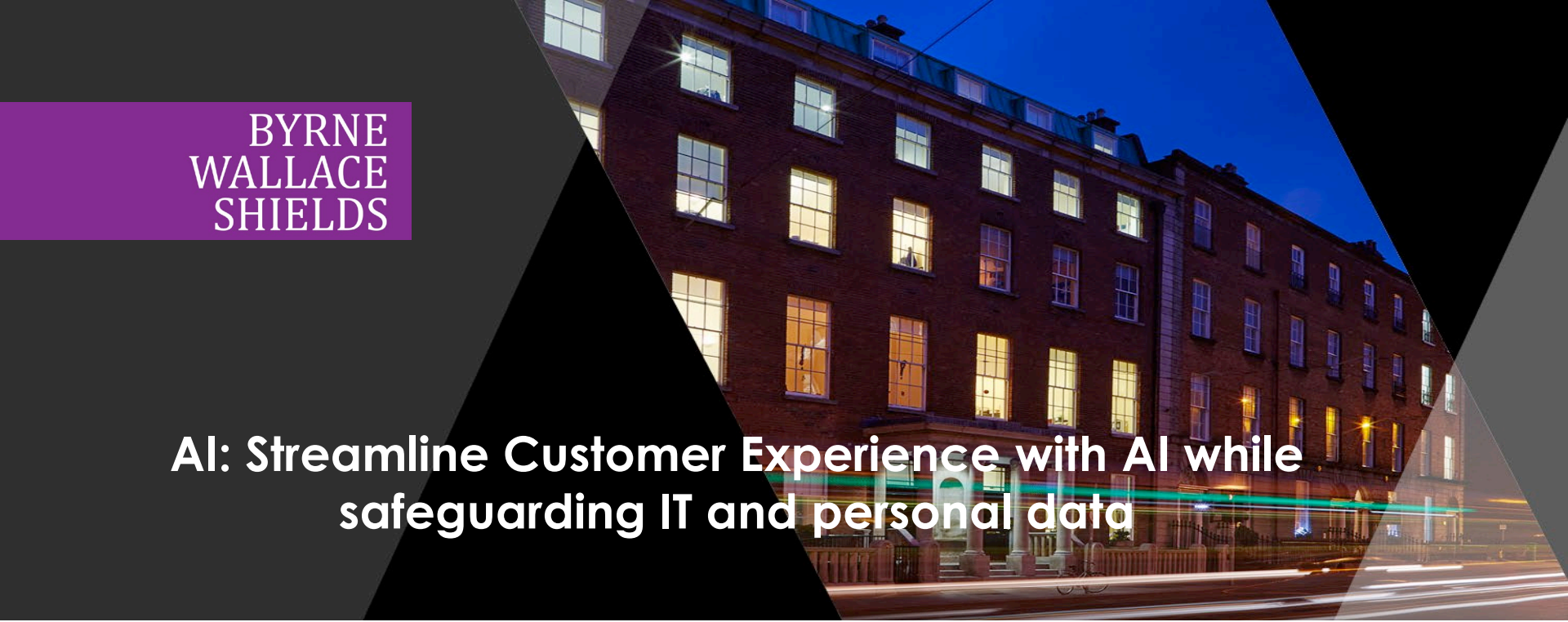
BYRNE WALLACE SHIELDS



AI: Streamline Customer Experience with AI while safeguarding IT and personal data

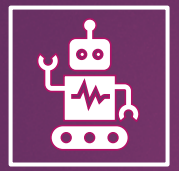
Jane O'Grady

29 May 2025

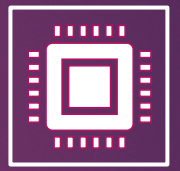
What is AI?

No standard global definition.

It is an umbrella term that covers a wide variety of processes and algorithms.



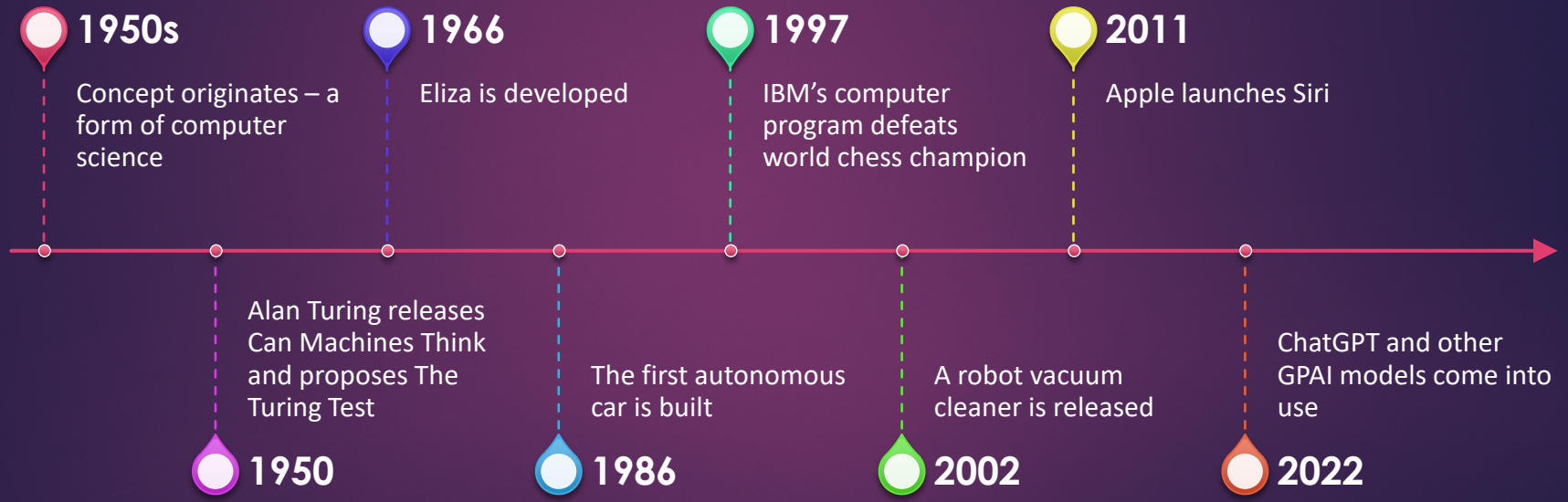
In 2019 (prior to EU AI Act): European Commission defined AI as "software and possibly hardware systems designed by humans that given a complex goal, act."



AI systems can operate in software (search engines, facial recognition systems) and can be embedded in devices (autonomous cars, IoT applications)

AI involves several approaches – machine learning (deep learning), machine reasoning (planning, scheduling, optimization) and robotics

History of AI



Uses of AI in Finance

- Fraud detection
- Customer authentication
- Cyber-security threat detection
- AML/CFT monitoring

- Chatbots customer service
- Personalised recommendations.
- Voice command features.

- Revenue forecasting
- Economic forecasting in text analysis
- Detecting patterns in unstructured datasets

- AI-based credit scoring
- Credit and insurance recommendations

Figure 1.3. Indicative types of financial firms currently experimenting with or deploying AI

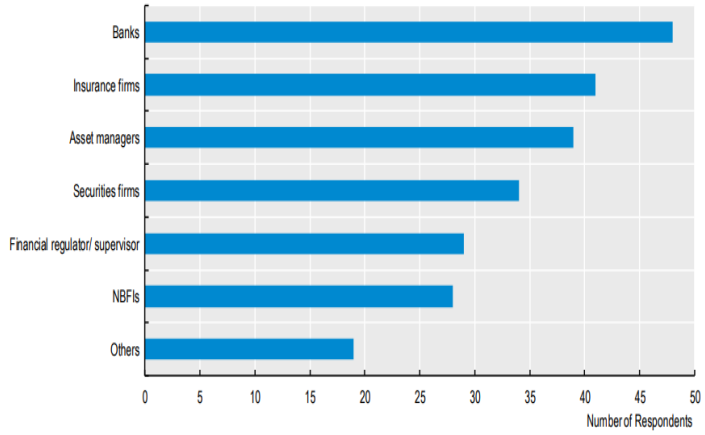
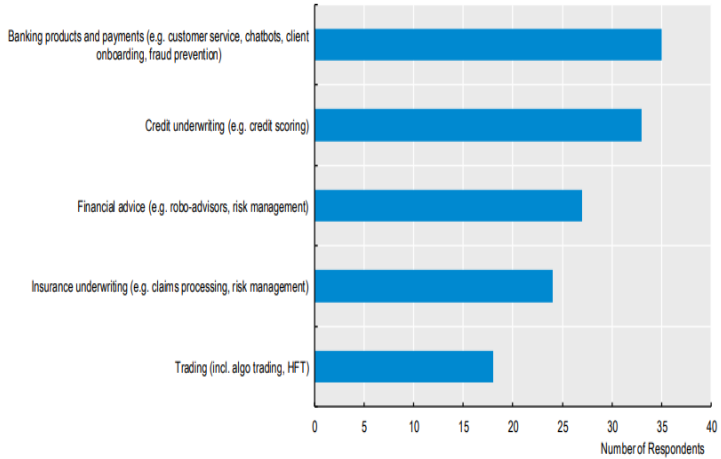


Figure 1.4. AI development or use involved in numerous products across sectors



Objectives of Irish and EU AI Regulation

Innovation Support

Prevents restrictions unless explicitly authorized by the AI Act

Risk-Based Approach

Categorises AI systems based on potential for harm

Human-Centric & Trustworthy

Protects health, safety, and fundamental rights

The EU AI Act entered into force in August 2024. Implementation began in February 2025 and continues until August 2027.

The Meaning Of AI Under The EU AI Act

The EU AI Act has a broad definition of AI:
"Machine-based system designed to operate with **varying levels of autonomy** and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, **infers, from the input it receives**, **how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments**"

Autonomy Levels

- Covers systems operating fully autonomously and those requiring human input.

Adaptiveness

- Includes systems that may adjust based on information provided to them.

Output Generation

- Encompasses systems that learn to generate outputs based on received information.

BYRNE WALLACE SHIELDS

Classification of AI Systems

The AI Act takes a risk based approach. It prohibits some AI systems and distinguishes between AI systems of high risk and limited risk.

Prohibited Practices

AI systems that are incompatible with EU values and fundamental freedoms will be prohibited.

High-Risk

AI systems that could cause significant harms if they fail or are misused.

Minimal-Risk AI

All remaining AI systems (e.g. spam filters).

Limited Risk

AI applications that pose the risk of manipulation or deceit (e.g. deep fakes). They are less regulated but have transparency obligations.

New Terminology

AI System

- All components needed to deploy AI in a specific context or application.
- Includes software, hardware, user interface, AI models and an AI System enables end users to interact with an AI model.

AI Model

- The algorithm or mathematical model trained to perform a particular task.
- Integrated into an AI System but an AI Model is not accessible to end users.

AI Provider

- Entity that develops or has an AI system developed and places it on the market or puts it into service under its own name or under its trade mark.
- Responsible for the market placement or service provision of a high-risk AI system, irrespective of whether the Provider designed or developed the system.

AI Deployer

- Entity that uses the AI under its authority except for non-professional personal use.
- May tip into becoming a Provider if it customises a high-risk AI system or modifies a limited risk AI system in such a way that it becomes high risk.

Article 5 - Eight Prohibited AI Practices

In force 2 February 2025	Subliminal, purposively manipulative or deceptive techniques
	Exploiting vulnerabilities.
	Social scoring
	Predicting criminality based on profiling*
	Facial recognition databases.
	The use of emotion recognition in the workplace or in educational settings.
**Exemptions apply for Ireland*	Biometric categorisation*
	Real-time remote biometric identification in public spaces for law enforcement purposes.*

High Risk AI Systems 2026 - 2027

High Risk AI Systems include

- Where an **AI system is a product itself** such as medical devices, toys, cars
- AI systems intended to be **used in the safety component of a product**

Certain standalone systems in the following fields – rules come in 2 August 2026

Biometrics	Critical infrastructure	Education	Employment
AI Systems evaluating access to essential services. **Covers AI Systems to assess creditworthiness, life and health insurance-related assessments or pricing.**	Immigration	Administration of Justice and Democratic Processes	Law enforcement

Obligations of **Providers** of High Risk AI Systems

1. Establish a **risk management system** throughout the high-risk AI system's lifecycle
2. Conduct **data governance**, ensuring that training, validation and testing datasets are relevant
3. Draw up **technical documentation** to demonstrate compliance
4. Automatically **recording events relevant to identifying national level risks** and substantial modifications throughout the system's lifecycle.
5. Design the AI system to allow deployers to **implement human oversight**.
6. Design the AI system to achieve appropriate levels of **accuracy, robustness, and cybersecurity**.
7. Establish a **quality management system**

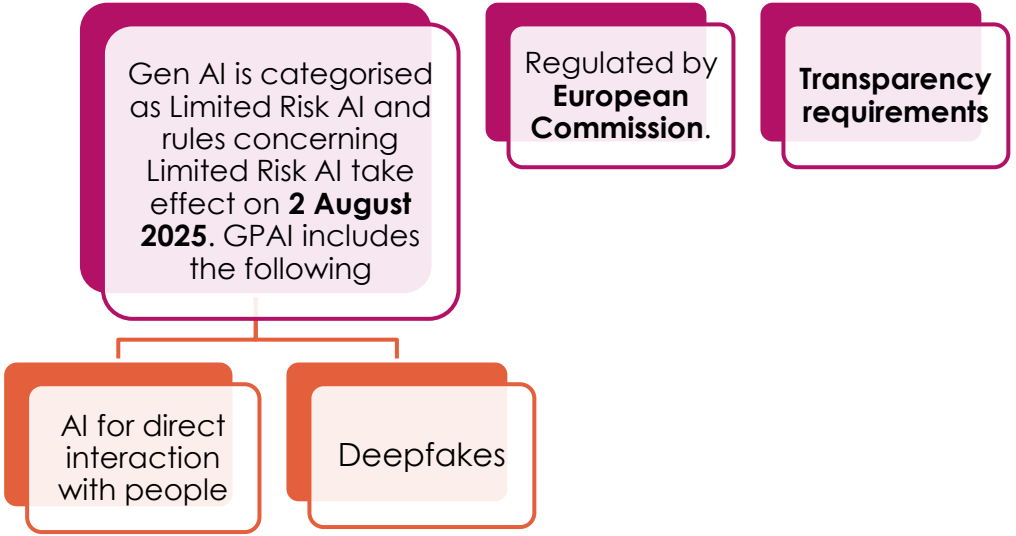
Obligations on **Deployers** of High Risk AI Systems

1. Implement **appropriate technical and organisational measures** to use high-risk AI systems in accordance with instructions
2. Assign **human oversight** to appropriate individuals
3. Ensure **input data** the deployer controls **is relevant and sufficiently representative** to the intended purpose of the AI system
4. **Monitor** the operation of the AI system
5. **Inform providers** if the AI System poses a risk.
6. **Keep logs generated by the AI system** for an appropriate period (at least six months).
7. **Cooperate** with the competent authorities

Special rules for financial institutions

- Providers and Deployers of High Risk AI Systems that are subject to EU rules on financial institutions can comply with their obligations vis-à-vis High Risk AI Systems by complying with specific requirements under financial services law.
- The AI Act provides that national financial supervisory authorities will act as the market surveillance authority of High-risk AI systems used by financial institutions.
- The Irish Government has indicated that the relevant national authority in Ireland will be the Central Bank of Ireland.

General Purpose AI Models



Minimal Risk AI Systems

Minimal Risk

- AI systems that pose no or minimal risk such as recommender systems and email spam filters.
- Largely exempt from the AI Act
- May be subject to other laws such as the GDPR

Open Source

- The AI Act does not cover open source AI systems unless they are:
- Are Prohibited
- Marketed / utilised as a high risk AI system
- Are subject to transparency obligations (Limited AI)

Compliance Timetable

2 May 2025

European Commission Code of Practice on GPAI due (draft code is published)

2 August 2025

Providers of GPAI models in place on 2 August 2025 need to comply with the AI Act by 2 August 2027.

Deadline to report to the Commission on national competent authorities resources.

Deadline to designate national competent authorities and market surveillance authorities.

Deadline for Member States to lay down rules for penalties and fines and notify them to the Commission.

Compliance Timeline (ctd)

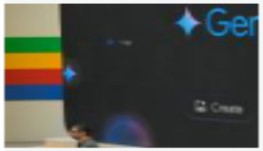
2 August 2026

- The remainder of the AI Act starts to apply. Includes for High Risk AI systems used in **biometrics,** critical infrastructure, education, **employment, access to essential public services**, law enforcement, immigration, and administration of justice.
- The Commission will review, and potentially amend, the list of high risk AI systems.
- Deadline for national rules on penalties

2 August 2027

- Providers of GPAI models placed on the market before 2 August 2025 must have taken the necessary steps to comply with GPAI obligations
- Rules for high risk systems falling under defined EU harmonised legislation come into force.

IT Risks - Hallucinations



Google's AI chatbot Gemini tells user to 'please die' and 'you are a waste of time and resources'

Gemini is supposed to have restrictions that stop it from encouraging or enabling dangerous activities, including suicide, but somehow, it still managed to tell one

news.sky.com

https://news.sky.com/story/googles-ai-chatbot-gemini-tells-user-to-please-die-and-you-are-a-waste-of-time-and-resources-13256734

19:57

AI hallucinations: ChatGPT created a fake child murderer

ChatGPT created a fake story about a Norwegian man, claiming that he killed his two children and went to jail. This never happened

noyb.eu

https://noyb.eu/en/ai-hallucinations-chatgpt-created-fake-child-murderer

19:58

ChatGPT hit with privacy complaint over defamatory hallucinations | TechCrunch

OpenAI is facing another privacy complaint in Europe over its viral AI chatbot's tendency to hallucinate false information -- and this one might prove

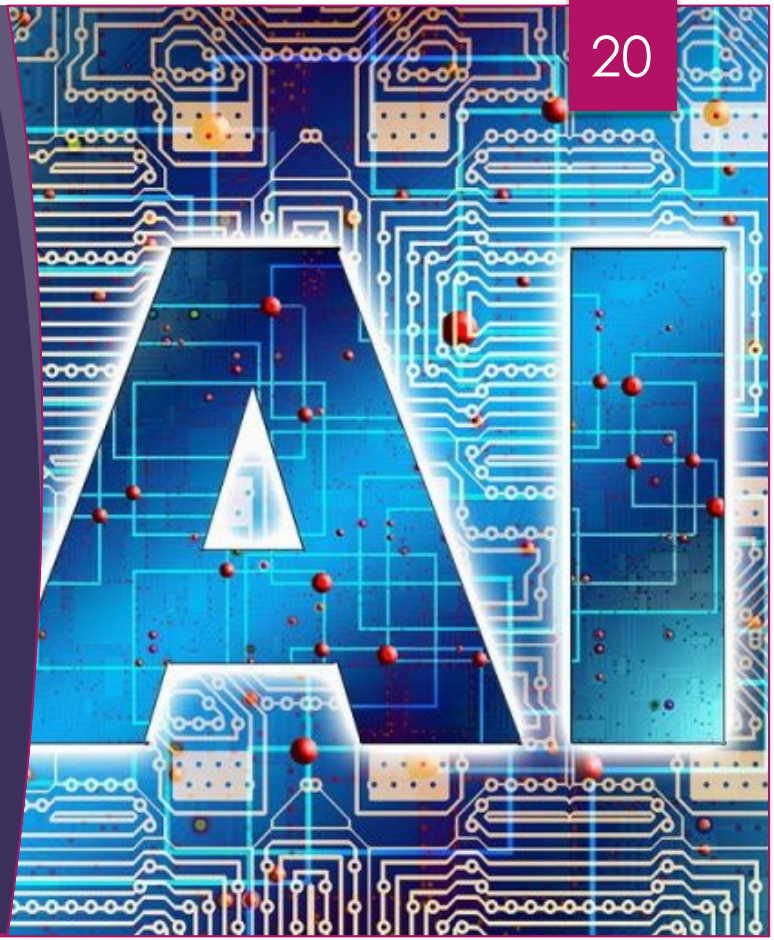
techcrunch.com

https://techcrunch.com/2025/03/19/chatgpt-hit-with-privacy-complaint-over-defamatory-hallucinations/

19:58

Safeguarding AI IT

1. Audit current AI Systems in use and identify potential future AI systems that may be used
2. Maintain an inventory of AI assets, including data, models, and infrastructure.
3. Identify risks linked to prohibited AI practices and take preventative measures
4. Implement human oversight and responsibility for AI Systems
5. Multi-factor authentication and strict access controls.
6. Data anonymization and pseudonymization.
7. Conduct and document training sessions

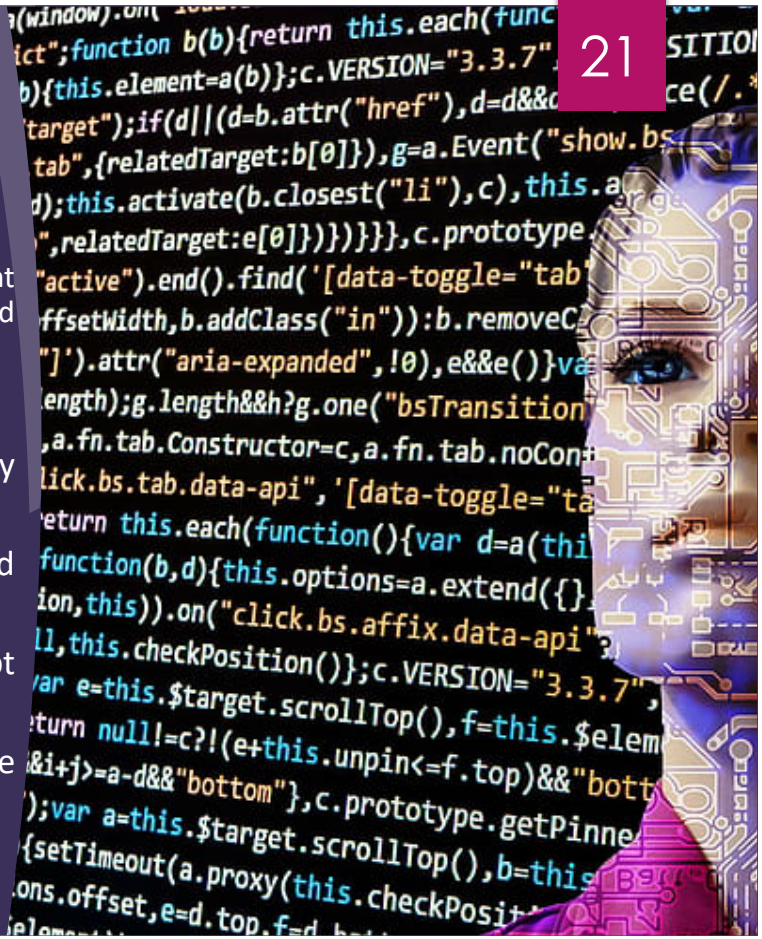


Safeguarding IT: AI Literacy

- Article 4 AI Act (since 2 February 2025)

  Organisations must ensure that staff using AI systems have a sufficient level of AI literacy. Not prescriptive but measures that can be adopted which in parallel help safeguard IT systems include:

- Tailor AI training to management and staff in different roles.
- Information about functioning and limitations of AI technology including awareness of automation bias
- Information about how are outputs produced, risk of bias and hallucinations.
- Ensure only authorised information can be used in the prompt or input data.
- Confidential information and personal data should only be used in compliance with organisation's policies
- Develop and implement an AI use policy



Data Protection Considerations

- **Security of data and compliance data protection principles** are required where personal data is used as part of an AI.
- Controllers of personal data in AI models or systems must have **data governance and decision making controls** in place that accord with the GDPR accountability principle.
- Data protection applies to datasets containing personal data – organisations need a legal basis to use the data and must out a **DPIA if the AI is new technology or combines datasets.** (Article 35 GDPR)
- **Automated Processing** - The AI Act does not prohibit automated decision making by AI Systems but Article 22 GDPR states that data subjects have the right not to be subject a solely automated decision that results in an outcome affecting them legally or otherwise having a significant similar effect

DPC Guidance

Guidance note on the use of LLMs and Data Protection

- What is the **purpose** and **legal basis** of the process. Are there **non- AI technologies** that can be used to achieve the same purpose?
- **Data sharing arrangements** with other organisations to ensure they have a **legal basis to use personal data** and the processing is **fair and transparent**.
- Obligation to account to individuals that make their personal data publicly accessible to assess how it can be used "***publicly accessible personal data still falls within the scope of the GDPR***"
- **Tell data subjects** what processing you are doing, how you are doing it, and how they can exercise their data protection rights (**Transparency requirement**)
- Requirement to comply with '**storage limitation**' for personal data you process on an AI system.
- Requirement to have personal data governance, design, policy and decision-making controls in place in accordance with **GDPR accountability requirements** where outcomes of AI processing might affect the rights and freedoms of individuals
- Consider other obligations like **copyright, safety and security**.

Challenges

- Ensuring data accuracy, reliability and interpretability
- Mitigating biases
- Privacy and cybersecurity
- Intellectual Property
- Maintaining clients' trust
- Regulatory uncertainty

BYRNE WALLACE SHIELDS

Key Takeaways

AI Act applies tiered regulation

Most AI systems will be subject to limited regulation

Keep up to date with EU and national regulatory trends and guidance

Be aware of parallels with other laws

Build compliance frameworks that can adapt

Adopt defensible positions to balance compliance with your organisation's goals. document justification of decisions

Phased Implementation

Enforcement will take time

Gradual rollout from February 2025 to August 2027.

Jane O'Grady

+353 1 6371554

jogrady@lbyrnewallaceshields.com