Interpreting the EU AI Act for Industry

Introduction

Artificial intelligence (AI) stands as a transformative force that is re-shaping industries, enhancing human capabilities, and driving economic growth. However, as AI's reach extends more into our daily lives the need for responsible and ethical AI governance and regulation has increased in importance.

Measures like the proposed EU AI Act present a significant factor that businesses need to understand and navigate. This landmark piece of legislation seeks to regulate AI applications and ensure their ethical and trustworthy use. While these regulations might appear challenging for organisations by potentially limiting the use of certain data sets and introducing measures like watermarking for AI-generated content, they are not insurmountable obstacles. Coupled with strict data privacy norms akin to GDPR, these regulations require businesses to adapt and innovate, rather than obstruct progress. To lead the way, organisations will need to ensure they have a deep understanding of regulatory guardrails.

The SFI ADAPT Centre for AI-Driven Digital Content Technology regognises the profound impact of the EU AI Act on industry and we work with organisations to harness the potential of AI while ensuring compliance and offering insights into its implications for industry. Our experts in AI, law, and policy come together to explore key aspects of the regulation and provide practical guidance to help organisations navigate the intricacies of the legislation.

We hope this information will provide a valuable bridge between academic research and our industry collaborators seeking to understand and guide the impact of AI technologies on their organisations.

To learn more about the ADAPT Centre, visit www.adaptcentre.ie

Focus on Research
Trustworthiness in ADAPT's AI Research

At the ADAPT Centre, we understand that the ethical dimensions of AI and trustworthy AI engagement are critical for the responsible development and deployment of AI technologies. Our approach to addressing technology ethics and trustworthy AI issues is driven by a commitment to equip researchers with the knowledge and tools necessary to navigate this complex landscape effectively. Our goal is to empower researchers to incorporate assessments and treatments of technology ethics risks into their publications, meeting the growing demand for such considerations in calls for papers.

Our dedicated research team at ADAPT has seen substantial growth in the field of AI/data ethics, with publications and PhD topics covering a wide range of areas such as machine translation, data governance, digital forensics, digital health, diversity and gender, human-computer interaction, transparency, accountability, social science practice, standardisation, self-tracking, and smart manufacturing. Many of our ongoing projects incorporate ethical assessments, analyses, or the development of ethical practices and tools.

As we move forward, our commitment to AI technology ethics remains unwavering. We recognise the importance of moving beyond performative ethics towards a more effective ethics of AI.

This involves crafting AI tools tailored for specific domains, revising professional practices, and instituting stringent regulatory and accountability structures. We believe in fostering transparent and meaningful dialogues with all stakeholders, ensuring that our research is both responsive and responsible.

The ADAPT Centre is dedicated to shaping the future of AI technology ethics, and we invite you to join us on this journey towards responsible and impactful AI innovation.

AI Technology Ethics within ADAPT's Research Programme

ADAPT researchers have identified a gap in societal expectations of AI and AI in practice, with the need to move from a performative to a truly effective AI ethical framework which recognises its limitations and the significant human labour it requires.

Effective AI ethics requires domain appropriate AI tools, updated professional practices and robust regulatory and accountability frameworks.

To further enhance ethical AI and data management within organisations, we recommend:

- engagement with governance and regulation;

- adoption of specific governance measures;

- monitoring and enforcement of those measures;

- and an iterative approach to updating measures.

**Click here to access the
ADAPT Ethic Canvas**

ADAPT Contribution to International AI Standards on Trustworthy AI

Challenge

The last five years have seen a fast-growing international recognition of both the economic benefits of AI and its potential for societal harm including through perpetuation of the unwanted bias, loss of control in safety-critical settings, loss of personal autonomy from automating content and opportunity routing and labour displacement through work automation. This promoted a global demand to move towards enforceable regulation in various jurisdictions that require international AI standards, conformance to which support the technical compliance to such regulations.

Response

ISO is the primary source of international standards, supporting regulatory compliance. Via the ISO-IEC Joint Technical Committee on ICT, a new international standardisation sub-committee on AI was formed - SC42. ADAPT collaborated with the National Standards Authority of Ireland (NSAI) to lead Ireland's significant contribution to SC42, acting as convener of its central Trustworthy AI working group and co-hosting its third international plenary meeting in Dublin.

Engagement

ADAPT researchers have contributed to SC42 standards as a lead editor to its Big Data Reference Architecture and technical contribution to standards on AI concepts and Terminology, Trustworthy AI, Governance of AI, AI Risk Management, AI Management Systems, AI Ethical and Societal Issues and AI Transparency.

Impact

ADAPT's contribution has improved the cohesiveness of the role of societal stakeholder engagement in AI management and governance processes and the semantic integrity and interoperability of concepts used, especially those related to knowledge engineering and NLP.

Next Steps

The EC has now requested that the European standards bodies CEN and CENELEC provide the harmonised standards that organisations will need to comply with the proposed EU AI Act. ADAPT researchers are contributing to the committee that is adapting SC42 standards for this purpose and making new research contributions on open, semantic analyses of how these standards satisfy the EU AI Act requirements, building on unique experience with similar mapping for GDPR.

TAIR (Trustworthy AI Requirements Ontology) Project

The TAIR Project, spearheaded by the ADAPT Centre, stands at the forefront of integrating AI standards and legal compliance, playing a crucial role in the evolving landscape of AI governance. With the upcoming AI Act set to establish a robust legal framework for AI technologies, standards are poised to play an indispensable role in ensuring trustworthy and compliant AI practices. The TAIR Project addresses this need by creating a comprehensive mapping between the AI Act and various management standards, providing clear and actionable guidance on how to align AI systems with legal requirements. ADAPT researchers are contributing to the development of standards that are not only technically sound but also legally robust, ensuring that AI technologies are deployed in a manner that is safe, transparent, and accountable.

Click to view diagram

ADAPT's
Discovery Experience

We know how to make AI impactful for your business
Take the right first steps in innovation and regulation, come on the journey with ADAPT

Roadmap

Develop and validate a credible plan for research-enabled innovation: Detailing your business challenges, research and innovation opportunities and the expected impact

Understand

Get the right experts around the table to understand your challenges and objectives

Ideate

Explore opportunities for multi-disciplinary impact with state-of-the-art AI and computer science research relevant to your business

Innovation through collaboration is best.

Gain access to over 350 research experts from diverse fields who are ready to be part of your innovation journey

CE Mark for AI Systems:
An extension of product safety law to artificial intelligence systems

The proposed AI Act includes the provision for use of the CE mark which is a well established method for indicating product safety. While the AI Act makes it an obligation for potentially risky applications to obtain a CE mark, we can foresee the use of the CE mark and similar certification mechanisms become a common practice within the AI value chain to communicate assurances and establish trust.
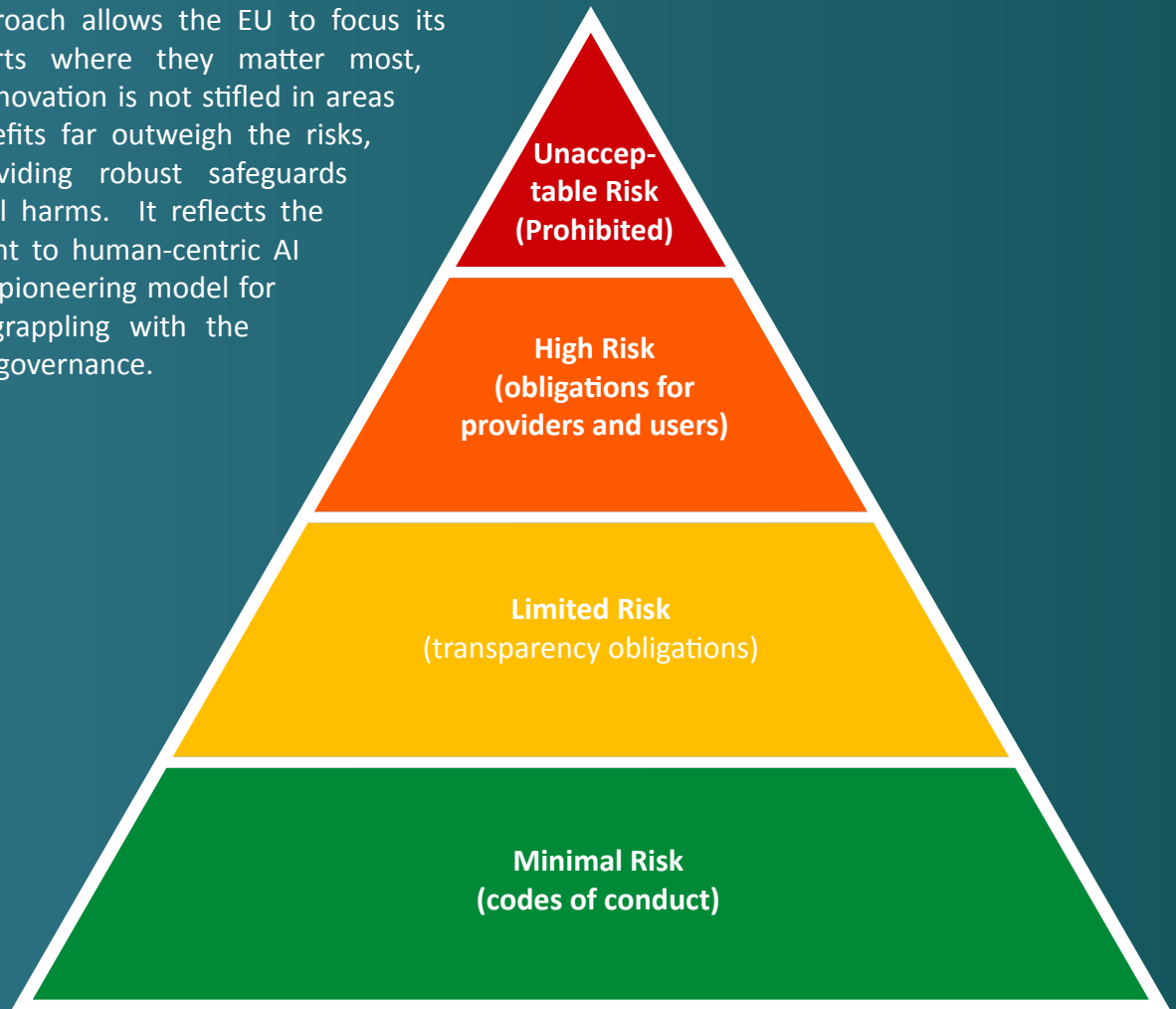
The EU AI Act's Risk-Based Approach to Regulating AI

In the draft, the Commission follows a graduated approach based on possible threats to EU values and fundamental rights.

This tiered approach allows the EU to focus its regulatory efforts where they matter most, ensuring that innovation is not stifled in areas where AI's benefits far outweigh the risks, while still providing robust safeguards against potential harms. It reflects the EU's commitment to human-centric AI and serves as a pioneering model for other nations grappling with the challenges of AI governance.

Unaccep-table Risk (Prohibited)

High Risk (obligations for providers and users)

Limited Risk (transparency obligations)

Minimal Risk (codes of conduct)

What constitutes high-risk AI?

In order to classify the risk level of an AI system, the purpose of the system needs to be examined. There are two criteria

- AI systems are considered high-risk if they are intended to be used as safety components of products covered by one of the CE standards listed in Annex II of the AI Regulation.

- Stand-alone AI systems that are listed in Annex III to the AI Regulation are also high-risk AI systems. For example, this is the case of AI in the areas of biometric identification, education and training, credit and emergency services, and management and operation of critical infrastructures. In the Commission's view, these systems are particularly likely to interfere with security, health and fundamental rights.

It should be noted that the provider bears the responsibility of correct classification.

Unlock Regulatory Compliance with ADAPT's Research Tool to Assess Risk

At ADAPT, we recognise the intricacies of data regulation. To help organisations navigate the various regulations in existence, ADAPT researchers have developed a groundbreaking tool that automates risk assessments across all regulations making it easier to develop AI in the confidence of being compliant. The risk assessment tool allows organisations to navigate the complexities of data regulation, discover risks that exist and then correlate those risks with regulatory requirements.
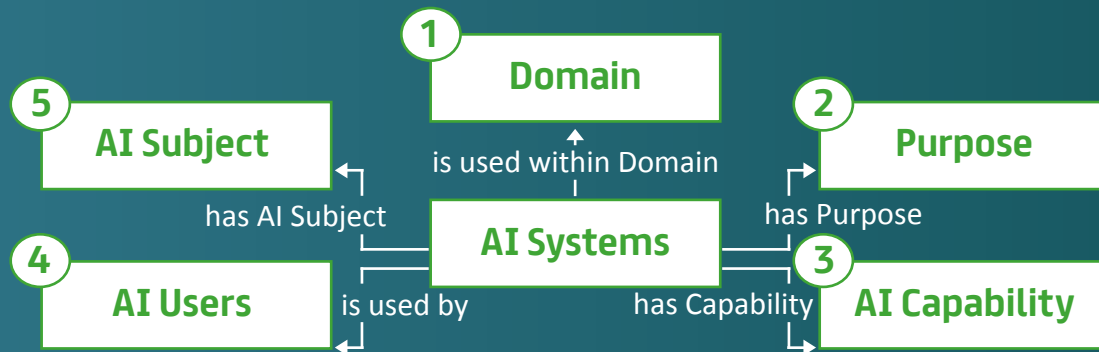
Definitions

Domain: the domain or sector or area within which the AI system is or will be deployed; e.g. Health, Education

Purpose: the purpose or end-goal for which the AI system is or will be used to achieve; e.g. Patient Diagnosis, Exam Assessment

Capability: the capability or application for what the AI system is or will be used to provide; e.g. Facial Recognition, Sentiment Analysis

User: the user or operator who is or will be using the AI system; e.g. Doctor, Teacher

Subject: the subject or individual or group which the AI system is or will be used towards; e.g. Patients, Students

[Read full research publication] [Click to use the ADAPT Centre High-Risk Tool]

Resources

Built using Open, Extensible, and Interoperable Standards

AIRO (AI Risk Ontology)

AIRO is an ontology for expressing risk of AI systems based on the requirements of the proposed AI Act and ISO 31000 series of standards. AIRO assists stakeholders in determining "high-risk" AI systems, maintaining and documenting risk information, performing impact assessments, and achieving conformity with AI regulations. AIRO is available at https://w3id.org/airo

VAIR (Vocabulary for AI Risks)

VAIR assists with identification and documentation of risks by providing a common vocabulary that facilitates knowledge sharing and interoperability between actors in the AI value chain. VAIR is available at https://w3id.org/vair

Data Privacy Vocabulary (DPV)

The Data Privacy Vocabulary (DPV) enables expressing machine-readable metadata about the use and processing of personal data based on legislative requirements such as the General Data Protection Regulation (GDPR). The DPV is a community standard and a state of the art resource that is being used by several academic projects and the industry for: Privacy Policies, Consent Records, Compliance Checking, Annotating code / documents, Risk Management, Data Breach Records, Impact Assessments (PIA / DPIA), Data Transfers, Register of Processing Activities (ROPA). Link for DPV: https://w3id.org/dpv

Read More Publications

- AIRO: An Ontology for Representing AI Risks Based on the Proposed EU AI Act and ISO Risk Management Standards

- To Be High-Risk, or Not To Be-Semantic Specifications and Implications of the AI Act's High-Risk AI Applications and Harmonised Standards

- EU's Proposed AI Act, Assessment List for Trustworthy AI (ALTAI), and ISO/IEC 42001 AI Management System

EMPOWER Data Governance

EMPOWER Data Governance is an ambitious collaborative research programme focused on addressing industry challenges across the ecosystem of data governance and data management. Tools, techniques, principles, and protocols are examined in the research programme to improve data governance in future and knowledge-driven ecosystems. It takes in the interdisciplinarity of research expertise from four SFI Research Centres: Lero, ADAPT, FutureNeuro and Insight.

The programme is providing industry with the agility to rapidly address research requirements and the ability to grow resources over the lifetime of the initiative. The vision for EMPOWER is to develop a global data ecosystem to effectively govern the vast amounts of data that move among actors within complex global information supply chains. The research will advance an alignment between business goals and societal needs to develop methodologies and tools addressing challenges around key areas such as reliability, reproducibility, privacy, provenance, consent, explainability, inclusiveness and avoidance of unfair bias.

EMPOWER'S 5 PILLARS

1. DATA MARKETS
Creates platforms to enable novel forms of data sharing in future ecosystems

2. REGULATORY SANDBOXES
Allows stakeholders to explore the impact of possible data and ethical AI regulations in a regulated sandbox.

3. PRIVACY-PRESERVING TECHNOLOGY
An innovative privacy-preserving technology that advances adaptive anonymity and differential privacy.

4. GOVERNANCE & STANDARDS
Takes into account the issues associated with data governance in inter-organisational relationships.

5. PEOPLE-CENTRIC DESIGN & ETHICS
Through a people-centric approach and ethical principles, trust is built and maintained across the entire data ecosystem.

Collaborate with ADAPT

Executive Director of Commercialisation
Declan McKibben
declan.mckibben@adaptcentre.ie
+353 (0) 87 919 2692

Senior Industry Partnership Manager
Edmond O'Connor
edmond.oconnor@adaptcentre.ie
+353 (0) 86 806 6711

collaboration@adaptcentre.ie

www.adaptcentre.ie

ADAPT Research on EU AI Act