WILLIAM FRY

The William Fry **AI Guide**

Insights and Guidance on the AI Act and other AI Legal Issues

Introduction to the **William Fry AI Guide**

William Fry was founded in 1847 and has always been at the cutting edge of technology, advising clients on various technological developments as they arose, and now, artificial intelligence (AI).

AI is having a significant impact on society and so it was inevitable that such a powerful technology would end up being regulated. On 1 August, 2024, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence – the AI Act – came into force in the EU.

William Fry is proud to be one of the leading voices internationally in this new field of AI law, and we have produced this Guide to help businesses address questions on AI and related legal matters, truly at the cutting-edge, given the novelty of this technology and the pace at which it is developing.

The William Fry AI Guide is designed as a practical tool to assist in navigating complex legal issues raised by AI. Part 1 of the Guide deals with the AI Act, and we provide a comprehensive overview of relevant pressing areas to be considered in the months after the AI Act enters into force, along with our own insights in terms of what businesses can consider doing to deal with the new legislation.

Part 2 of the Guide addresses various AI-related legal issues that we see arise in our daily work, often deeply connected with our work in relation to intellectual property, contracts, data protection and corporate transactions. Part 2 provides practical considerations for dealing with these areas of law when they involve an AI component.

We hope that you enjoy reading this Guide, and that you find it helpful in addressing the legal issues raised by AI.

Who Should Use This Guide?

This guide is intended for a diverse audience:

- **Business Leaders and Managers:** To understand the strategic implications of the AI Act on their operations and innovation efforts.
- **In-house Legal Practitioners:** To gain in-depth knowledge of the regulatory requirements and provide informed counsel to clients.
- **Compliance Officers:** To develop and maintain AI governance frameworks within their organizations.
- **AI Developers and Engineers:** To ensure their AI solutions comply with legal standards and ethical guidelines.

By providing clear, actionable insights, this guide aims to equip businesses with the knowledge and tools needed to successfully navigate the AI Act, fostering a future where AI technology is both leveraged for innovation and responsibly managed.

For further guidance and support on AI compliance, please contact Leo Moore, Barry Scannell, David Cullen, Rachel Hayes, or any member of the William Fry Technology Department.

Table of **Contents**

PART 1
The AI Act

1. A Practical Guide to the AI Act – A General Overview

Introduction

In this section, we provide a general overview of the AI Act, before delving deeper into specific parts of the legislation in further sections. The AI Act became effective on 1 August, 2024, and is a principles-based piece of legislation which takes a risk-based approach to regulating this new technology. Unacceptable risk systems are prohibited under the AI Act, while high-risk systems are heavily regulated. There are also rules on General-Purpose AI models and systems, regulatory sandboxes, and AI literacy requirements, which are addressed below. We also provide information on key dates, and steps to compliance which businesses may wish to consider.

A. Overview of the AI Act

1. Prohibited Practices

The AI Act addresses several key areas, starting with the prohibition of certain AI practices due to their potential to cause significant harm or violate fundamental rights.

The Act bans manipulative or deceptive AI systems that use subliminal techniques to distort human behaviour and impair decision-making. This prohibition targets AI systems that employ imperceptible audio or visual stimuli to influence consumer choices unknowingly.

AI systems that exploit vulnerabilities based on age, disability, or socio-economic status are also prohibited. This includes systems targeting children, elderly individuals, or economically disadvantaged groups.

Social scoring is another prohibited practice under the AI Act. AI systems that evaluate or classify individuals based on their social behaviour or personal characteristics, leading to unjustified or disproportionate treatment, are banned. Such systems can result in discrimination and exclusion, violating fundamental rights.

The AI Act also prohibits predictive policing systems used solely for predicting criminal offences based on profiling or assessing personality traits. This prohibition ensures that AI systems do not unjustly target individuals based on profiling without human assessment of their involvement in an activity based on objective and verifiable facts.

Untargeted facial recognition databases are restricted under the Act. AI systems that create or expand facial recognition databases through untargeted scraping of images from the internet or CCTV footage are prohibited to protect privacy and prevent misuse of biometric data.

Emotion recognition in workplaces and educational institutions is banned unless used for medical or safety reasons. This regulation prevents the potential misuse of AI systems to infer emotions in sensitive environments, where power imbalances could lead to exploitation.

AI systems that categorise individuals based on biometric data to infer sensitive characteristics such as race, political opinions, or sexual orientation are prohibited to avoid discrimination and privacy violations.

Real-time remote biometric identification systems are heavily restricted for law enforcement purposes, with strict conditions and safeguards to prevent misuse and protect individual rights.

2. High-Risk AI Systems

In addition to prohibitions, the AI Act classifies certain AI systems as high-risk, subjecting them to stringent regulatory requirements. High-risk AI systems include certain of those used in critical infrastructure, education, employment, essential services, law enforcement, migration, and the administration of justice. Use of these systems requires providers to maintain technical documentation, implement a quality management system, ensure data governance, and conduct conformity assessments. Deployers must ensure proper use, monitor performance, maintain records, and comply with data protection laws.

3. General-Purpose AI Models and Systems

The AI Act also regulates general-purpose AI models and systems. These models are defined by their ability to perform various tasks across different applications. If these models possess high-impact capabilities, they are classified as having systemic risk. Providers of general-purpose AI models must ensure compliance with documentation, data protection, and transparency obligations. Deployers are responsible for ensuring proper use and reporting any substantial modifications that might change the AI system’s risk classification.

4. AI Literacy

AI literacy is another focus of the AI Act. AI literacy involves the skills and knowledge needed to make informed decisions regarding AI systems. Organisations must ensure their staff possess adequate AI literacy, supported by initiatives from the European AI Board. Measures to promote AI literacy include developing training programmes and collaborating with industry groups and regulatory bodies.

5. Regulatory Sandboxes

Regulatory sandboxes are established to allow providers to test innovative AI systems in real-world conditions. These frameworks, governed by a sandbox plan, are designed to foster innovation while ensuring regulatory compliance. Competent authorities provide guidance, supervision, and support, aiming to mitigate risks and enhance legal certainty. Small and medium-sized enterprises (SMEs) and start-ups receive priority access and tailored support services within these sandboxes.

B. Key Dates

- **12 July 2024:** The AI Act published in the Official Journal.
- **1 August 2024:** The AI Act becomes law.
- **2 February 2025:** Rules on Prohibited AI Systems come into effect
- **2 August 2025:** Rules on General-Purpose AI Models and Systems come into effect.
- **2 August 2026:** Rules on Annex III High-Risk AI systems and establishment of regulatory sandboxes come into effect.
- **2 August 2027:** Rules on Annex I High-Risk AI systems come into effect.

C. Enforcement and Penalties

- Non-compliance with the rules on Prohibited AI Systems will attract substantial administrative fines of up to €35 million or, if an undertaking, 7% of the offender's total worldwide annual turnover for the preceding financial year, whichever is higher. Non-compliant AI systems can also be taken off the EU market.

- For high-risk AI, non-compliance with specific obligations related to operators or notified bodies can result in administrative fines of up to €15 million or, if the offender is an undertaking, up to 3% of its total worldwide annual turnover for the preceding financial year, whichever is higher. This includes obligations of providers (Article 16), authorised representatives (Article 22), importers (Article 23), distributors (Article 24), deployers (Article 26), and requirements and obligations of notified bodies (Article 31, Article 33(1), (3) and (4), or Article 34), as well as transparency obligations for providers and deployers (Article 50).

- Supplying incorrect, incomplete, or misleading information to notified bodies or national competent authorities in response to a request can result in fines of up to €7.5 million or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

- For SMEs, including start-ups, each fine is capped at the lower of the specified percentages or amounts.

D. Steps to Compliance

The basic framework suggested for compliance is set out below however different categories of AI systems will attract different compliance obligations, which are set out in the following sections.

1. **Conduct an AI Inventory**

   Create a comprehensive inventory of all AI systems in use. Categorise based on purpose, functionality, and data processed.

2. **Assess AI Systems**

   Review AI systems to determine if they fall under prohibited or high-risk categories. Focus on customer interaction, marketing, decision-making, and sensitive data processing systems.

3. **Implement Compliance Measures**

   Discontinue or modify non-compliant AI systems. Establish policies for ongoing monitoring and assessment.

4. **Training and Awareness**

   Educate employees on regulations and compliance importance. Provide training on identifying and mitigating risks associated with AI practices.

5. **Documentation and Reporting**

   Maintain detailed records of AI systems, assessments, and compliance measures. Prepare to provide documentation to regulatory authorities.

Conclusion

The AI Act represents a comprehensive effort by the EU to regulate AI technologies and protect fundamental rights. Compliance not only avoids penalties but also fosters trust and ethical AI practices. By proactively assessing and modifying AI systems, businesses can effectively navigate these regulations and maintain a competitive edge in the rapidly evolving technological landscape.

2. Prohibited AI Systems Compliance

Introduction

The the AI Act marks a pivotal step in regulating AI by establishing a framework to ensure ethical AI use while safeguarding fundamental rights. The AI Act introduces strict rules on the deployment and use of certain AI systems. The AI Act bans certain types of AI systems which pose an unacceptable risk to fundamental rights, with fines for non-compliance greater than those for GDPR breaches. Here, we provide a detailed and practical guide for businesses to navigate the AI Act's rules on Prohibited AI Systems.

Key AI Act Articles:

Article 5 – Prohibited AI practices

Article 99(3) – Penalties

A. Overview of Prohibited AI Practices

Under Article 5 of the AI Act, the following AI practices are prohibited:

1. **Manipulative or Deceptive AI Systems:**
   - AI systems that use subliminal techniques or purposefully manipulative methods to distort human behaviour and impair decision-making, resulting in significant harm.
   - Examples include AI systems that employ imperceptible audio or visual stimuli to influence consumer choices unknowingly.

2. **Exploitation of Vulnerabilities:**
   - AI systems that exploit vulnerabilities due to age, disability, or specific social or economic situations to cause significant harm.
   - This includes AI systems that target children, elderly individuals, or economically disadvantaged groups.

3. **Social Scoring:**
   - AI systems that evaluate or classify individuals based on their social behaviour or personal characteristics, leading to unjustified or disproportionate treatment.
   - Social scoring by public or private entities can result in discrimination and exclusion, violating fundamental rights.

4. **Predictive Policing Based on Profiling:**
   - AI systems used solely for predicting criminal offences based on profiling or assessing personality traits.
   - This prohibition does not apply to AI systems that support human assessments based on objective and verifiable facts.

5. **Untargeted Facial Recognition Databases:**
   - AI systems that create or expand facial recognition databases through untargeted scraping of images from the internet or CCTV footage.

6. **Emotion Recognition in Workplaces and Educational Institutions:**
   - AI systems designed to infer emotions in workplaces and educational settings, unless used for medical or safety reasons.

7. **Biometric Categorisation:**
   - AI systems that categorise individuals based on biometric data to infer sensitive characteristics such as race, political opinions, or sexual orientation.

8. **Real-Time Remote Biometric Identification for Law Enforcement:**
   - While this is not a primary focus for most businesses, it is important to note that real-time remote biometric identification systems are heavily restricted for law enforcement purposes, with strict conditions and safeguards.

Key Dates:

- **12 July 2024:** The AI Act published in the Official Journal.
- **1 August 2024:** The AI Act will become law.
- **2 February 2025:** Rules on Prohibited AI Systems come into effect.

B. Enforcement and Penalties

Non-compliance with the rules on Prohibited AI Systems will attract substantial administrative fines of up to €35 million or, if an undertaking, 7% of the offender's total worldwide annual turnover for the preceding financial year, whichever is higher. Non-compliant AI systems can also be taken off the EU market.

C. Steps to Compliance:

1. **Conduct an AI Inventory:**
   - Begin by creating a comprehensive inventory of all AI systems currently in use within the business.
   - Categorise these systems based on their purpose, functionality, and the data they process.
2. **Assess AI Systems Against Prohibited Practices:**
   - Review each AI system to determine if it falls under any of the prohibited categories outlined in Article 5.
   - Pay particular attention to systems designed for customer interaction, marketing, decision-making, and those processing sensitive data.
3. **Implement Compliance Measures:**
   - If any AI systems are identified as potentially prohibited, develop a plan to either discontinue their use or modify them to ensure compliance.
   - Establish internal policies and procedures for ongoing monitoring and assessment of AI systems to prevent non-compliance.
4. **Training and Awareness:**
   - Educate employees, especially those involved in AI development and deployment, about the new regulations and the importance of compliance.
   - Provide specific training on identifying and mitigating risks associated with prohibited AI practices.
5. **Documentation and Reporting:**
   - Maintain detailed records of all AI systems, assessments, and compliance measures undertaken.
   - Be prepared to provide documentation to regulatory authorities if required.

Conclusion

In conclusion, navigating compliance with the AI Act's regulations on Prohibited AI systems is crucial for businesses operating within (and sometimes, outside) the EU. With significant penalties for non-compliance, including hefty fines and market restrictions, companies must proactively assess and modify their AI systems to adhere to legal requirements. This involves conducting thorough audits, implementing compliance measures, training staff, and maintaining comprehensive documentation. By taking these steps, businesses can ensure ethical AI use while safeguarding fundamental rights, thereby aligning with both regulatory expectations and societal values.

3. High-Risk AI Systems

Introduction

The AI Act introduces a series of obligations in relation to AI systems classified as high-risk due to their potential impact on health, safety, and fundamental rights. This section provides an overview of how high-risk AI systems are classified under the AI Act, the exceptions to such classifications, and outlines the obligations and necessary steps for compliance for providers and deployers. It covers key requirements such as risk management, data governance, documentation, transparency, and cybersecurity. It aims to help businesses navigate the obligations they must satisfy concerning high-risk AI systems.

Key AI Act Articles:

Article 6, Annex I – Conditions to be a high-risk AI system

Article 6, Annex III – List of high-risk AI systems

Articles 16, 22, 23, 24, 26, 31, 33(1, 3, 4), 34, 50 – Obligations on parties

A. Overview of High-Risk AI Systems

CLASSIFICATION OF HIGH-RISK AI SYSTEMS

The AI Act classifies high-risk AI systems based on their use and potential impact on safety and fundamental rights.

ARTICLE 6: CLASSIFICATION RULES FOR HIGH-RISK AI SYSTEMS

1. **Annex I High-Risk AI:**
   - An AI system is high-risk pursuant to Annex I if it meets both of these conditions:
     - The AI system is used as a safety component of a product, or is itself a product, covered by Union harmonisation legislation listed in Annex I, such as the Machinery Regulations and the Medical Devices Regulations.
     - The product or the AI system requires a third-party conformity assessment before being placed on the market or put into service, as required by the Union harmonisation legislation in Annex I.

2. Annex III High-Risk AI:

- AI systems listed in Annex III are considered high-risk. This annex includes AI systems used in:
- **Biometrics:**
  - Remote biometric identification systems.
  - AI systems for biometric categorisation based on sensitive attributes.
  - Emotion recognition systems (bear in mind that these are prohibited in the workplace or educational settings).
- **Critical Infrastructure:**
  - AI systems used as safety components in managing critical infrastructure like digital infrastructure, road traffic, water, gas, heating, and electricity.
- **Education and Vocational Training:**
  - AI systems determining access or admission to educational institutions.
  - AI systems evaluating learning outcomes or monitoring student behaviour during tests.
- **Employment and Work Management:**
  - AI systems for recruitment or selection of personnel.
  - AI systems making decisions on employment conditions, promotions, or terminations.
  - AI systems monitoring and evaluating employee performance and behaviour.
- **Access to Essential Services:**
  - AI systems evaluating eligibility for public assistance, healthcare, or social services.
  - AI systems used for creditworthiness assessment or insurance risk assessment.
  - AI systems for emergency response services.
- **Law Enforcement:**
  - AI systems assessing the risk of criminal offences.
  - AI systems used as polygraphs or evaluating the reliability of evidence.
  - AI systems assessing the risk of offending or re-offending.
  - AI systems used for profiling in criminal investigations.
- **Migration, Asylum, and Border Control:**
  - AI systems used as polygraphs or risk assessment tools for entry into Member States.
  - AI systems evaluating applications for asylum, visas, or residence permits.
  - AI systems detecting or identifying individuals in migration contexts.
- **Administration of Justice and Democratic Processes:**
  - AI systems assisting judicial authorities in researching and interpreting facts and the law.
  - AI systems influencing election outcomes or voting behaviour.

3. Exceptions:

- Certain AI systems listed in Annex III may not be classified as high-risk if they:
  - › Perform narrow procedural tasks.
  - › Improve results of previously completed human activities.
  - › Detect patterns without influencing decision-making.
  - › Perform preparatory tasks for assessments relevant to Annex III use cases.
- AI systems that perform profiling are always considered high-risk.

4. Provider Responsibilities:

A provider means a person or entity that develops an AI system or a general-purpose AI model, or that has an AI system or a general-purpose AI model developed, and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

The following requirements apply to providers of AI systems under the AI Act:

- Identification and Contact Information:
  - › Clearly indicate the provider's name, registered trade name or trademark, and contact address on the AI system or its packaging and accompanying documentation.
- Quality Management System:
  - › Implement a quality management system that includes regulatory compliance strategies, design and development procedures, data management, risk management, post-market monitoring, incident reporting, and communication with authorities.
- Technical Documentation:
  - › Maintain comprehensive and up-to-date technical documentation that demonstrates compliance with the AI Act's requirements and is available for review by national competent authorities and notified bodies.

- Automatic Logging:
  - Ensure high-risk AI systems have the capability to automatically record events (logs) throughout their lifecycle for traceability and monitoring purposes.
- Conformity Assessment:
  - Ensure that the AI system undergoes the appropriate conformity assessment procedure before being placed on the market or put into service.
- EU Declaration of Conformity and CE Marking:
  - Draw up an EU declaration of conformity and affix the CE marking to the AI system or its packaging to indicate compliance with the AI Act.
- Registration Obligations:
  - Comply with registration obligations, including registering the high-risk AI system in the EU database if required.
- Corrective Actions and Duty of Information:
  - Take necessary corrective actions to address non-compliance, withdraw, disable, or recall the AI system if it poses risks, and inform relevant parties and authorities.
- Cooperation with Authorities:
  - Provide information and documentation to national competent authorities upon request and grant access to logs and other necessary data for compliance verification.
- Accessibility Requirements:
  - Ensure the AI system meets accessibility requirements in line with relevant EU directives.

5. Deployer Responsibilities

The following requirements apply to deployers (users, other than use in the course of a personal, non-professional activity) of AI systems under the AI Act:

- Ensure Proper Use:
  - Use high-risk AI systems in accordance with the provided instructions for use.
  - Assign competent personnel for oversight and ensure that they are adequately trained.
- Data Management:
  - Ensure that input data is relevant and representative for the AI system's intended purpose.
- Monitor Operation:
  - Continuously monitor the AI system's performance and compliance.
  - Suspend use and inform authorities if any risks or serious incidents are identified.
- Record-Keeping:
  - Maintain logs generated by the AI system for a period appropriate to its purpose, typically at least six months.

- Inform Affected Parties:
  - Notify workers and representatives before deploying high-risk AI systems in the workplace.
  - Inform individuals when they are subject to decisions made by high-risk AI systems.
- Compliance with Data Protection:
  - Use information provided under the AI Act to comply with data protection impact assessments as required by GDPR.
- Annual Reporting:
  - Submit annual reports on the use of certain high-risk AI systems, such as post-remote biometric identification systems, to relevant authorities.

Key Dates:

- **12 July 2024:** The AI Act is published in the Official Journal.
- **1 August 2024:** The AI Act will become law.
- **2 August 2026:** Rules on Annex III AI systems come into effect.
- **2 August 2027:** Rules on Annex I AI systems come into effect.

B. Enforcement and Penalties

- The AI Act imposes significant fines for non-compliance with its provisions, especially for high-risk AI systems. Non-compliance with specific obligations related to operators or notified bodies can result in administrative fines of up to €15 million or, if the offender is an undertaking, up to 3% of its total worldwide annual turnover for the preceding financial year, whichever is higher. This includes obligations of providers (Article 16), authorised representatives (Article 22), importers (Article 23), distributors (Article 24), deployers (Article 26), and requirements and obligations of notified bodies (Article 31, Article 33(1), (3) and (4), or Article 34), as well as transparency obligations for providers and deployers (Article 50).

- Supplying incorrect, incomplete, or misleading information to notified bodies or national competent authorities in response to a request can result in fines of up to €7.5 million or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

- For SMEs, including start-ups, each fine is capped at the lower of the specified percentages or amounts.

C. Steps to Compliance

Depending on whether the business is a provider or deployer of a high-risk AI system, the following compliance steps should be implemented (as applicable).

1. Determine High-Risk Classification

- Identify Applicability:
  - Assess if the AI system falls within high-risk categories specified in Annex III.
  - Verify if the AI system is a safety component requiring third-party conformity assessments (Annex 1).
- Document Assessment:
  - If an AI system is not deemed high-risk, document the assessment and be prepared to present it to competent authorities.

2. Implement a Risk Management System

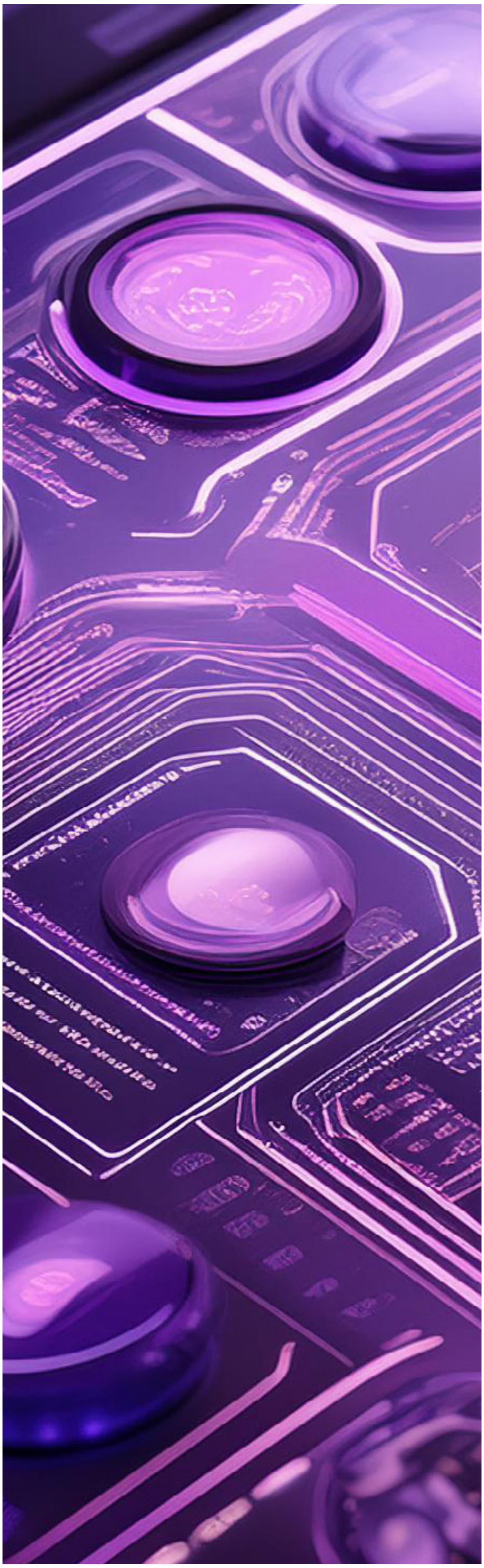
- Establish Risk Management Processes:
  - Develop and implement a risk management system that includes continuous risk identification, analysis, and mitigation.
  - Regularly review and update risk management measures.
- Integrate Human Oversight:
  - Ensure that the AI system includes mechanisms for effective human oversight and intervention.

3. Ensure Data Quality and Governance

- Use High-Quality Datasets:
  - Employ relevant, representative, and bias-free datasets for training, validation, and testing.
  - Implement data governance practices to maintain dataset quality.
- Address Data Bias:
  - Detect, prevent, and mitigate biases in datasets to avoid discrimination and ensure fairness.

4. Maintain Technical Documentation

- Prepare Comprehensive Documentation:
  - Document the AI system’s design, development, and compliance measures.
  - Ensure documentation is clear, comprehensive, and updated regularly.
- Use Simplified Forms for SMEs:
  - SMEs can use simplified technical documentation forms provided by the Commission.



5. **Establish Record-Keeping Practices**
   - Enable Automatic Logging:
     - › Ensure the AI system can automatically record events to facilitate traceability and post-market monitoring.
   - Maintain Logs for Required Period:
     - › Keep logs for a minimum of six months or as specified by applicable laws.

6. **Provide Transparent Information and Instructions**
   - Develop Clear Instructions for Use:
     - › Prepare concise, complete, and accessible instructions for the AI system's use.
     - › Include information on the system's characteristics, limitations, and human oversight measures.
   - Facilitate Interpretation of Outputs:
     - › Ensure that the AI system's outputs are interpretable and actionable by deployers.

7. **Ensure Robustness, Accuracy, and Cybersecurity**
   - Design for Accuracy and Robustness:
     - › Implement measures to achieve and maintain high levels of accuracy and robustness throughout the AI system's lifecycle.
   - Implement Cybersecurity Measures:
     - › Protect the AI system against cybersecurity threats through appropriate technical and organisational measures.

8. **Conduct Conformity Assessment**
   - Undertake Required Assessments:
     - › Ensure the AI system undergoes the relevant conformity assessment procedure before being placed on the market.
   - Affix CE Marking:
     - › Indicate conformity with the AI Act by affixing the CE marking to the AI system or its packaging.

9. **Monitor Post-Market Performance**
   - Establish Post-Market Monitoring:
     - Implement systems to monitor the AI system's performance and compliance after it has been placed on the market.
   - Report Serious Incidents:
     - Inform competent authorities and relevant parties about any serious incidents or non-compliance issues.

10. **Ensure Continuous Compliance**
    - Review and Update Compliance Measures:
      - Regularly review and update risk management, data governance, and documentation practices to ensure ongoing compliance.
    - Cooperate with Authorities:
      - Cooperate with competent authorities in providing information, documentation, and access to logs as required.

Conclusion

The AI Act places significant responsibilities on providers and deployers to ensure High-Risk AI systems are safe, transparent, and compliant with regulatory requirements. Organisations must implement robust risk management, data governance, and cybersecurity measures to meet these obligations. The penalties for non-compliance underscore the importance of adherence to the AI Act, making it crucial for businesses to stay informed and proactive in their compliance efforts. By doing so, they not only mitigate legal risks but also contribute to the responsible development and deployment of AI technologies.

4. General Purpose AI Models and Systems

Introduction

This section focuses on the obligations businesses will have under the AI Act concerning general-purpose AI (**GPAI**) models and systems. Here, we explore the definition and classification of general-purpose AI models and systems, and the responsibilities that come with developing and deploying these models and systems. This section also outlines the GPAI obligations for providers and deployers, emphasising the importance of compliance to mitigate risks and ensure the safe use of AI technology.

Key AI Act Articles:

Article 3 – Definitions

Article 51 – GPAI Models with systemic risk

Article 25 – Providers' responsibilities

Article 53 and 55 – GPAI Model providers' obligations

Article 50 – Transparency obligations

Article 88 – Enforcement

A. Overview of General-Purpose AI Models and Systems

1. **Definition and Importance:**

- General-Purpose AI Model: An AI model trained with large datasets, capable of performing a wide range of tasks and integrated into various downstream systems or applications (Article 3(63)).
- General-Purpose AI System: An AI system based on a general-purpose AI model that serves multiple purposes directly or when integrated into other AI systems (Article 3(66)).
- Their importance lies in their versatility and widespread applicability, which necessitates robust regulatory oversight to manage risks and ensure ethical deployment.

2. **Classification of General-Purpose AI Models with Systemic Risk:**

    › A general-purpose AI model is classified as having systemic risk if it has high-impact capabilities, such as significant computational power (exceeding 10^{25} FLOPs) or other criteria set by the European Commission (Article 51). FLOPs (Floating Point Operations per Second) measure the computational power of a system by counting the number of floating-point calculations it can perform per second. This high computational threshold indicates the model's ability to handle extensive and complex tasks, necessitating robust regulatory oversight. Systemic risks may include major accidents, disruption of critical sectors, serious consequences to health and safety, and actual or reasonably foreseeable negative effects on democratic processes, and public and economic security. Systemic risk increases with model capabilities and model reach.

3. **Responsibilities along the AI Value Chain:**

    - Providers, deployers, and other third parties can be considered providers of high-risk AI systems if they substantially modify a general-purpose AI system's intended purpose, leading to it becoming a high-risk AI system (Article 25).
    - Providers of general-purpose AI models must cooperate with downstream providers to ensure compliance with the AI Act's obligations (Article 25(4))

4. **Obligations for Providers of General-Purpose AI Models:**

    - Draw up and maintain technical documentation of the model's training and evaluation (Article 53).
    - Make available documentation and information to downstream providers to understand the model's capabilities and limitations (Article 53(b)).
    - Put in place a policy to comply with EU copyright law, ensuring all content used for training respects reserved rights (Article 53(c)).
    - Publish a summary of the content used for training the model (Article 53(d)).

5. **Special Obligations for Providers of General-Purpose AI Models with Systemic Risk:**

    - Perform model evaluations using state-of-the-art protocols, including adversarial testing (Article 55).
    - Mitigate systemic risks and ensure cybersecurity protections are in place (Article 55).

6. **Transparency Obligations (Article 50):**

    - Providers of AI systems, including general-purpose AI systems, that generate synthetic content must ensure the outputs are marked in a machine-readable format as artificially generated or manipulated.
    - Technical solutions for these markings should be effective, interoperable, robust, and reliable, considering technical feasibility and costs.

7. **Deployer Obligations**

    - Deployers, defined as entities using an AI system under their authority (Article 3(4)), must ensure that the AI systems they use comply with the AI Act's requirements.
    - Deployers must collaborate with providers to maintain compliance and report any substantial modifications that might change the AI system's risk classification.

Key Dates:

- **12 July 2024:** The AI Act published in the Official Journal.
- **1 August 2024:** The AI Act will become law.
- **2 August 2025:** Rules on General Purpose AI Models and Systems come into effect.

B. Enforcement and Penalties

1. **Supervision and Enforcement:**

    - The AI Office and national authorities will monitor compliance, with the AI Office having exclusive powers to enforce obligations related to general-purpose AI models (Article 88).
    - Providers must respond to documentation requests and facilitate evaluations by the AI Office (Articles 91 and 92).

2. **Fines and Penalties:**

    - The European Commission can fine providers of general-purpose AI models up to 3% of their total worldwide annual turnover from the previous financial year or €15 million, whichever is higher.
    - This happens if the provider is found to have intentionally or negligently violated the provisions of the AI Act, failed to comply with a request for documents or information under Article 91, provided incorrect, incomplete, or misleading information, ignored a measure requested under Article 93, or did not provide the European Commission with access to the general-purpose AI model or a model with systemic risk for evaluation under Article 92.

C. Steps to Compliance

1. **Conduct an AI Inventory:**
   - Begin by creating a comprehensive inventory of all AI systems currently in use within the organisation.
   - Categorise these systems based on their purpose, functionality, and the data they process.

2. **Assess AI Systems Against General-Purpose AI Models and Systems Rules:**
   - Review each AI system to determine if it could be classified as general-purpose AI model or system.

3. **Implement Compliance Measures:**
   - If any AI systems are identified as general-purpose AI model or system, develop a plan to ensure compliance.
   - Establish internal policies and procedures for ongoing monitoring and assessment of AI systems to prevent non-compliance.

4. **Training and Awareness:**
   - Educate employees, especially those involved in AI development and deployment, about the new regulations and the importance of compliance.
   - Provide specific training on identifying and mitigating risks associated with general-purpose AI models or systems.

5. **Documentation and Reporting:**
   - Maintain detailed records of all general-purpose AI models or systems, assessments, and compliance measures undertaken.
   - Be prepared to provide documentation to regulatory authorities if required.

Conclusion

Ensuring compliance with the obligations for general-purpose AI models is crucial for fostering trust and promoting ethical AI practices. By taking proactive steps to assess, document, and monitor AI systems, businesses can navigate these regulations effectively and maintain a competitive edge in a rapidly evolving technological landscape.

5. AI Literacy Requirements

Introduction

The AI Act introduces a legal obligation to ensure adequate levels of AI literacy within organisations. Knowledge and education in relation to AI are essential in order to properly deploy the technology. The AI Act has recognised this, and requires organisations to have the requisite level of AI literacy amongst their staff, likely involving AI training. Here we provide a detailed and practical guide for businesses to navigate their obligations to ensure AI literacy in their organisations.

Key AI Act Articles:

Article 3 – Definitions

Article 4 – AI Literacy measures

A. Overview of AI Literacy Requirements

Under Article 4 of the AI Act, the following AI literacy measures are required:

1. **Definition and Importance of AI Literacy:**
   - AI literacy is defined as the skills, knowledge, and understanding that enable providers, deployers, and affected persons to make informed decisions regarding AI systems. This includes awareness of opportunities, risks, and potential harms associated with AI.
   - AI literacy is crucial for the ethical deployment of AI, ensuring that all stakeholders understand the implications of AI use and can manage associated risks effectively.

2. **Measures to Ensure AI Literacy:**
   - Organisations must ensure their staff and other individuals involved in AI operations possess adequate AI literacy. This includes understanding the technical aspects of AI systems, proper application during development and deployment, and interpreting AI outputs correctly.

3. **Supporting Structures:**

   - **European Artificial Intelligence Board (AI Board):** The AI Board will support the European Commission in promoting AI literacy, public awareness, and understanding of AI systems' benefits, risks, safeguards, and related rights and obligations.
   - **Voluntary Codes of Conduct:** The European Commission and Member States will facilitate the creation of voluntary codes of conduct to enhance AI literacy among developers, operators, and users of AI systems.

Key Dates:

- **12 July 2024:** The EU will publish the AI Act in the Official Journal.
- **1 August 2024:** The AI Act will become law.
- **2 February 2025:** Rules on AI literacy requirements come into effect.

B. Enforcement and Penalties

Article 4 will likely impact the extent of enforcement measures taken against organisations for other AI Act infringements. For example, supplying incorrect, incomplete, or misleading information to notified bodies or national authorities can result in fines up to €7.5 million or 1% of the offender's total worldwide annual turnover for the preceding financial year, whichever is higher. It is therefore important to bear this in mind if providing authorities with confirmation of the level of AI literacy within the business.

C. Steps to Compliance:

1. **Assess Current AI Literacy Levels:**

   - Evaluate the current level of AI literacy within the business.
   - Identify gaps in knowledge and understanding among staff involved in AI development, deployment, and operation.

2. **Develop and Implement AI Literacy Programmes:**

   - Design training programmes tailored to different roles within the organisation and to knowledge gaps identified. These should cover technical aspects of AI, ethical considerations, risk management, and compliance requirements.
   - Ensure continuous learning opportunities to keep pace with technological advancements and regulatory changes.

3. **Establish Internal Policies and Procedures:**
   - Develop policies that mandate regular AI literacy training for all relevant staff. Include these policies in the organisational compliance framework.
   - Set up procedures for monitoring and assessing the effectiveness of AI literacy initiatives.
4. **Collaborate with Industry and Regulatory Bodies:**
   - Engage with industry groups, regulatory bodies, and educational institutions to stay informed about best practices and new developments in AI literacy.
5. **Documentation and Reporting:**
   - Maintain detailed records of AI training programmes and compliance measures.
   - Be prepared to provide documentation to regulatory authorities if required.

Conclusion

Ensuring AI literacy is not just about avoiding penalties but also about fostering trust and promoting ethical AI practices. By taking proactive steps to assess, educate, and monitor AI literacy, businesses can navigate these regulations effectively and maintain a competitive edge in a rapidly evolving technological landscape, while ensuring high levels of AI literacy within their organisation.

6. Regulatory Sandboxes

Introduction

This section addresses the AI Act's provisions on regulatory sandboxes, highlighting their role in fostering innovation while maintaining regulatory oversight. Here, we explore the key aspects, dates, enforcement mechanisms, and compliance steps, which are essential for navigating these sandboxes effectively.

Key AI Act Articles:

Article 57 – AI regulatory sandboxes

Article 58 – Detailed arrangements for, and functioning of, AI regulatory sandboxes

Article 59 - Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox

Article 60 - Testing of high-risk AI systems in real world conditions outside AI regulatory sandboxes

Article 61 - Informed consent to participate in testing in real world conditions outside AI regulatory sandboxes

A. Overview Regulatory Sandboxes in the AI Act

WHAT ARE THEY?

Within the AI Act, regulatory sandboxes are defined as frameworks established by competent authorities. These frameworks allow providers or prospective providers to test innovative AI systems in real-world conditions for a limited period. The operation of these sandboxes is governed by a "sandbox plan", which details the objectives, conditions, timeframe, methodology, and requirements for the activities conducted within the sandbox. This plan is a mutually agreed document between the AI provider and the competent authority, ensuring clear guidelines and expectations for the testing phase. The establishment of AI regulatory sandboxes aims to improve legal certainty, support the sharing of best practices, foster innovation, facilitate regulatory learning, and enhance market access for SMEs and start-ups.

ESTABLISHMENT

The Act mandates that each Member State must establish at least one AI regulatory sandbox at the national level within 24 months of the regulation's entry into force. These sandboxes may also be established jointly with other Member States or by participating in existing sandboxes, provided they offer an equivalent level of national coverage. Additionally, Member States can establish further sandboxes at regional or local levels or in cooperation with other Member States. The European Data Protection Supervisor may also establish an AI regulatory sandbox specifically for EU institutions and bodies.

To support the effective and timely operation of these sandboxes, Member States must allocate sufficient resources and ensure cooperation among relevant authorities. These sandboxes provide a controlled environment to facilitate the development, training, testing, and validation of AI systems before their market deployment, following the specific sandbox plan agreed upon by the involved parties.

ROLE OF COMPETENT AUTHORITIES

Competent authorities are tasked with providing guidance, supervision, and support within the sandbox. This includes identifying and mitigating risks, particularly those related to fundamental rights, health, and safety. Authorities also issue documentation and exit reports, which detail the activities and outcomes of the sandbox testing. These reports can be used by providers to demonstrate regulatory compliance. The Commission and the AI Board have the authority to access exit reports to aid in their regulatory tasks.

Competent authorities retain supervisory powers and can suspend sandbox activities if significant risks are identified. Participants remain liable under applicable laws but may be exempt from administrative fines if they adhere to the sandbox plan and follow the guidance provided by authorities in good faith. The framework is designed to facilitate cross-border cooperation among national authorities and ensure coordination within the AI Board framework.

ROLE OF AI OFFICE

The AI Office is responsible for maintaining a public list of sandboxes to encourage interaction and cooperation. National authorities must submit annual reports on the progress, incidents, best practices, and outcomes of their sandboxes to the AI Office and Board. These reports help inform regulatory practices and may lead to adjustments in the regulatory framework.

ROLE OF COMMISSION

The Commission will develop detailed arrangements for the establishment and operation of sandboxes through implementing acts. These acts will specify eligibility and selection criteria, procedures for application and participation, and terms and conditions for participants. Sandboxes must ensure fair and transparent access, particularly for SMEs and start-ups, and facilitate the involvement of various stakeholders in the AI ecosystem.

PERSONAL DATA

When personal data processing is involved, data protection authorities must be included in the sandbox operation. Personal data collected for other purposes may be processed within sandboxes under specific conditions, primarily when developing AI systems for substantial public interest. This processing must comply with data protection laws, and data should be handled in a separate, protected environment with appropriate safeguards.

TESTING OUTSIDE SANDBOXES

Providers can also test high-risk AI systems in real-world conditions outside sandboxes, provided they meet specific conditions and obtain necessary approvals. This testing must ensure informed consent from participants, and providers must implement measures to protect participants' rights and safety.

SME/ START-UP SUPPORT

The AI Act prioritises support for SMEs and start-ups by ensuring they have priority access to sandboxes and tailored support services. Member States are encouraged to establish communication channels and provide guidance to SMEs throughout their development. The Commission will support these efforts by providing standardised templates and maintaining an information platform for stakeholders.

Key Dates:

- **12 July 2024:** The AI Act published in the Official Journal.
- **1 August 2024:** The AI Act will become law.
- **2 August 2026:** Member States' competent authorities will need to have established at least one AI regulatory sandbox at national level.
- **Annual Reporting:** Member States must submit annual reports to the AI Office and the Board starting one year after the establishment of the sandboxes.

B. Enforcement and Penalties

- Competent authorities have the power to supervise, guide, and support participants within the sandboxes. They are tasked with identifying and mitigating risks, particularly those affecting fundamental rights, health, and safety. If significant risks are detected and cannot be effectively mitigated, authorities can suspend or terminate the testing process within the sandbox.

- Article 57(12) specifies that providers participating in sandboxes remain liable for any damage caused to third parties. However, if they adhere to the sandbox plan and act in good faith following the guidance of the competent authorities, they are shielded from administrative fines under the AI Act.

C. Steps to Compliance:

1. **Understand the AI Act:** Familiarise yourself with the AI Act's requirements and the specific obligations for the business's AI system based on its risk classification.

2. **Participate in Sandboxes when required:** Engage with national competent authorities to participate in AI regulatory sandboxes. This involves preparing a sandbox plan (Article 3(54)) that outlines objectives, conditions, timeframes, and methodologies for sandbox activities.

3. **Follow Guidelines:** Adhere to the guidance and supervision provided by competent authorities. This includes implementing risk mitigation measures and maintaining detailed records of testing and validation activities.

4. **Annual Reporting:** Comply with reporting obligations by submitting required documentation and reports to competent authorities, the AI Office, and the Board.

5. **Exit and Conformity Assessment:** Upon successful completion of sandbox activities, utilise the exit report and written proof provided by competent authorities to streamline the conformity assessment process for market entry.

Conclusion

Regulatory sandboxes are a cornerstone of this framework, offering a controlled environment for developing and testing AI systems. By understanding the requirements and leveraging the support offered through sandboxes, AI providers can navigate the regulatory landscape effectively, fostering innovation while ensuring compliance. The establishment of these sandboxes, alongside stringent oversight and guidance, aims to create a robust and innovative AI ecosystem within the EU.

7. Biometric Categorisation Systems

Introduction

This section is a guide to compliance with the AI Act's regulations on biometric categorisation systems. It explains the distinctions between prohibited biometric systems, which infer sensitive attributes and are banned, and high-risk biometric systems, which require strict regulatory adherence.

The AI Act's treatment of biometric categorisation systems is nuanced, particularly when distinguishing between prohibited and high-risk biometric applications. Article 3(40) defines a biometric categorisation system as one that assigns individuals to specific categories based on biometric data, unless it is ancillary to another commercial service and necessary for technical reasons. This distinction is crucial in understanding the broader regulatory landscape.

This section outlines steps for compliance, including system assessment, legal requirement understanding, implementation of safeguards, risk assessment, documentation, monitoring, training, and staying informed on legal developments.

Key AI Act Articles:

Article 3 – Definitions

Article 5 – Prohibited AI practices

Article 6: Classification Rules for High-Risk AI Systems

Article 6, Annex III – List of high-risk AI systems

Article 50 – Transparency obligations

Article 16, 22, 23, 24, 26, 31, 33(1, 3, 4), 34, 50 – Obligations on parties

A. Overview of Biometric Categorisation Systems under the AI Act

BIOMETRIC DATA

Biometric data, as defined in Article 3(34), includes personal data resulting from processing related to physical, physiological, or behavioural characteristics. Article 3(35) extends this to biometric identification, involving the automated recognition of these characteristics to establish identity. The AI Act, places significant emphasis on the sensitivity and potential misuse of such data.

PROHIBITED APPLICATIONS

Article 5(g) prohibits the placing on the market, putting into service, or use of biometric categorisation systems that deduce or infer sensitive attributes such as race, political opinions, or sexual orientation. This prohibition is specific and absolute, aiming to prevent systems from making inferences that could lead to discrimination or privacy violations. Recital 30 supports this by highlighting that while categorising datasets lawfully acquired for attributes like hair colour or eye colour may be permissible in law enforcement, deducing sensitive personal attributes is strictly prohibited.

HIGH-RISK APPLICATIONS

In contrast, high-risk biometric categorisation systems, as referenced in Article 6(2) and detailed in Annex III, are subject to stringent regulation rather than outright prohibition. These systems, used for purposes like identifying sensitive or protected attributes, are considered high-risk due to the potential for significant harm or influence on decision-making outcomes. Recital 54 underscores the high-risk classification by noting the discriminatory potential and technical inaccuracies that could affect protected characteristics like age, ethnicity, or race.

Deployers of high-risk biometric categorisation systems must adhere to specific obligations under Article 50(3), including the obligation to inform individuals exposed to these systems and to process data in compliance with GDPR and other relevant EU regulations. This reflects the Act’s intent to ensure transparency and safeguard individual rights, even for high-risk systems.

PROHIBITED OR HIGH-RISK?

The key difference lies in the nature and sensitivity of the categorisation. Prohibited systems deduce or infer sensitive attributes from biometric data, while high-risk systems involve categorising biometric data in ways that could indirectly affect individuals' rights and outcomes.

The difference seems to be that biometric categorisation will be considered high-risk if sensitive attributes are readily apparent, but it will be prohibited if such attributes are inferred or deduced from other data.

Prohibited systems are outright banned due to their inherent risk of severe misuse and discrimination. In contrast, high-risk systems are regulated to ensure that they are used responsibly and with necessary safeguards to protect individual rights.

This distinction can lead to confusion, particularly where the line between sensitive inferences and lawful categorisations is blurred. For instance, while a system categorising images by hair or eye colour for law enforcement purposes might be high-risk and regulated, a system inferring someone's political beliefs from facial recognition data is prohibited. Navigating these nuances requires careful legal interpretation and compliance with both the AI Act and relevant national laws, ensuring that biometric technologies are deployed ethically and legally.

Furthermore, the overlap between national laws and the AI Act's provisions adds another layer of complexity. For example, Ireland's specific opt-outs under Recital 40 indicate that certain uses of biometric categorisation in law enforcement may be permissible under national law, despite the broader EU prohibition. This necessitates a detailed understanding of both Union and Member State regulations to navigate compliance effectively.

The regulatory framework's reliance on the context and purpose of biometric categorisation systems means that stakeholders must be vigilant in distinguishing between acceptable high-risk applications and outright prohibited practices. This vigilance is crucial to avoid unintentional breaches of the AI Act, given the severe implications of using these technologies improperly.

Key Dates:

- **12 July 2024:** The AI Act published in the Official Journal.
- **1 August 2024:** The AI Act will become law.
- **2 February 2025:** Article 5 Biometric Categorisation Systems are banned.
- **2 August 2026:** Rules on Annex III Biometric Categorisation Systems come into effect.

B. Enforcement and Penalties

- Non-compliance with the rules on Prohibited AI Systems will attract substantial administrative fines of up to €35 million or, if an undertaking, 7% of the offender's total worldwide annual turnover, whichever is higher. Non-compliant AI systems can also be taken off the EU market.
- The AI Act imposes significant fines for non-compliance with its provisions, especially for high-risk AI systems. Non-compliance with specific obligations related to operators or notified bodies can result in administrative fines of up to €15 million or, if the offender is an undertaking, up to 3% of its total worldwide annual turnover for the preceding financial year, whichever is higher. This includes obligations of providers (Article 16), authorised representatives (Article 22), importers (Article 23), distributors (Article 24), deployers (Article 26), and requirements and obligations of notified bodies (Article 31, Article 33(1), (3) and (4), or Article 34), as well as transparency obligations for providers and deployers (Article 50).
- Supplying incorrect, incomplete, or misleading information to notified bodies or national competent authorities in response to a request can result in fines of up to €7.5 million or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher.
- For SMEs, including start-ups, each fine is capped at the lower of the specified percentages or amounts.

C. Steps to Compliance:

1. **Understand and Categorise the Business's Biometric System**
    - Identify the Type of System:
        - › Determine if the business's system is a biometric categorisation system or a biometric identification system.
        - › Assess whether the business's system deduces sensitive attributes (e.g. race, political opinions, sexual orientation) or if it categorises non-sensitive attributes (e.g. hair colour, eye colour).
2. **Assess the Legal Requirements**
    - Prohibited Systems (Article 5(g)):
        - › Verify if the business's system deduces or infers sensitive attributes.
        - › Ensure that such systems are not placed on the market, put into service, or used.
    - High-Risk Systems (Article 6(2) and Annex III):
        - › Identify if the business's system falls under high-risk categories as defined in Annex III.
        - › Understand the regulatory requirements for high-risk systems.

3. **Implement Necessary Safeguards for High-Risk Systems**
   - Compliance with GDPR and EU Regulations:
     - Ensure all data processing complies with GDPR and relevant EU regulations.
     - Implement robust data protection measures.
   - Transparency and Notification:
     - Inform individuals exposed to high-risk biometric categorisation systems.
     - Provide clear information on data processing purposes and their rights.
4. **Conduct a Risk Assessment and Mitigation Plan**
   - Risk Analysis:
     - Perform a thorough risk assessment to identify potential harms and discriminatory impacts.
   - Mitigation Strategies:
     - Develop and implement strategies to mitigate identified risks.
     - Regularly review and update mitigation measures.
5. **Documentation and Record-Keeping**
   - Maintain Records:
     - Keep detailed records of compliance measures, risk assessments, and mitigation plans.
     - Document the decision-making process and any consultations with legal or technical experts.
6. **Regular Monitoring and Audits**
   - Continuous Monitoring:
     - Regularly monitor the operation of high-risk systems for compliance.
     - Implement a mechanism for ongoing review and improvement.
   - Independent Audits:
     - Conduct independent audits to ensure compliance with the AI Act and related regulations.
7. **Training and Awareness**
   - Employee Training:
     - Train employees on compliance requirements, data protection, and ethical use of biometric systems.
     - Ensure all staff understand the importance of adhering to legal and regulatory standards.

Conclusion

In summary, while the AI Act provides a structured approach to regulating biometric categorisation systems, the fine line between prohibited and high-risk applications demands thorough understanding and careful application of the law. The potential for confusion underscores the need for clear guidance and robust compliance mechanisms to ensure that the deployment of such technologies aligns with both legal requirements and ethical standards.

8. Emotion Recognition Systems

Introduction

Emotion recognition systems will now be regulated under the AI Act. These systems, which infer or identify emotions from biometric data, present unique challenges and risks that demand stringent regulatory measures. This section outlines the steps to ensure compliance with the AI Act.

Key AI Act Articles:

Article 3 - Definitions

Article 5 – Prohibited AI practices

Article 6 – Classification rules for high-risk AI systems

Article 9 - Risk management system

Article 16, 22, 23, 24, 26, 31, 33, 34, 50 – Obligations on parties

A. Overview of Emotion Recognition Systems

DEFINING EMOTION RECOGNITION SYSTEMS

According to Article 3(39) of the EU AI Act, an "emotion recognition system" is defined as an AI system that identifies or infers emotions or intentions based on biometric data. Biometric data, as per Article 3(34), includes any personal data resulting from technical processing of physical, physiological, or behavioural characteristics such as facial images or fingerprints. Recital 18 further elaborates that emotion recognition systems encompass AI technologies that identify a range of emotions including happiness, sadness, anger, and more. However, it excludes systems detecting physical states like fatigue unless such systems are used for safety purposes, such as those preventing accidents involving pilots or drivers, and that are otherwise captured by the AI Act.

PROHIBITIONS AND HIGH-RISK CLASSIFICATIONS

The EU AI Act takes a cautious approach towards the deployment of emotion recognition systems in sensitive environments. Article 5(1)(f) outright prohibits the use of these systems in workplaces and educational institutions, unless they serve a medical or safety purpose. This prohibition stems from concerns articulated in Recital 44, which highlights the significant scientific uncertainties and potential discriminatory outcomes associated with these technologies. The variability in emotional expressions across different cultures and individuals can lead to unreliable and biased results, thus justifying their restricted use in contexts where power imbalances are pronounced.

Moreover, Annex III of the AI Act categorises emotion recognition systems as high-risk AI systems, subject to stringent regulatory requirements. This classification is rooted in Recital 54, which underscores the potential for biased and discriminatory outcomes, particularly when these systems are used for critical applications involving biometric data.

TRANSPARENCY AND DATA PROTECTION OBLIGATIONS

Transparency is a cornerstone of the AI Act’s regulatory framework. Article 50(3) mandates that deployers of emotion recognition systems must inform individuals exposed to these technologies about their operation. This requirement ensures that individuals are aware of when their biometric data is being processed to infer emotions. This transparency obligation is complemented by the GDPR, which governs the processing of personal data, including biometric data, under Regulations (EU) 2016/679 and (EU) 2018/1725.

The GDPR, particularly through its stipulations on special categories of personal data under Article 9(1), reinforces the stringent protections around biometric data. Any processing of such data must comply with the GDPR’s requirements, ensuring that the rights and freedoms of individuals are safeguarded. Recital 132 of the AI Act reiterates that transparency obligations must be fulfilled in a manner accessible to all, especially considering the needs of vulnerable groups such as individuals with disabilities.

BALANCING INNOVATION AND REGULATION

The EU AI Act’s stringent measures on emotion recognition systems reflect a balanced approach aimed at fostering innovation while protecting fundamental rights. By categorising these systems as high-risk and imposing strict transparency and data protection obligations, the Act seeks to mitigate the potential harms associated with these technologies.

Recital 63 clarifies that the high-risk classification does not inherently legalise the use of emotion recognition systems under other Union or national laws. Instead, their deployment must always align with existing legal frameworks, including the Charter of Fundamental Rights of the European Union and the GDPR. This ensures a comprehensive legal oversight that transcends the AI Act’s provisions, embedding robust safeguards against the misuse of biometric data.

Key Dates:

- **12 July 2024:** The AI Act published in the Official Journal.
- **1 August 2024:** The AI Act will become law.
- **2 February 2025:** Article 5 Emotion Recognition Systems in the workplace or educational settings are banned.
- **2 August 2026:** Rules on Annex III Emotion Recognition Systems come into effect.

B. Enforcement and Penalties

- Non-compliance with the rules on Prohibited AI Systems will attract substantial administrative fines of up to €35 million or, if an undertaking, 7% of the offender's total worldwide annual turnover, whichever is higher. Non-compliant AI systems can also be taken off the EU market.
- The AI Act imposes significant fines for non-compliance with its provisions, especially for high-risk AI systems. Non-compliance with specific obligations related to operators or notified bodies can result in administrative fines of up to €15 million or, if the offender is an undertaking, up to 3% of its total worldwide annual turnover for the preceding financial year, whichever is higher. This includes obligations of providers (Article 16), authorised representatives (Article 22), importers (Article 23), distributors (Article 24), deployers (Article 26), and requirements and obligations of notified bodies (Article 31, Article 33(1), (3) and (4), or Article 34), as well as transparency obligations for providers and deployers (Article 50).
- Supplying incorrect, incomplete, or misleading information to notified bodies or national competent authorities in response to a request can result in fines of up to €7.5 million or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher.
- For SMEs, including start-ups, each fine is capped at the lower of the specified percentages or amounts.

C. Steps to Compliance:

1. Understand the Scope and Definitions

- Emotion Recognition Systems: Consider whether the business's system fits the definition of 'emotion recognition system' in Article 3(39), identifying or inferring emotions from biometric data (as defined in Article 3(34)).

2. Assess Prohibitions and High-Risk Classifications

- Prohibitions: Verify that the business's use case does not fall under prohibited scenarios, such as use to infer emotions in workplaces or educational institutions, unless for medical or safety purposes (Article 5(1)(f)).
- High-Risk Systems: Determine if the business's system is classified as high-risk under Annex III, which requires stringent regulatory compliance.

3. **Implement Transparency Measures**

   - Inform Affected Individuals: As mandated by Article 50(3), inform individuals when their biometric data is being processed to infer emotions. Ensure this information is accessible, considering the needs of vulnerable groups (Recital 132).

4. **Ensure Data Protection Compliance**

   - GDPR Alignment: Align the business's data processing activities with the GDPR requirements, particularly regarding special categories of personal data (Article 9(1) GDPR).
   - Safeguards: Implement appropriate safeguards to protect the rights and freedoms of individuals, as required by the GDPR and reiterated in Recital 132 of the AI Act.

5. **Conduct Risk Management**

   - Risk Assessment: Perform a thorough risk assessment to identify potential biases and discriminatory outcomes, as highlighted in Recitals 44 and 54.
   - Mitigation Measures: Implement measures to mitigate identified risks, ensuring the system's fairness and reliability.

6. **Maintain Documentation and Records**

   - Record Keeping: Maintain detailed records of compliance efforts, including transparency measures, risk assessments, and data protection safeguards.

7. **Engage with Regulatory Authorities**

   - Consultation: Engage with relevant regulatory authorities to ensure the business's compliance strategy aligns with the latest regulatory expectations and guidelines.

8. **Continuous Monitoring and Improvement**

   - Ongoing Review: Continuously monitor the performance of the business's emotion recognition system and review compliance measures regularly.
   - Updates and Training: Keep the personnel informed about updates in regulations and provide regular training on compliance requirements.

9. **Legal and Ethical Considerations**

   - Legal Alignment: Ensure the system's deployment aligns with the Charter of Fundamental Rights of the European Union and other relevant legal frameworks.
   - Ethical Standards: Adhere to ethical standards, promoting transparency, fairness, and accountability in the use of emotion recognition technologies.

Conclusion

The regulation of emotion recognition AI systems under the EU AI Act marks a significant advancement in AI governance. By defining these systems, identifying their risks, and embedding stringent transparency and data protection measures, the EU aims to harness the benefits of AI while mitigating its risks. The interplay with the GDPR further strengthens the regulatory landscape, ensuring that the deployment of emotion recognition technologies respects individual rights and maintains public trust. As AI continues to evolve, such comprehensive regulatory frameworks will be crucial in balancing innovation with ethical considerations.

9. Extraterritorial Reach

Introduction

The AI Act is poised to become a landmark piece of legislation in AI regulation, with its extraterritorial scope being one of its most significant and far-reaching aspects. This article examines the extraterritorial provisions of the AI Act and their implications for global AI governance, focusing on the obligations of providers of high-risk AI systems and general-purpose AI (GPAI) models and the crucial role of authorised representatives.

Key AI Act Articles:

Article 2– Scope

Article 3 – Definitions

Article 22 – Authorised Representatives of providers of high-risk AI systems

Article 54 – Authorised Representative

Article 53 – Obligations for Providers of General-Purpose AI Models

A. Scope and Extraterritorial Reach

The scope of application for the AI Act is outlined in Article 2, encompassing actors both within and outside the EU. According to Article 2(1)(a), the AI Act applies to providers placing on the market or putting into service AI systems or GPAI models in the EU, irrespective of whether those providers are established or located within the EU or in a third country.

The extraterritorial nature of the AI Act is particularly evident in its application to providers and deployers of AI systems established in third countries. Article 2(1)(c) specifically addresses this extraterritorial reach by including providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the system is used in the EU. This output-based jurisdiction is a key aspect of the AI Act's extraterritorial scope.

B. Role of Authorised Representatives for Providers Established Outside the EU

A key mechanism for enforcing the extraterritorial reach of the AI Act is the concept of the "authorised representative." An 'authorised representative' is defined under Article 3(5) of the AI Act as a natural or legal person located or established in the EU who has received and accepted a written mandate from a provider of an AI system or a GPAI model who is established in a third country to perform and carry out on its behalf the obligations and procedures established by the AI Act.

The AI Act distinguishes between authorised representatives for high-risk AI systems (Article 22) and those for GPAI models (Article 54). However, the underlying principle remains the same: ensuring accountability within the EU's jurisdiction.

C. High-Risk AI Systems

Article 22 of the AI Act mandates that providers of high-risk AI systems established in third countries must appoint an authorised representative in the EU before making their systems available on the EU market. The authorised representative's responsibilities include:

- verifying the EU declaration of conformity and technical documentation;
- keeping these documents and other relevant information at the disposal of competent authorities for ten years;
- providing information and documentation to competent authorities upon request;
- cooperating with authorities on risk mitigation actions; and
- complying with registration obligations where applicable.

Importantly, Article 22(4) of the AI Act empowers the authorised representative to terminate the mandate if they believe the provider is acting contrary to the AI Act, and requires them to inform the relevant market surveillance authority and notified body about such termination.

D. General-Purpose AI Models

Similarly, Article 54 of the AI Act requires providers of GPAI models established in third countries to appoint an authorised representative in the EU. Their responsibilities include verifying technical documentation, providing information to demonstrate compliance, and cooperating with authorities on actions related to the GPAI model.

These provisions ensure that there is always an entity within the EU's jurisdiction that can be held accountable for compliance with the AI Act, regardless of where the AI system or model originates.

E. Obligations for Providers

Article 53 of the Act outlines specific obligations for providers of GPAI models, which apply regardless of the provider's location. These include maintaining technical documentation, providing information to AI system providers who intend to integrate the model, complying with EU copyright law, and publishing a summary of training content.

F. Context and Justification

Recital 22 of the AI Act provides crucial context for understanding the extent of the AI Act's extraterritorial application, stating that certain AI systems should fall within the scope of the AI Act even when they are not placed on the market, put into service, or used in the EU. This includes scenarios where an EU-based operator contracts services to a third-country operator involving an AI system that would qualify as high-risk.

Recital 106 of the AI Act further extends the extraterritorial reach in the context of copyright compliance, stipulating that providers of GPAI models must comply with EU copyright law, regardless of where the training of these models takes place. This ensures a level playing field among providers, preventing competitive advantages based on less onerous legal obligations applying outside the EU.

G. Implications for Global AI Governance

The extraterritorial scope of the AI Act has significant implications for global AI governance. The AI Act's broad reach, along with the requirements for authorised representatives and specific obligations for providers, may encourage non-EU companies and countries to align their AI development and deployment practices with EU standards to maintain access to the EU market. This could potentially lead to the AI Act becoming a de facto global standard for AI regulation.

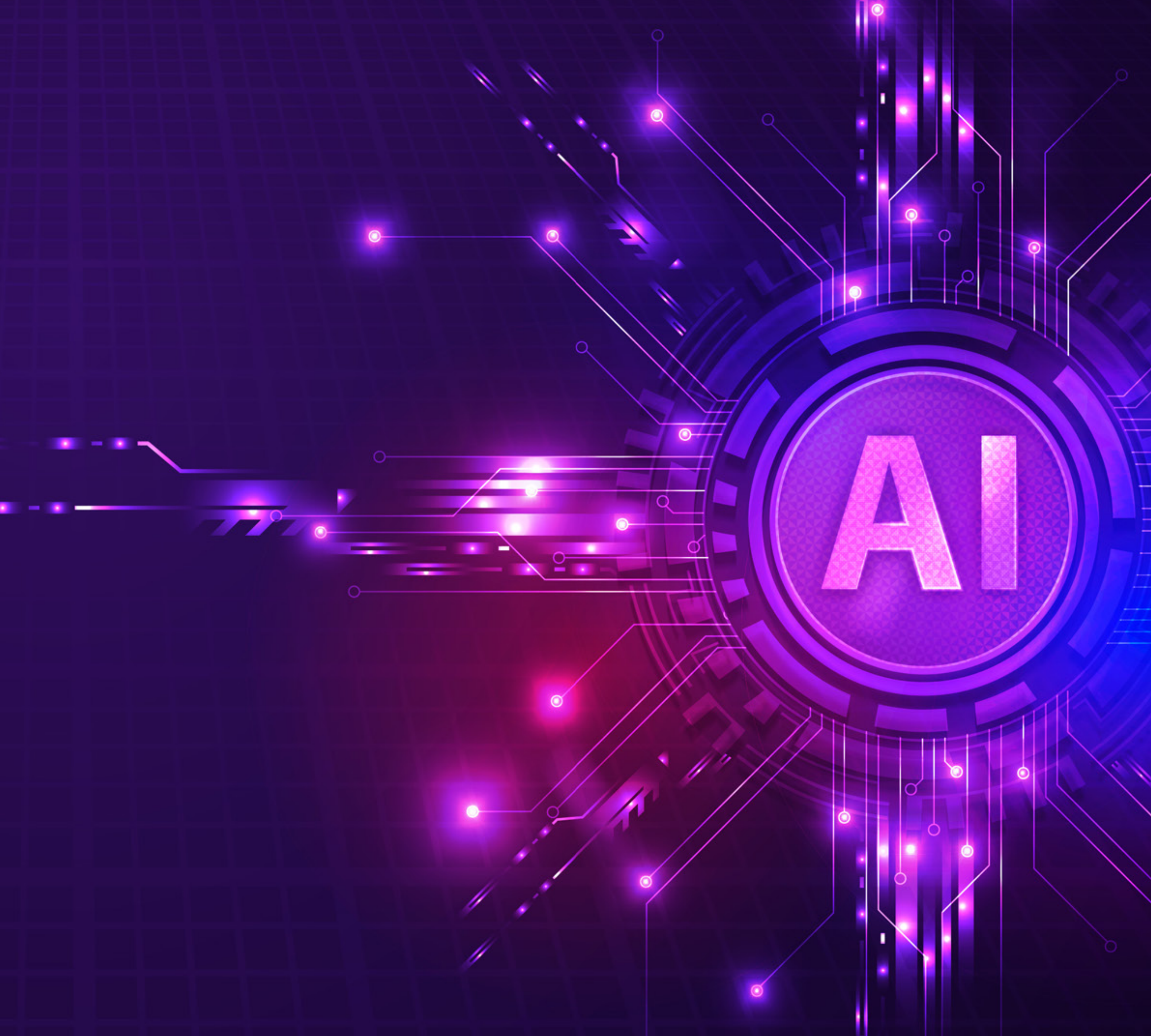
However, these provisions may also create challenges for companies operating across multiple jurisdictions. Non-EU entities will need to carefully assess their AI systems, ensure compliance with the AI Act, establish a presence in the EU through an authorised representative, and meet the various obligations if they intend to serve EU customers or process EU-origin data, even if their AI systems are not directly deployed within the EU.

Conclusion

The extraterritorial scope of the AI Act represents a bold and comprehensive step in regulating AI on a global scale. By extending its reach beyond EU borders, requiring representation for third-country providers, and imposing specific obligations on providers of both high-risk AI systems and GPAI models, the AI Act aims to ensure comprehensive protection for EU citizens and maintain a level playing field for AI providers serving the EU market.

As the AI Act moves towards implementation, its extraterritorial provisions will likely spark further debate and potentially influence the development of AI governance frameworks worldwide. Stakeholders across the global AI ecosystem must closely monitor these developments and adapt their strategies to navigate this evolving regulatory landscape.

PART 2
A Practical Guide to AI Legal Issues



1. AI and Intellectual Property

Introduction

Understanding the interaction between AI and IP rights is critical for organisations. This section addresses the legal implications of using copyrighted materials to train AI and the IP complexities of AI-generated content. Proactively managing these IP issues is essential to mitigate risks and leverage AI's potential effectively.

AI, systems, which rely on large datasets for training, present unique challenges concerning intellectual property (IP) rights. As AI is increasingly integrated into various business operations, understanding these IP implications becomes crucial for organisations.

A. Overview

Many potential issues arise in relation to IP rights, particularly with regards to IP infringement and ownership. This section provides an overview of the critical IP considerations for organisations, focusing on the materials used to train AI systems (**Inputs**) and the content they generate (**Outputs**).

B. Issues to Consider

INPUT

Typically, general-purpose AI systems are trained using a substantial dataset, which often contain IP protected material scraped from the internet via a process known as text and data mining (**TDM**). The TDM process may constitute copyright infringement unless authorisation (such as a licence) has been obtained from the relevant rightsholder or the TDM is carried out on the basis of a lawful exception.

OUTPUT

The content generated by AI systems can also give rise to IP issues:

- **Infringement:**
  Whether an organisation is developing or deploying an AI system, the nature of its Output can result in IP infringement. Where the AI system has been trained on protected works, Output that reproduces or resembles any of the protected works could attract claims of infringement. Liability here could exist both for the organisation which developed the AI system, and for the organisation deploying it, depending on the terms of use between the parties. Different IP rights other than copyright may also be similarly affected, including trade marks, patents or even trade secrets.

- **Ownership:**
  Determining the ownership of AI-generated works can be complex. Courts globally are grappling with the question of ownership of content generated using AI. In some decisions to date, there has been a requirement for human authorship to enjoy copyright protection, as seen in recent rulings in the US, UK, and some parts of the EU. The U.S. Copyright Office and US courts have been explicit in their determination that in the U.S, works created by AI cannot obtain a copyright registration. In Ireland however, there may be scope for IP rights to be attributable to AI Output. Under Irish law, the *'author'* of a work which is computer-generated is the "*person by whom the arrangements necessary for the creation of the work are undertaken*". Some experts believe this could apply in the context of works generated by AI. Further questions arise over whether the person who made the necessary arrangements is the individual who prompted the AI system, or the individual or company who created the AI system, or perhaps a combination of these. While there is a path by which AI Output may attract IP protection in Ireland, issues of ownership of such content have yet to be tested in the Irish courts.

C. Next Steps

- **Audit AI Training:** review datasets used for AI training and ensure compliance with terms of use and licensing agreements, and/or reserve the organisation's rights in relation to the use of its proprietary information for the training of AI.
- **Implement Clear Policies:** establish policies regarding the use of third-party IP in AI training, the use of IP in prompting AI systems, and the ownership of AI-generated output.
- **Contractual Protections:** ensure that contracts for AI clearly outline IP rights, including licences, permissions and exceptions. It is important that these contracts also address potential liabilities and indemnities related to IP infringements.

INPUT

Organisations should consider the following in relation to training AI:

- **Dataset Terms of Use:** many publicly available datasets can be used for research purposes only. Organisations must ensure they have the right to use these datasets in a commercial context.

- **Rightsholders' Approval:** verify whether IP rights holders have given appropriate permissions for their work to be used for AI training purposes.
- **Exceptions for Use:** where there is no explicit permission from an IP rightsholder for the use of their work, organisations should check whether they could rely on another ground to use the material. For example, under EU law, there are exceptions which permit the use of publicly available copyright material for TDM if the owner has not expressly reserved their rights against TDM.

Organisations seeking to protect their IP should consider the following:

- **Reservation of Rights:** organisations which wish to prevent the use of their data for TDM purposes should ensure that they have expressly and appropriately reserved their rights in this regard.
- **Licences:** organisations should ensure that any licence granted over the use of their IP is sufficiently clear about the use permitted of protected material for AI-training purposes.
- **Confidentiality/Ownership of Prompts:** particular attention should be paid to contractual clauses relating to confidentiality and ownership over any input to the relevant AI system, to mitigate risks relating to inadvertent loss of IP protection or disclosure of protected works.

OUTPUT

Organisations should consider the following in relation to Output:

- **Human Involvement:** it is important to determine whether works created with the help of AI had sufficient human contribution to secure protection under different IP legislative regimes.
- **Other Barriers to IP protection:** before AI is deployed, organisations should consider whether they will be able to assert IP rights over the content generated. Could the Output inadvertently infringe on a third party's IP rights? Do the terms of any licence to use the AI system prevent ownership over the Output? Is any open source code used which may prevent IP ownership?
- **IP Infringement:** establish whether any of the organisation's IP rights have been infringed by AI systems. While AI systems are often trained on third party datasets, IP rightsholders must prove that their works have been actually copied, regardless of potential similarities to the protected works in the Output.

Conclusion

AI brings various IP considerations for organisations, whether the organisation needs to protect its IP or whether the organisation develops or deploys AI itself.

2. AI and Data Protection

Introduction

Artificial Intelligence (**AI**) systems, especially generative AI, often rely on processing large volumes of data, which very often includes personal data (**PD**). This places them firmly within the scope of the General Data Protection Regulation (**GDPR**), raising significant concerns about privacy and data protection. While AI is not explicitly referenced in the GDPR, the GDPR is technology-neutral, such that many of its provisions are relevant to AI (e.g. profiling, automated decision-making, etc.) and equally challenged by it. The GDPR and AI Act will apply in tandem, meaning compliance with each legal regime is necessary. Owing to the interplay between AI and data protection, the AI Act makes various references to the GDPR and its application to AI systems.

Ultimately, AI represents a new way of processing PD, given AI systems' dependency on data. This reality lends itself to the GDPR's risk- and principles-based legal framework. Moreover, the evolving nature of the risks associated with AI technologies is such that GDPR compliance lends itself to addressing and mitigating them – for example, through conducting risk assessments (such as Data Protection Impact Assessments (**DPIAs**) and legitimate interest assessments), maintaining records of processing activities, implementing appropriate technical and organisational measures, implementing privacy by design and privacy by default and complying with transparency obligations.

Navigating this intersection of AI and data protection requires careful consideration. Here is what organisations need to know:

A. Overview

It is recommended that organisations adopt a principles-based approach when deploying or developing AI systems and governance, by applying the data protection principles outlined in the GDPR. The assessment of the interplay between AI and data protection obligations will be context-specific in each case.

The GDPR has several key principles that may present challenges for organisations acting as controllers when using AI systems, namely:

1. TRANSPARENCY, LAWFULNESS AND FAIRNESS

A fundamental aspect of the GDPR is that PD must be processed, lawfully, fairly and in a transparent manner.

1.1 Lawfulness of Processing

1.1.1 To process any PD, a controller must have a legal basis to do so under the GDPR. When it comes to AI systems, the applicable (and appropriate) legal basis/bases to legitimise the processing of PD will be hugely context-specific and, in most instances, will be preconditioned by a "necessity" requirement under the GDPR. For example:

1.1.2 The type of AI system – how was it trained, with what data, how will it be deployed/function, etc.?

1.1.3 The purposes for which an AI system is being trained and/or deployed by the controller – what is the AI system seeking to address for the controller (i.e. the use case)?

1.1.4 The controller's relationship with the individuals whose PD will be processed – is it direct or indirect?

1.1.5 Is there an existing data protection notice implemented such that the purposes of processing via an AI system are compatible with the original purposes of processing and within the reasonable expectations of individuals?

1.1.6 In general, the AI Act does not provide an express legal basis for controllers to process PD for the purposes of an AI system. As such, a legal basis under the GDPR must be identified (subject to certain exceptions to this position under the AI Act).

1.1.7 It is best practice to consider the applicable legal basis/bases for each phase of an AI system's lifecycle (to the extent applicable for a controller), be that training, development and/or deployment, along with the data protection role of each actor concerned in the processing. The applicable legal basis/bases will differ for a provider and deployer because they will generally have different purposes for processing PD.

1.2 Fairness

1.2.1 The principle of fairness is a crucial aspect of GDPR compliance regarding the interplay between AI and data protection due to the potential for bias and discrimination. PD must not be processed in a manner that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to individuals.

1.2.2 An important aspect of compliance with this principle is that the responsibility for ensuring compliance with the GDPR should not be transferred from a controller to end users. Controllers must not include provisions in their terms and conditions of use that data subjects are responsible for their inputs, as ultimately, it is the controller that is responsible for complying with the GDPR.

1.2.3 Transparency

1.2.3.1 Informing individuals about how their PD have been obtained, why their PD will be processed and how they will be used is all part of the GDPR's transparency obligations. However, this is challenged when it comes to AI systems because it is not possible, in every use-case, to identify:

1.2.3.2 the source of data which trained an AI system (particularly where data have been scraped from the internet or taken from user-generated content);

1.2.3.3 how an AI system operates and processes PD (e.g. the opacity of how an AI system works can be a black box and not a glass box);

1.2.3.4 whether an AI system uses PD; and

1.2.3.5 whether the use of PD by an AI system is within the reasonable expectations of individuals (e.g. to whom the PD relates).

1.3 See also our AI Literacy Practical Guide.

2. Accuracy

2.1 AI, particularly public and "out of box" generative AI systems, poses challenges for the GDPR's data accuracy principle. These AI systems can be very accomplished at giving output data that is factually incorrect (e.g. AI hallucinations) but the GDPR requires organisations to ensure the accuracy of all PD processed and that it is up-to-date.

2.2 In practice, it will be critical to implement policies (including human involvement and human intervention) to ensure accuracy at each stage of an AI system's lifecycle in a reasonable and proportionate manner (e.g. data collection, data analysis, etc.). For example, once an AI system is operational, organisations should implement a policy to inform end users to verify the accuracy of any output data and not to presume such accuracy.

2.3 A further dimension to this principle is ensuring that PD remain up-to-date. As such, it will be necessary to assess whether an AI system remains dynamic once it is in operation, such that it is continually autonomous, self-learning, adapting and changing, as this means data may be continually updated and, therefore, processed.

3. Data subject rights

3.1 AI systems must respect and facilitate the exercise of data subject rights under the GDPR, including access, rectification, and erasure of data. Implementing privacy by design and default principles, and maintaining accurate records of processing activities are essential for compliance.

B. Issues to Consider

1. Determine your organisation's obligations under the GDPR.

As a first step, from an accountability perspective, there are certain key factual questions to assess to determine your obligations as a controller of PD, namely:

a. **what** is the AI system being used for? and

b. **who** is using the AI system?

2. Determine what impact assessments your organisation must conduct

In addition to the well-established circumstances in which a Data Protection Impact Assessment (DPIA) must be conducted under Article 35 of the GDPR, the AI Act also requires a DPIA to be conducted for high-risk AI systems. In practice, a combined DPIA that meets the requirements of both the GDPR and the AI Act will meet a controller's obligations under each piece of legislation.

Deployers of an AI system may also be required to conduct a Fundamental Rights Impact Assessment (**FRIA**) under the AI Act. Where a FRIA must also be conducted by a controller (in addition to a DPIA), the elements of a FRIA can be included in the same DPIA – meaning one document will suffice. It is recommended that existing template DPIAs be reviewed and revised to ensure that they meet the requirements of both the GDPR and the AI Act.

If you rely on legitimate interests as a legal basis, then you will need to consider a legitimate interest assessment.

3. Train your staff

The AI Act's AI literacy requirements impose an obligation on providers and deployers of AI systems to take measures that ensure a sufficient level of AI literacy among their staff and other persons dealing with the operation and use of AI systems on their behalf. In complying with this requirement, providers and deployers must take into account the technical knowledge, experience, education and training of staff in the context of the AI system(s) being used and the persons or groups of persons on which the AI system(s) are to be used.

C. Next Steps

In summary, AI developers and deployers must comply with the GDPR and demonstrate compliance with their accountability legal framework. This means leveraging existing data protection governance frameworks to deploy AI systems. To ensure compliance and mitigate risks, organisations should:

1. Review the lawful basis of all processing related to the use and/or training of AI systems within your organisation.

2. Assess the necessity and appropriateness of PD processing by AI systems, prioritising data protection and privacy considerations.

3. Create an inventory of AI systems deployed or under development, including those from external vendors and partners.

4. Conduct comprehensive AI impact assessments to identify and mitigate risks, aligning with GDPR and AI Act requirements, which may include DPIAs/FRIAs.

5. Review, adapt, and revise data protection policies, documents, due diligence questionnaires, and vendor contracts to incorporate AI-specific requirements and safeguards.

6. Provide ongoing training and awareness initiatives to ensure staff understand the ethical and legal implications of using AI systems, emphasising data protection and privacy.

Conclusion

By embracing these considerations and integrating data protection principles into AI governance, organisations can foster trust, accountability, and compliance in AI-driven initiatives.

3. AI and Cybersecurity

Introduction

Since the advent of large language models and other forms of generative AI, organisations have witnessed the transformative power of this technology. Many businesses (perhaps unknowingly) already leverage AI to streamline processes and plan to further capitalise on its potential. Despite their benefits, such emerging technologies can create vulnerabilities within organisations, making them more susceptible to cyberattacks. At the same time, threat actors are incorporating AI into their arsenal to hack systems.

In this brief guide, we explore the interplay between AI and cybersecurity, as well as the legislation coming down the tracks to regulate these areas.

A. Overview

The emergence of new technologies has altered the threat landscape in the cybersecurity space. In response to this, and as part of the EU's Digital Reforms Package, the EU has revised existing cybersecurity rules and proposed new legislation concerning cybersecurity and AI.

Organisations should consider the legislation coming down the tracks in this space:

1. NIS 2 Directive (NIS 2)

NIS 2 is an overarching cybersecurity framework which will replace previous EU cybersecurity laws under the NIS 1 Directive. NIS 2 aims to protect critical infrastructure and operational resilience by harmonising cybersecurity standards across Member States. NIS 2 will enter into force on 18 October 2024. It triggers legal obligations for a wider span of critical infrastructure entities in various sectors, meaning that organisations previously not in scope of EU cybersecurity legislation may now be caught. In-scope entities must implement technical, operational and organisational measures to comply with cyber risk management, reporting and information sharing. They must analyse their business operations, including the use of any machine learning or AI technologies, to ensure that robust cybersecurity systems are in place.

2. EU Artificial Intelligence Act (AI Act)

Organisations deploying AI must also take note of the incoming AI Act. The AI Act divides AI systems into different categories based on their risk categorisation and prescribes rules accordingly. Organisations deploying 'high risk' AI systems should note that, under the AI Act, they must ensure that such systems meet certain cybersecurity and resilience standards and perform consistently in those respects throughout their lifecycle. This includes incorporating, where appropriate, technical solutions to prevent, detect, respond to and control data poisoning, model poisoning, model evasion, confidentiality attacks or model flaws.

3. Cyber Resilience Act (CRA)

Manufacturers of software or hardware with digital elements will come under the scope of the impending CRA. This piece of legislation, still in draft form, will require manufacturers to incorporate cybersecurity into the design, development and distribution of products, test for and remediate vulnerabilities of products both pre- and post-launch on the market, and undertake conformity assessments of products to demonstrate compliance with cybersecurity obligations. Where such products comprise an AI system, this system will need to be taken into account in meeting these obligations.

B. Issues to Consider

1. **Regulatory Compliance**
   The new cyber laws (such as NIS 2) render cybersecurity a non-negotiable issue for organisations and a board-level issue. Organisations should assess whether they fall within the scope of NIS 2, the AI Act and/or the CRA, either due to the nature of their business, the size of their organisation or their use of AI. Where businesses are caught by these laws, it is imperative that they prepare to meet the obligations imposed under NIS 2. Significant penalties are attributable to non-compliance, with organisations facing substantial fines. Notably, board members will be subject to personal liability for non-compliance with cybersecurity obligations under NIS 2 from October 2024. As such, organisations must focus on whether they are subject to NIS 2's baseline standards and implement them into security frameworks accordingly.

2. **Strategic Implementation of AI**
   While organisations should be aware of the potential for AI systems to expose them to greater vulnerabilities, they should also note that AI can be a valuable tool for increasing cyber-resilience. AI has multiple applications in cybersecurity, from fraud detection to analysis and prevention. An increasing number of organisations are already deploying AI to assist their cybersecurity personnel to defend against cyberattacks. AI can identify and mitigate potential cyber risks by analysing data and detecting weaknesses in software and networks via penetration testing. The ability of AI to analyse communication patterns makes it particularly useful in recognising and intercepting phishing attempts and even in simulating such attacks to help train employees. Under NIS 2, organisations are encouraged to use machine learning or AI systems to enhance their cybersecurity capabilities and the security of network and information systems.

C. Next Steps

Organisations should take the following steps to address AI and cybersecurity challenges effectively:

1. **Conduct Comprehensive Audits**
   Evaluate current AI and cybersecurity practices to identify vulnerabilities and compliance gaps. This includes analysing the use of AI technologies and their potential impact on cybersecurity.

2. **Engage with Legal and Technical Experts**
   Consult with legal advisors and cybersecurity professionals to navigate the complexities of emerging legislation such as NIS 2 and the AI Act. Develop a proactive strategy to ensure compliance and mitigate risks.

3. **Integrate AI Thoughtfully**
   Consider using AI not only as a tool for efficiency but also as a means to bolster cybersecurity. Ensure that AI systems are designed and implemented with security in mind, addressing potential vulnerabilities from the outset.

Conclusion

Organisations must recognise the intertwined nature of AI and cybersecurity. The EU's Digital Reforms Package, including the NIS 2 Directive, AI Act, and draft CRA, underscores the importance of integrating robust cybersecurity measures in AI deployment (and more generally).

Businesses should develop a solutions-oriented roadmap to navigate these regulatory landscapes and enhance their cyber resilience. William Fry's Technology Regulation team is equipped to guide organisations through these challenges, ensuring they thrive in the digital era.

Note: NIS 2 will take effect on 18 October 2024. At the time of publication of this text, the transposing legislation has not been introduced under Irish law

4. AI and Contracts

Introduction

Organisations are increasingly using AI solutions to drive innovation, enhance productivity, streamline operations and gain a competitive edge.

Contracting for AI solutions involves unique challenges and considerations that differ significantly from traditional SaaS agreements. These complexities arise due to AI's dynamic and evolving nature, the vast amount of data it processes, and its inherent ability to learn and make autonomous decisions.

In this section, we outline the essential considerations to bear in mind from both a customer and a provider perspective when contracting for AI solutions via SaaS agreements.

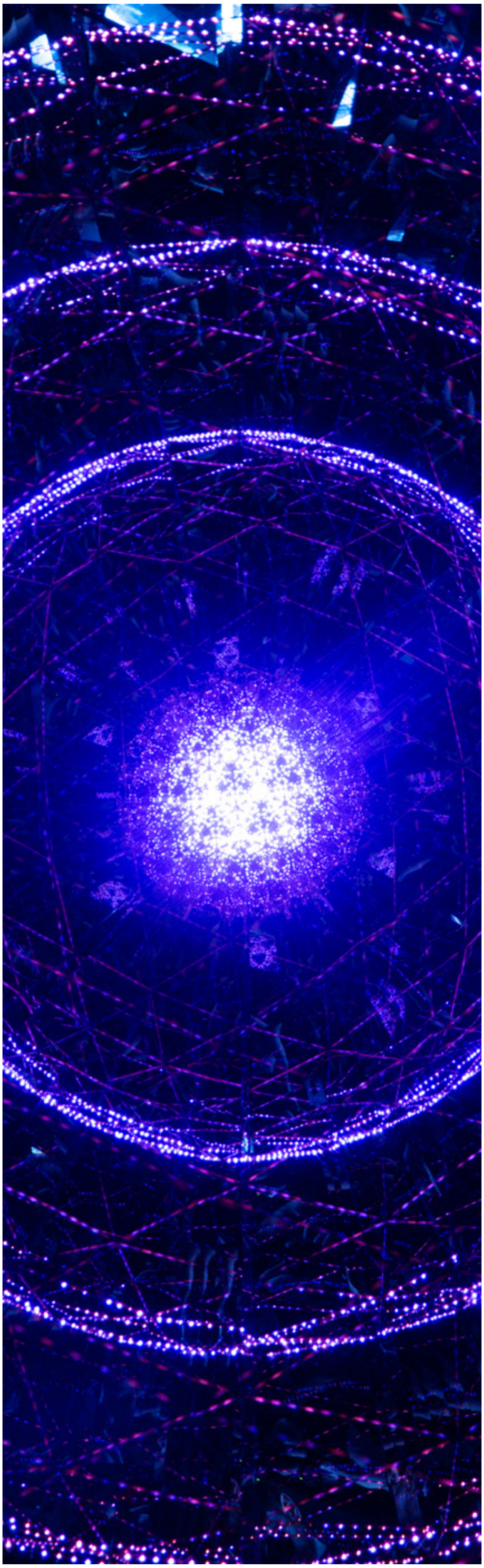
A. Overview of AI and Contracts

Contracting for AI solutions via SaaS agreements involves addressing unique complexities due to the dynamic nature of AI, its reliance on large datasets, and its capacity for autonomous decision-making. Key considerations include clearly defining the scope of AI services, specifying data rights and usage, determining intellectual property ownership, allocating liability, setting performance metrics, ensuring regulatory compliance, and establishing clear termination and exit strategies. These elements are crucial for managing risks and ensuring that both providers and customers understand their rights and responsibilities, thus fostering a transparent and effective partnership.

B. Issues to Consider

1. Comprehensive Due Diligence

Pre-signing, Customers should conduct a thorough due diligence process, led by legal and technical experts to evaluate the reliability, capability, and legal compliance of both the AI solution provider and the solution itself. Key aspects include assessing regulatory compliance, ownership of intellectual property, data management and security practices, technical proficiency, and the performance of the product.



2. Definition and Scope of AI Services

Clear and precise contractual definitions are crucial to differentiate between conventional software and AI-based systems. Parties should ensure that definitions are broad enough to encompass various AI types and processes, specific functionalities, and adaptive behaviours.

Providers should clearly define the scope of AI services, including functionalities, limitations, and intended use, to manage risks and customer expectations.

3. Data Management and Security

AI solutions depend heavily on data, making data management and security paramount. Contracts should address data sourcing rights, accuracy, integrity of training data sets, data management practices, compliance with data protection legislation and any data localisation or international transfer requirements. Responsibilities regarding data security and handling must be clearly defined.

Customers should also ensure that the contract contains a data deletion obligation upon termination of the contract (except for circumstances where the provider is required by law to retain a copy).

4. Intellectual Property Rights

Clear delineation of ownership rights to the AI technology and associated IP is essential. Contracts should define the ownership of inputs and data used for training the AI solution and the outputs generated by the AI system. Contracts should also address the licensing, use, and protection of existing IP incorporated into the AI solution.

5. Performance Standards and Metrics

Establishing performance standards and metrics is essential for evaluating the effectiveness of the AI solution. Customers should ensure that the contract contains clear, measurable standards for accuracy, efficiency, and other relevant metrics.

Providers should include flexible provisions to monitor and adapt performance metrics as the AI system evolves.

6. Modification and Scalability

Anticipating the need for modifications and scalability is crucial. Contracts should outline processes for updating the AI solution, incorporating new features, and scaling operations to meet evolving business needs. Flexibility in contractual terms enables adaptation to changing legal and technological requirements seamlessly.

7. Liability and Risk Allocation

Comprehensive liability provisions are crucial. However, addressing liability is often complex due to the autonomous nature of AI. Contracts should consider the allocation of liability, caps on liability, whether liability should be strict or fault based, and exclusion clauses.

Providers should have in place both an Acceptable Use Policy (AUP) and Terms of Use Policy (ToU) to mitigate risks associated with customer (and customer's end users) misuse of the AI solution.

8. Warranties

Warranties should address the unique nature of AI systems while guaranteeing specified performance, freedom from defects, and compliance with applicable laws.

Customers should seek warranties on data accuracy, non-discriminatory outputs, and where the AI system is continuously learning and evolving, a warranty that the learning and adaptation processes will not compromise the systems integrity or its compliance with specified standards.

Providers should ensure their warranties are accurate and that they have warranty and indemnity insurance in place.

9. Indemnities

Customers should seek indemnities for breaches of data protection legislation, IP infringement, and failure of the AI system to perform as agreed.

Providers should negotiate these provisions to achieve fair risk allocation, including strict caps on liability and exclusions for certain damages or claims.

10. Responsible AI Considerations and Regulatory Compliance

Embedding responsible AI considerations and regulatory compliance requirements into AI contracts is essential to ensure responsible AI deployment. Contracts should outline expectations for algorithmic transparency, fairness, and accountability, with mechanisms for auditing and oversight.

Customers should include provisions to ensure AI systems adhere to ethical principles and comply with relevant laws and regulations such as the GDPR and the AI Act.

Providers should include provisions guaranteeing that customers use the solution ethically and responsibly.

11. Future-Proofing the Agreement

Future-proofing AI related SaaS agreements requires proactive measures to anticipate and adapt to emerging technologies and regulatory frameworks. Clauses enabling renegotiation or automatic updates based on technological advancements or legal changes ensure that contracts remain relevant and enforceable over time.

C. Next Steps

Customers should prioritise the following steps:

1. **Determine your Requirements:** Conduct an initial assessment of your organisation's AI needs and its use cases for AI.

2. **Impact Assessments:** Conduct impact assessments to determine your organisation's risk appetite for integrating an AI solution. Determine the risks associated with implementing the specific AI system and whether these risks can be mitigated.

3. **Engage Experts:** Involve legal and technical experts early in the contracting process to ensure all relevant aspects are comprehensively addressed.

4. **Conduct Thorough Due Diligence:** Perform detailed evaluations of potential AI providers and solutions to ensure reliability, compliance, and suitability for your needs. We recommend using the AI Act as a benchmark to assess whether the provider has implemented appropriate technical and organisational measures, similar to how you would assess whether a processor, under the GDPR, has in place appropriate technical and organisational measures in place using Article 28(1) of the GDPR as a benchmark.

Providers of AI solutions should prioritise the following steps:

1. **AI Act Compliance:** At the outset, Providers must move towards ensuring that it, its products and services and the contracts governing same are compliant with the AI Act.

2. **Identify Objectives and Deliverables:** Identify what the customer is looking to achieve in deploying your AI solution and its intended use case in order to assess the product or service's suitability.

3. **Supporting Documentation:** Ensure that you have all of the supporting documentation in place for the AI solution, such as an AUP and ToU.

4. **Anticipate Questions:** Ensure that you are in a position to anticipate any questions that may arise during the due diligence process to avoid contractual delays. This includes, ensuring that you are able to provide information on your data management practices and any technical and organisational measures you have in place to ensure an adequate level of information security in relation to your products and services.

Conclusion

Contracting for AI solutions demands meticulous attention to detail and a comprehensive understanding of the nuances involved. By addressing the key considerations outlined above, organisations can mitigate the risks associated with AI and navigate the complexities of AI contracts effectively.

5. AI and Corporate Transactions

Introduction

The rapid growth of AI companies and the increasing use of AI technologies in 2023 and so far in 2024 has impacted the global M&A market. There were some major investments last year, including investments by Amazon and Microsoft who invested a combined $15.3 billion into AI companies such as OpenAI, Anthropic and InflectionAI. Whether a large or small investment into an AI company or a company using AI in its services, it is important to ensure that the due diligence process and resulting transaction documents accurately identify and address any risks raised during the process created by this new technology.

This section covers the practical steps investors should consider when investing in companies that use AI or provide AI as their product or service.

A. Overview of AI and Corporate Transactions

As we have seen in the past with the introduction of any new technology and its impact on corporate transactions, new issues arise, often based on existing principles. From an AI perspective, new issues arise from the innovative and dynamic nature of AI, such as the heavy reliance on the use of data to train AI models and the evolving global regulatory framework, such as the AI Act Such issues can arise in the due diligence stage and should be adequately reported on and addressed in the transaction documents.

B. Issues to Consider at the Due Diligence Stage

1. Ensure your Due Diligence Questionnaire includes AI specific questions:

A Due Diligence Questionnaire ("**DDQ**") is sent out at the outset of a due diligence ("**DD**") exercise. At the very least, especially if the target is an AI-based company, we recommend including questions in relation to the use, development, or otherwise of AI systems in the target company. Doing so at this early stage will help determine the use of AI by the target company and how it deploys it, in compliance with laws such as IP or the GDPR.

2. Review the AI Assets of the target company from an AI Act perspective:

Once you know whether the company uses or develops AI systems or not (as identified in the DDQ process or otherwise), the next step is to determine the applicability of the AI Act to the AI system either developed/owned or used by the target company. It is important to note that different types of AI systems carry varying obligations based on risk categorisation under the AI Act. Additionally, consideration should be given to evaluating the long-term viability and roadmap of the product from both a strategic and legal perspective to ascertain if it will be subject to future obligations including a CE marking and/or AI office registration under the AI Act.

3. Do your background on how the target develops/uses AI systems:

- **Training and Data Quality:** How has the AI model been trained? What measures are in place to ensure data quality and data rights?
- **Data Sources:** Where has the data been obtained that is used to train the data set?
- **Intellectual Property Rights:** If developing AI, how are the rights in the data and algorithms of the AI system protected? What measures has the target company taken to protect rights and know-how in the data, algorithms and software that constitute the AI product(s)? Any gaps in appropriate measures should also be identified.
- **Output Ownership:** Who owns the outputs of the AI system? Where do the ownership rights reside?
- **Confidentiality:** How is confidential information protected? Are there confidentiality clauses in contracts and NDAs in place where required?

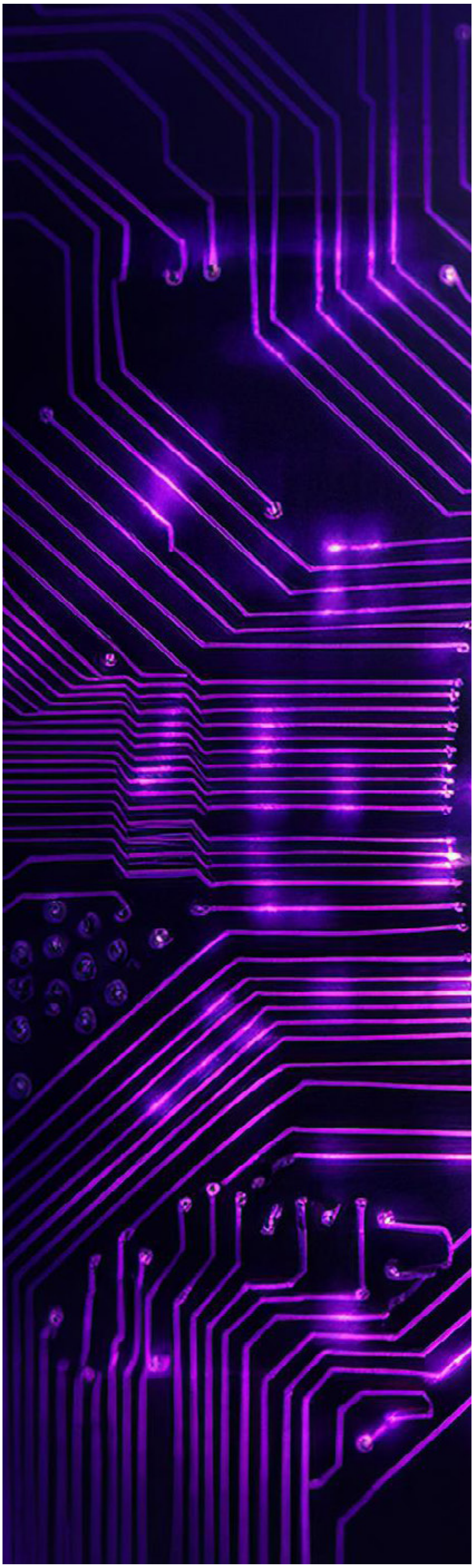
Remember that protecting AI innovation requires a combination of strategies involving a hybrid approach, including copyright, patent, third-party licences, licensing agreements, database protections and trade secrets.

4. Review contracts for risks specific to AI:

If a target company's main product is an AI product, an extensive review of the customer contracts and acceptable use policy should be conducted to ensure the following aspects are adequately addressed:

- › **IP Ownership:** Consider who owns the system's inputs and outputs and determine whether this would be considered a red flag in the context of the transaction.
- › **Data Re-Use Rights:** Assess the target company's rights to reuse customer data and any associated liability exclusions or limitations.
- › **Liability and Indemnities:** Assess the liability position of the target company and whether it provides an indemnity for potential damages caused by its tools or not.
- › **AI Act Compliance:** Although not a requirement until the AI Act comes into force, a review should be conducted of the customer terms of use to ensure compliance with the AI Act as well as the acceptable use policy of the AI system.

If the target company does not develop or sell AI as its main product or service but is heavily reliant on the use of AI in delivering its products or services, the same review should be conducted on the supplier contracts which the target company has with those AI providers. Of course, the assessment and reporting of these contracts will be substantially different on the customer side than the vendor side.



5. **Data protection risks of using AI:**

Keep in mind that the GDPR applies to AI systems processing personal data. Assess how the target company demonstrates compliance with the GDPR and the AI Act by evaluating its data and AI governance framework, including data quality control, data retention policies and data sharing practices.

When evaluating AI products that handle personal data, consider the following:

- **Data Origin:** Understand how the data has been obtained, including its source and origin.
- **Special Category Personal Data:** Assess whether the data includes special category personal data such as ethnic or political information.
- **Compliance Program:** Determine if the target company has a data protection compliance program in place and ensure it is materially compliant with data protection laws.

IMPACT ON TRANSACTION DOCUMENTS

As always, the DD conducted on a target company will impact the transaction documents such as the Share Purchase Agreement ("**SPA**") or Asset Purchase Agreement ("**APA**").

It may be the case that the current IP and IT representations and warranties are broad enough to cover any risks identified in the DD process from the use or development of AI systems. However, for transactions where AI is of strategic importance to the target company, it may be best to use the belt and braces approach and include AI-specific warranties in a similar way to how open-source software warranties for the unique risks posed by that software are incorporated. At a bare minimum, the warranties should cover IP rights in the AI product, third party licences and ownership, compliance with laws including data protection and the AI Act, if applicable and the absence of infringement claims or other product use-related claims.

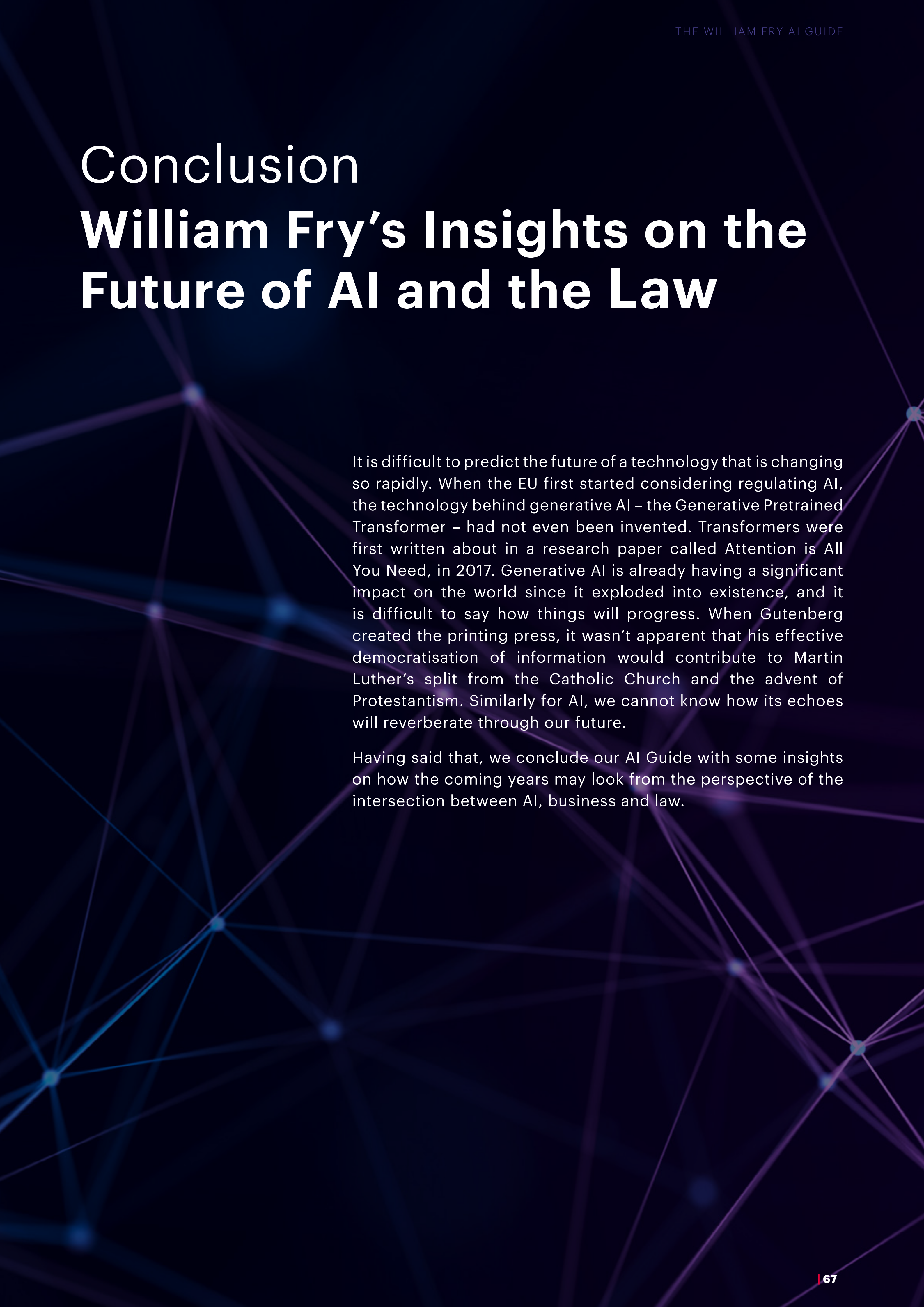
C. Next Steps

Although not entirely reinventing the wheel, it is essential to adjust the due diligence process in any corporate transaction when AI is involved. It is important to ask the right questions to get the right answers in the DD process. If the process reveals material risks in relation to the use or development of AI systems, this can impact the valuation or in more extreme cases, result in pens down on the deal.

It is therefore imperative that the due diligence process is carried out adequately and ensure that the risks identified are mirrored in the representations and warranties set out in the SPA or APA. It is also important to remember that so many legal implications concerning AI are currently unclear, meaning that such risks may be reduced or changed in the future as laws are developed to address this new technology.

Conclusion

As this analysis has demonstrated, conducting thorough due diligence is crucial in identifying and mitigating risks associated with AI. Investors must adapt their approaches to account for the evolving regulatory landscape, such as the AI Act, and ensure that transaction documents reflect these considerations. This involves including specific warranties related to AI, particularly concerning intellectual property rights, compliance with data protection laws, and AI governance frameworks. As AI continues to evolve, so too must the strategies employed in mergers and acquisitions, necessitating a dynamic and forward-looking approach to legal and commercial due diligence. This adaptability will be key to successfully navigating the complexities of AI in corporate transactions.



Conclusion
William Fry's Insights on the Future of AI and the Law

It is difficult to predict the future of a technology that is changing so rapidly. When the EU first started considering regulating AI, the technology behind generative AI – the Generative Pretrained Transformer – had not even been invented. Transformers were first written about in a research paper called Attention is All You Need, in 2017. Generative AI is already having a significant impact on the world since it exploded into existence, and it is difficult to say how things will progress. When Gutenberg created the printing press, it wasn't apparent that his effective democratisation of information would contribute to Martin Luther's split from the Catholic Church and the advent of Protestantism. Similarly for AI, we cannot know how its echoes will reverberate through our future.

Having said that, we conclude our AI Guide with some insights on how the coming years may look from the perspective of the intersection between AI, business and law.

Regulatory Frameworks: Balancing Innovation and Oversight

Governments are drafting comprehensive frameworks like the AI Act to ensure transparency, accountability, and ethical AI use. These regulations, while potentially costly, build trust and safety, crucial for widespread adoption. Companies that adapt early can showcase a commitment to ethical practices, gaining a competitive edge in trust-sensitive markets.

The emergence of AI-specific regulations signals a significant shift in governmental approaches to technology governance. Businesses must anticipate and adapt, investing in legal expertise and compliance infrastructure to meet new standards for AI transparency and accountability. This regulatory landscape may also drive innovation, as companies strive to meet higher safety and ethical standards, setting new benchmarks globally.

Some aspects of the AI Act remain unclear, with implementation guidelines by 2 February 2025, and Codes of Practice by 2 May 2025. Extraterritorial elements, in particular, may only be clarified through court decisions, and businesses' responses to these regulations remain to be seen.

Operational Efficiency and AI Liability: Opportunities and Challenges

AI improves operational efficiency by automating processes and enhancing decision-making but also introduces complex liability issues. Traditional liability frameworks may not adequately address scenarios involving autonomous systems like self-driving cars or AI-driven medical devices. Companies need to work with legal professionals to establish clear guidelines and insurance models defining liability and accountability. This will likely lead to new legal concepts and insurance products tailored to AI.

Navigating these challenges requires businesses and legal frameworks to evolve together, potentially creating new liability structures and insurance models specific to AI systems. This evolution can spur innovation in both legal and business practices, fostering better risk management strategies.

Data Governance and Strategic Business Impact

The reliance on data for AI highlights the importance of robust data governance. Companies must implement comprehensive data protection strategies aligned with global standards, addressing both legal compliance and consumer trust. This focus on data protection is strategic, as consumers increasingly value privacy.

Strategically using AI-driven insights within legal bounds can offer competitive advantages, such as personalised marketing and enhanced customer experiences, while respecting consumer rights. Successfully managing these issues can improve brand reputation and customer loyalty. Additionally, ethical data use can drive the development of advanced analytics tools, improving decision-making and engagement.

Intellectual Property and AI Innovation

The question of intellectual property (IP) in AI-generated works, particularly concerning copyright, is a frontier issue. As AI systems contribute more to creative processes, sectors like software, media and design must address the complexities of IP rights. This could involve lobbying for legal reforms or developing internal policies to handle the co-creation of works between humans and AI. The outcome of these debates will significantly impact competitive dynamics, influencing how companies protect and leverage their innovations.

AI-generated works challenge traditional IP notions, prompting a re-evaluation of authorship. Industries are exploring new IP protection forms that recognise AI's contributions, potentially unlocking new innovation avenues while protecting creators' rights. Legal frameworks accommodating AI's role in innovation could stimulate investment and drive economic growth.

Ethical AI, Corporate Governance, and Societal Impact

Ethical AI considerations are becoming integral to corporate governance. Companies are expected to implement guidelines ensuring fair, transparent, and unbiased AI systems. Regulatory frameworks, like the AI Act, require certain companies to conduct regular audits to identify and mitigate potential biases. These measures are crucial for building trust with consumers and stakeholders, enhancing sustainability and corporate reputation.

Ethical AI practices, beyond regulatory requirements, are key to maintaining public trust. They can lead to positive societal outcomes, such as reducing bias and promoting fairness in services. Moreover, ethical AI can boost corporate reputation and foster a culture of responsibility, benefiting both businesses and society.

Workforce Transformation: Reskilling and New Opportunities

AI-driven automation is transforming the workforce, potentially displacing jobs while creating new opportunities. The legal implications include adapting employment laws to protect workers' rights, particularly around retraining and job security. Companies must invest in upskilling and reskilling programmes to help their workforce transition to new roles created by AI technologies. This proactive approach mitigates the social impact of automation and aligns business practices with emerging legal and ethical standards.

Focusing on workforce development helps ensure a smooth transition to new business models. AI can also augment human capabilities, leading to more efficient and innovative work practices, benefiting both employees and employers.

Emerging AI Technologies: Autonomous Agents and Multimodal AI

New AI technologies, like autonomous agents and multimodal AI, are set to revolutionise various sectors. Autonomous agents can optimise processes in industries such as logistics, finance, and customer service. Multimodal AI, integrating data from multiple sources, enhances applications in healthcare, education, and entertainment, providing more holistic insights. These technologies promise significant improvements in efficiency, personalisation, and overall user experience.

AI in Medicine and Life Sciences: Transformative Potential

AI is poised to transform medicine and life sciences, significantly improving diagnostics, treatment planning, and patient care. AI algorithms can analyse medical images with high accuracy, assisting in early diagnosis and personalised treatments. In drug discovery, AI accelerates research and development, potentially leading to faster, more effective treatments. The use of AI in genomics and precision medicine offers tailored therapies, improving patient outcomes and reducing healthcare costs. These advancements not only enhance care quality but also increase accessibility to cutting-edge medical technologies globally.

Conclusion:
A View of AI's Future

The integration of AI into business and legal frameworks presents both challenges and opportunities. Regulatory frameworks and ethical considerations are crucial for responsible AI use, while the potential benefits are vast. AI technologies can drive efficiencies, foster innovation, and lead to transformative advancements in fields like healthcare. A balanced approach, embracing both opportunities and challenges, is essential.

Regardless of what the future holds, William Fry will be there for its clients, as we have been since 1847. If you need any assistance in relation to AI, please contact Barry Scannell, Leo Moore, David Cullen, Rachel Hayes, or any other member of the Technology Group at William Fry.

Our Team

Leo Moore
PARTNER
Head of Technology
+353 1 639 5234
leo.moore@williamfry.com

David Cullen
PARTNER
Technology
+353 1 639 5202
david.cullen@williamfry.com

John O'Connor
PARTNER
Co-head of FinTech
+353 1 639 5183
john.oconnor@williamfry.com

Barry Scannell
PARTNER
Technology
+353 1 639 5393
barry.scannell@williamfry.com

Rachel Hayes
PARTNER
Technology
+353 1 6395 218
rachel.hayes@williamfry.com

Susan Walsh
CONSULTANT
Technology
+353 1 639 5109
susan.walsh@williamfry.com