure transparency obligations are targeted, proportionate and reflects differences between systems.**
    - Many firms are proactive in providing transparency on certain AI systems.
    - Ensure consistency with other legislative acts on transparency e.g., Digital Services Act[15].
    - Clarify the scope of transparency obligations (Art. 52) in relation to "*AI interacting with natural persons*", given AI is integrated in many user-facing systems, e.g., providing directions, recommendations, and predictions.

V. Measures in Support of Innovation

Recommendations to co-legislators:

27. **Strengthen the provision for AI regulatory sandboxes (Art. 53)**.
    - Support the use of regulatory sandboxes[16] to test and scale up research as appropriate[17]. Enable shared learning between innovators, regulators, and enterprise - both large and small. Regulatory sandboxes offer an opportunity for capacity building within regulators as much as enabling further beneficial trustworthy digital innovation across Europe[18].
        - Consider making this voluntary provision an obligation for Member States. Europe is successful in research output in AI. However, there is more to do in linking this to delivery of business needs and in co-ordinating efforts between Member States.

[15] Ibec priorities on digital services package (May, 2021), including transparency in the Digital Services Act (DSA).

[16] A regulatory sandbox or "testbed" is a framework "organised and administered" by a relevant regulator on a "case by case" basis that offers participating public or private organisations a strictly limited flexibility to test new products, services, or business models with reduced regulatory requirements; and "includes mechanisms to ensure regulatory objectives" (Attrey et al., 2020).

[17] Ibec (2020) https://www.ibec.ie/-/media/documents/influencing-for-business/digital-policy/ibec-open-digital-future-ai-paper.pdf

[18] Regulators and participants point to several 'sandbox' benefits including, enhanced accountability; greater knowledge sharing; enhanced ability of innovators to attract finance; and supporting public value projects (Attrey et al., and ICO, 2020).

- Encourage Member States to ensure national competent authorities (Article 59) that will establish and oversee regulatory sandboxes or similar frameworks are adequately resourced for such a task and share experiences.
    - This investment should be considered cost neutral in the long run. Adequate resources are certainly important in acquiring and developing regulators' capacities on AI. However, so could the experience and incremental learning that regulatory sandboxes can offer.
    - Shared experience can encourage a uniform approach across the digitalised single market[19].
- Engage industry and innovators in the establishment of regulatory sandboxes (Art. 53(6)).
- Safeguard the experimental nature of sandbox schemes to ensure their practicality and encourage uptake[20]. Very high compliance requirements within sandboxes schemes would hamper effective innovation. Businesses must be able to experiment in a flexible but controlled manner.

28. **Support and broaden measures in Article 55.**
    - Support measures that reduce the regulatory burden for small scale providers and users. Expand such measures given that several large organisations treat their innovation labs as start-ups.

VI. Governance

Chapter 1: European AI Board

Recommendations to co-legislators:

29. **Ensure the European AI Board has adequate resources**.

Chapter 2: National Competent Authorities

Recommendations to co-legislators:

30. **Encourage Member States to ensure national competent authorities (Art. 59), designated to enforce the AIA, have adequate resources**.

[19] There is a variance in approach, due in part to the case-by-case nature of regulatory sandboxes. Nevertheless, regulatory sandboxes share some common features: demonstrable innovation and societal benefits; defined temporal or sectoral limits; and safeguards "to ensure regulatory objectives" (Attrey et al., 2020).

[20] https://data.consilium.europa.eu/doc/document/ST-13026-2020-INIT/en/pdf

VIII. Post Market Monitoring, Information Sharing, Market Surveillance

Recommendations to co-legislators:

Chapter 1: Post Market Monitoring

Recommendations to co-legislators:

31. **Limit requirements (Art. 61) to those that can actually be fulfilled by a provider of high-risk systems**. Such monitoring may be challenging in cases of a product with an integrated AI system. In addition, many systems placed on the market learn form the end user or operator.

Chapter 3: Enforcement

Recommendations to co-legislators:

32. **Enable a right to challenge the necessity and proportionality of access to data and documentation by market surveillance authorities (Art. 64).**
    - Providers might not retain control of a dataset over the AI lifecycle.
    - Providers should not be required to violate EU, Member State, or applicable third-country laws in providing access to Market Surveillance authorities.

33. **Avoid fragmentation of the digitalised single market and a harmonised AIA**. Clarify the procedure for dealing with AI systems presenting a risk at national level (Art. 65 and 67).
    - Market surveillance authorities, in any Member State, appear able to order the withdrawal of a high-risk AI system from the market, even if the system fully complies with the Regulation, in cases where the system "presents a risk to the compliance obligations under Union or national law intended to protect fundamental rights or to other aspects of public interest protection" (Art. 67(1)).
    - We recommend a harmonised application of the AIA and further clarity on this procedure to avoid market uncertainty or fragmentation.

IX. Code of Conduct

Recommendations to co-legislators:

34. **Encourage a bottom-up, outcome-driven approach that reflects global standards in developing codes of conduct.** Use the principles: inclusiveness, consensus, transparency, effectiveness, technology neutrality, and impartiality. This will ensure we can encourage and benefit from trustworthy AI outside the EU but also that AI developed within the EU can move across borders easily.

- Voluntary codes of conduct (Art. 68) can enhance trust and foster uptake of AI applications that do not qualify as high-risk.
- Non - ‘high-risk” AI should not be subject to the same mandatory requirements for high-risk AI systems set out in Title III, Chapter 2 of the proposal. Codes of conduct using stringent legal requirements are inappropriate for lower-risk applications, burdensome, and unlikely to incentivise industry participation or provide clarity for users.

X. Confidentiality and Penalties

Recommendations to co-legislators:

35. **Strengthen provisions on confidentiality (Art. 70). Ensure permission to exchange information with third countries is consistent with EU-third country trade agreements. Safeguard innovation.**
    - Article 70 of the AIA does not appear to specify technical and organisational requirements that receiving authorities and notified bodies must comply with in the confidential treatment of sensitive data and trade secrets, apart from the definition of general protection objectives (e.g., protection of "*intellectual property rights*" in Article 70 (1) (a)).

36. **Review the proportionality of the proposed sanctions regime (Art. 71).**
    - Sanctions proposed in the AIA exceed the sanction regime in the GDPR (Article 71(3)).
    - Further define triggers for sanctions. Ensure uniform interpretation and application of the sanction regime and avoid fragmentation of the digitalised single market.

About Ibec

Ibec is Ireland’s largest lobby group and business representative. We campaign for real changes to the policies that matter most to business. Policy is shaped by our diverse membership, who are home grown, multinational, big and small and employ 70% of the private sector workforce in Ireland. With 38 trade associations covering a range of industry sectors, 6 offices around Ireland as well as an office in Brussels. With over 240 employees, Ibec communicates the Irish business voice to key stakeholders at home and abroad. Ibec also provides a wide range of professional services and management training to members on all aspects of human resource management, occupational health and safety, employee relations and employment law.

www.ibec.ie/digitalpolicy
@ibec_irl
Connect with us on LinkedIn