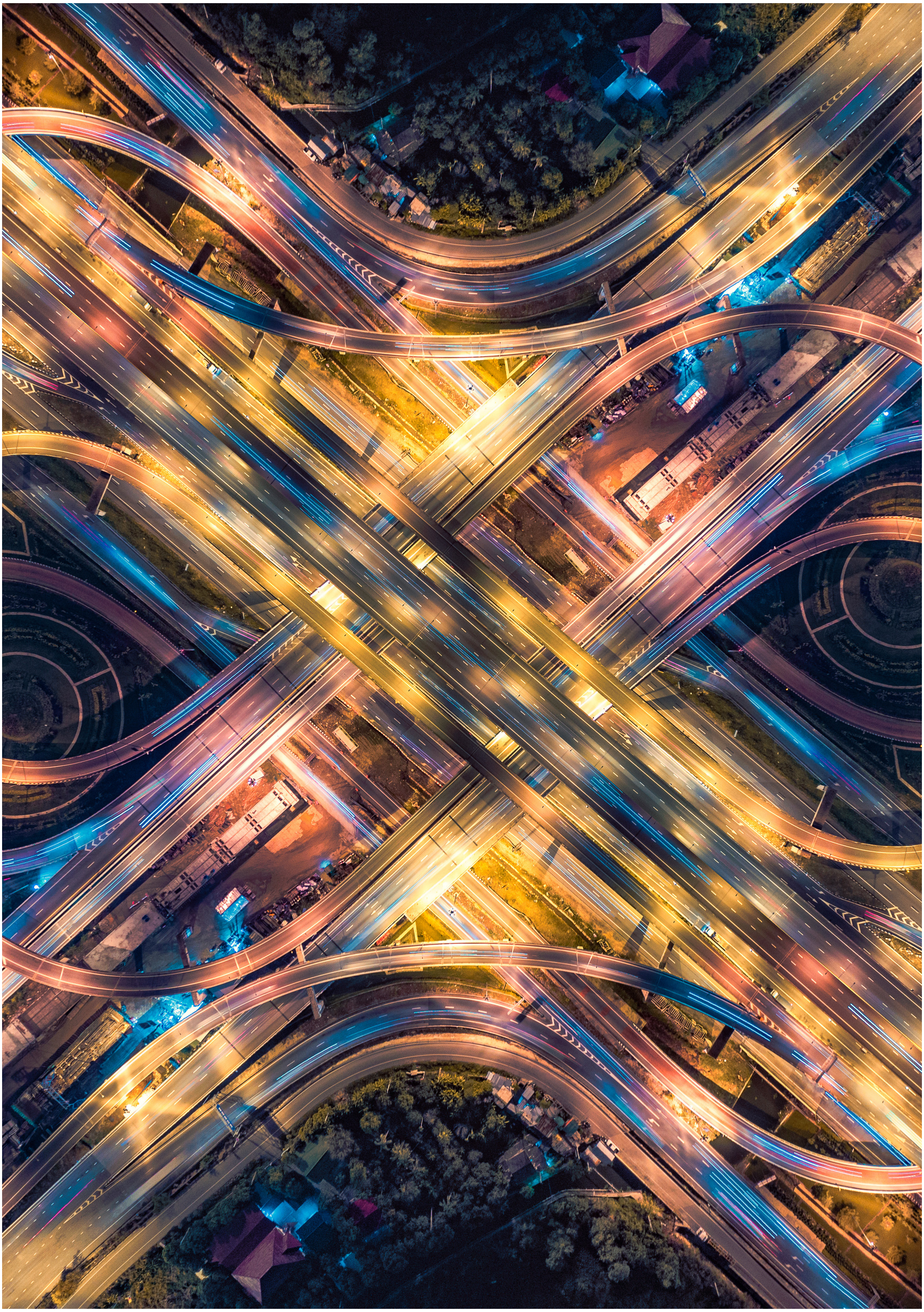
EU AI REGULATION HANDBOOK

The future regulation of technology

DLA PIPER



A new regulatory landscape

On 21 April 2021, the European Commission published its long-awaited proposal for a Regulation on Artificial Intelligence[1] (**"AI Regulation" or "Regulation"**). The AI Regulation will have broad reaching implications for the entire supply chain of AI Systems and the lifecycle of how these systems are designed, built, and run. Whilst of course, this is not the final text of the AI Regulation, it gives us a clear line of sight as to the direction and regulatory structure the EU will adopt, which will be structured as follows:

1. certain **"Prohibited AI Practices"** will be banned outright;
2. there will be a complex compliance regime for those building and deploying **"High-Risk AI Systems"**; and
3. there will be a new transparency regime for AI that poses **"manipulation risks"** (such as chatbots, deep fakes and emotion recognition systems).

In the wake of constant rule change, whether caused by Brexit, GDPR, or otherwise, all organisations using, supplying, or creating technology will need to understand the implications of the proposed AI Regulation. Businesses throughout the EU will be impacted, but so too anyone who wishes to sell into the single market, as there are broad extra-territorial effects in a manner reminiscent of the GDPR.

In particular, organisations should consider whether they need to take active steps to change processes, channels or business strategies so as to remain compliant, as well as looking at the technical feasibility of some of the new requirements. From the Board perspective, organisations will also need to determine whether the new rules bring opportunity or add to their regulatory and compliance cost of operation.

In this Handbook we will help you navigate the new AI Regulation by placing it in context, examining its key provisions, and considering how businesses looking to deploy AI solutions in the near future can adopt 'compliance by design' principles to ensure readiness for the new regulatory landscape.

This is important now. If your strategy involves AI in the European market, then understanding this draft AI Regulation is key in order to ensure you do not face a costly remediation exercise when the regulation comes into effect.

For those short on time, please see our 'speed read' of the AI Regulation here.

[1] European Commission, proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, 21 April 2021 COM(2021) 206 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELLAR%3Ae0649735-a372-11eb-9585-01aa75ed71a1

Contents

1.
Context to the EU AI Regulation

Since the term AI was coined in 1956, studies of human and machine intelligence have sought the most useful applications for the combination of raw computing power, large data sets, and complex algorithms. The last 30 years have seen AI move from theory to wider practical application, leading to the acceleration of the many product and service offerings with which we are now familiar. As 'good AI' proliferates, the attendant opportunities for discrimination, error, fraud and injury also increase, leading to commentators and organisations around the world promulgating various forms of ethical principles, design standards, and proposed rules. Now the EU has gone a step further, finally publishing the long-awaited proposal for a new legal framework, representing the most comprehensive proposed regulatory regime for AI seen in the market to date.

So, why did the Commission feel the need to create a Regulation in the first place?

EU White Paper on AI Regulation

The proposed AI Regulation follows the Commission's White Paper of Spring 2020 in which the Commission first proposed regulating the area to ensure the adoption of 'Trustworthy AI' by way of a principles-based legal framework targeting, in particular, "high risk" AI. Whilst the introductory paragraphs which precede the proposed AI Regulation state that stakeholders were largely supportive of that White Paper's proposals, it is fair to say that the response was mixed. Some sectors, and even some Member States, argued that the Commission was proposing a path of over-regulation; in their view plugging gaps in the existing legal frameworks of equality law, data protection, consumer law, product liability and so on would suffice. But undeterred, the Commission has put forward a proposed AI Regulation which will impose a significant compliance burden on those deploying AI or its outputs in an EU context.

Aims of the proposed AI Regulation

The central aim of the new AI Regulation is to ensure that any AI Systems within the EU are safe and comply with existing law on fundamental rights and EU values, taking a proportionate and risk-based approach. The Regulation seeks to enhance the governance and effective enforcement of these rights in the context of AI. The Commission further states that through this Regulation, it seeks to facilitate investment and innovation in order to develop a single market for lawful, safe, and trustworthy AI Systems by providing legal certainty on AI and its applications.[2] However, the Commission noted its concern that differing national rules may lead to fragmentation of the internal market and decrease legal certainty for operators that develop or use AI Systems.[3] Overall, the Regulation aims to take account of the fundamental rights of individuals while ensuring free movement of AI-based goods and services across borders by harmonising the Member States' approach to regulating the development, marketing and use of AI.[4]

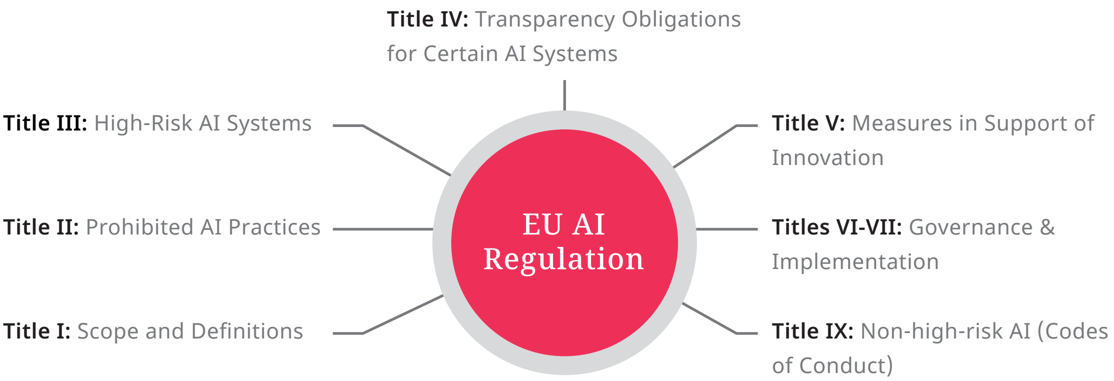
[2] Explanatory Memorandum, paragraph 1.1.
[3] AI Regulation, Recital 2.
[4] AI Regulation, Recital 1.

The proposed AI Regulation has grand ambition. In its explanatory memorandum to the Regulation, the Commission highlights that it seeks to strengthen the EU's role in shaping global norms and standards of AI Systems to be consistent with EU values and interests.[5] As we have seen with the proliferation of GDPR-like regulations around the world, it will be interesting to see whether the nomenclature and conceptual approach of the Commission is followed in other countries, or whether competing incompatible legal frameworks emerge.

Shaping Europe's Digital Future

The proposed AI Regulation forms part of a broader package of work by the Commission on related matters including the updating of the Machinery Directive and General Product Safety Directive and various initiatives under the EU Strategy for Data. It also takes into account numerous other initiatives such as the European Parliament's Framework for Ethical AI and its proposed Regulation on Liability for the Operation of AI Systems (which proposes, amongst other things, updating the current product liability regime).

THE DIAGRAMS BELOW PROVIDE A QUICK ENTRY POINT INTO WHAT IS A LONG AND COMPLEX PROPOSED REGULATION, STARTING WITH A VIEW OF THE STRUCTURE OF THE PROPOSED REGULATION:



EU AI Regulation

Title IV: Transparency Obligations for Certain AI Systems

Title III: High-Risk AI Systems

Title V: Measures in Support of Innovation

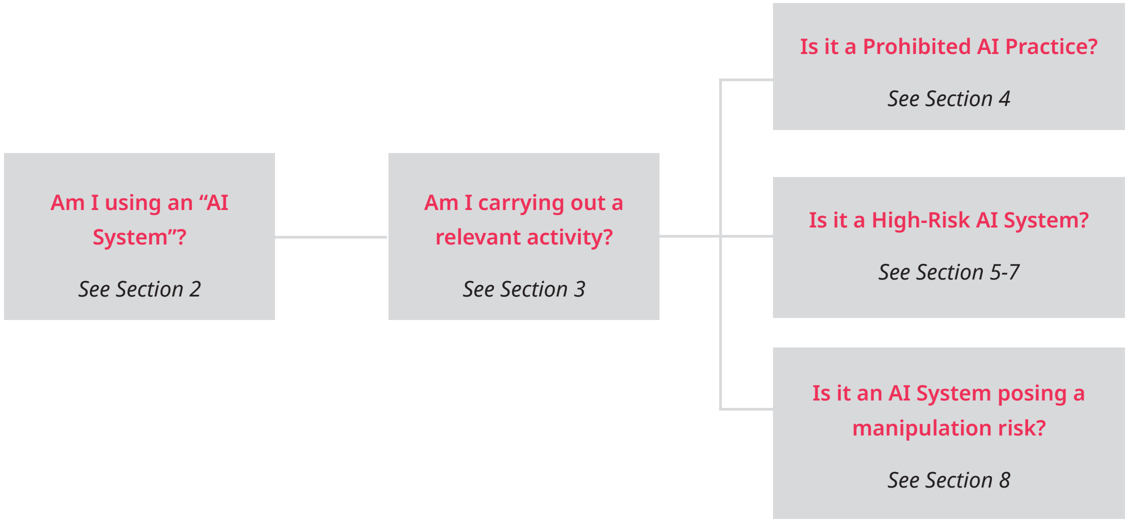
Title II: Prohibited AI Practices

Titles VI-VII: Governance & Implementation

Title I: Scope and Definitions

Title IX: Non-high-risk AI (Codes of Conduct)

THIS DIAGRAM ACTS IS A GUIDE FOR NAVIGATING THIS HANDBOOK TO DETERMINE WHETHER OR NOT THE REGULATION APPLIES TO YOU:



Am I using an "AI System"?

See Section 2

Am I carrying out a relevant activity?

See Section 3

Is it a Prohibited AI Practice?

See Section 4

Is it a High-Risk AI System?

See Section 5-7

Is it an AI System posing a manipulation risk?

See Section 8

[5] Explanatory Memorandum, paragraph 1.3.

2.
What does the Regulation apply to?

Before understanding whether your specific activities will be regulated, you must start by working out whether the proposed Regulation *could* even apply to you. First, by working out whether you are even using an AI System and secondly whether you are an entity who falls under the scope of the Regulation.

In this section we start with AI Systems.

What is an "AI System"?

The proposed definition of AI Systems is deliberately broad and it helps to break down the definition. An AI System covers:

1. **Software**;
2. **Developed** with one or more of the specified **techniques and approaches** in Annex I to the AI Regulation (which the Commission can amend over time through delegated acts). Currently, these techniques include:
   a. **Machine-learning approaches**;
      i. *which includes supervised, unsupervised, and reinforcement learning, using a wide variety of methods including deep learning;*
   b. **Logic- and knowledge-based approaches**;
      i. *including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;*
   c. **Statistical approaches**;
      i. *including Bayesian estimation, search and optimization methods;*
3. Which can, for a **given set of human-defined objectives**, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

Analysis

It is clear that this definition is very broad and covers less "cutting edge" technology than some may consider to be true AI. This is clearly intentional.

FUTURE PROOFING

In its recitals, the proposal states that the definition of "AI Systems" seeks to be a single, future-proof definition to both ensure legal certainty and provide the flexibility to accommodate future technological developments.[6] The recital, outlining some of the characteristics of AI, elaborates that AI Systems can be autonomous or can be formed as a component of a product or one that serves the functionality of a product. To future-proof the Regulation, it further highlights a need for the definition to be complimented by an updated list of specific techniques and approaches (which may be further updated by the Commission).

[6] AI Regulation, Recital 6.

MORE THAN AI?

Instinctively, the term 'AI' might tend to suggest that the Regulation is framed to apply to any of the most cutting-edge machine learning techniques. However, the broad definition of AI Systems adopted in the Regulation means that **many existing AI Systems** based upon widely deployed search algorithms may also be caught by the regime.

These systems may have everyday applications currently in use; it may surprise users that they are to be called "AI".

MORE TO COME?

It should also be noted that the AI Regulation grants the Commission the ability to adopt delegated acts to amend the list of techniques and approaches listed above in line with technological advances.[7] The explanatory memorandum to the proposal envisages a "detailed list" of the techniques and approaches used by software[8] and it is therefore possible that further detail on the three approaches listed above or indeed an increase in the number of techniques/approaches that constitute AI Systems may be included by the Commission in the near future.

[7] AI Regulation, Article 4.

[8] Explanatory Memorandum, paragraph 5.2.

3. What activities are relevant?

So, you have an AI System, but does it apply to your business? In this Section we look at who is potentially regulated, which is based largely on the activities you will undertake.

Broadly it covers those who undertake the following activities in relation to an AI System, who will be caught by some level of the Regulation and now will have to consider whether their use of AI will be regulated:

1. If you are a **Provider**[9] established ***inside or outside the EU*** and are doing the following:

   a. **Placing onto the market:** the first making available of an AI System on the EU market

   b. **Putting into service in the market:** the supply of an AI System for first use directly to the user, or for a provider's own use within the EU Market for its intended purposes.

2. If you are a **User**[10] of an AI System located ***within the EU***:

   - effectively using an AI System in the EU outside of a personal or non-professional activity.

3. If you are a **Provider or User** of AI Systems that is located ***outside the EU***

   - but where the output produced by the AI System is used ***within the EU***.[11]

Analysis

OPERATORS

There are a broad range of Operators in the chain of supply to whom these activities could relate and so are potentially regulated. In the Regulation these are termed as **providers, users, authorised representatives, importers and distributors**, together "**Operators**". Not all have the same level of obligation and we look at this further in Section 6.

It is important to note that there are slight nuances to each of the definitions, as they account for various stages of an AI System's development/distribution, and as such are treated differently throughout the proposed AI Regulation.

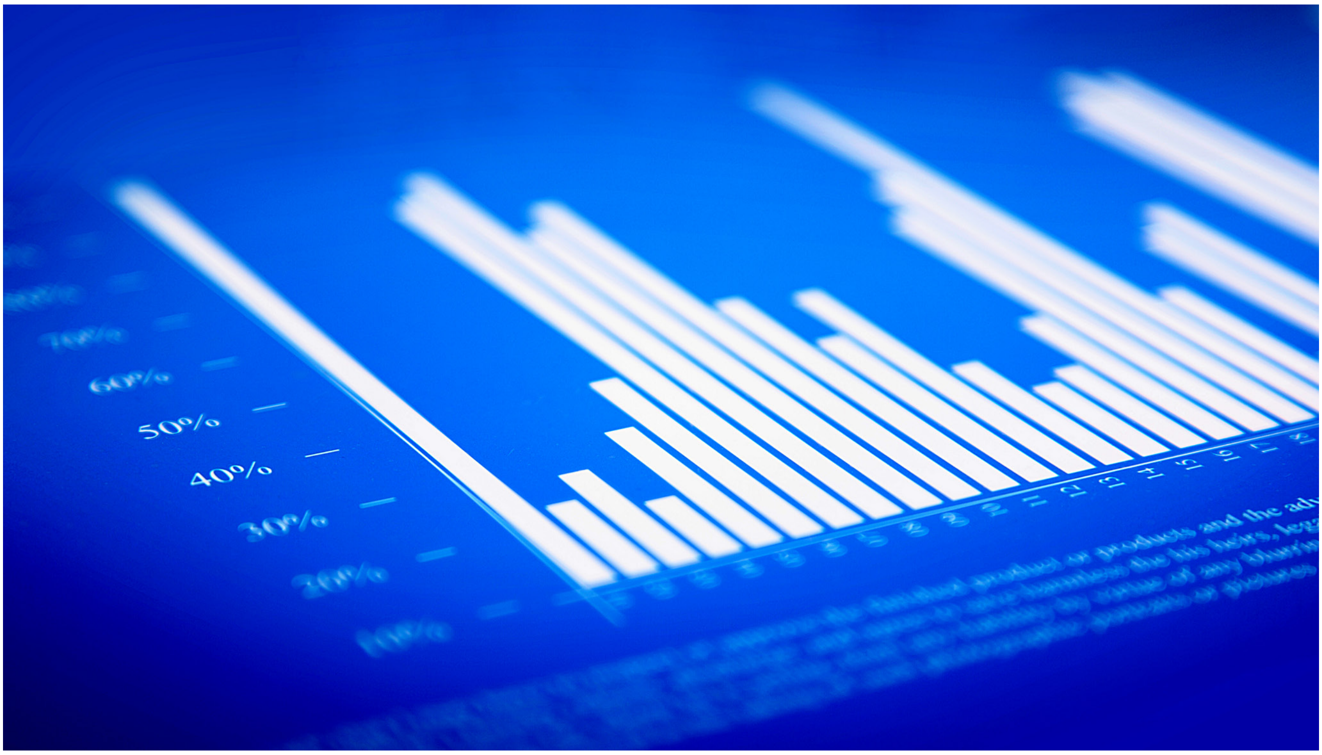
TERRITORY

The Commission wishes to use the Regulation as a basis to engage with third countries and international organisations on issues relating to AI. As with other recent EU regulations, including the GDPR, the proposed Regulation has express extra-territorial reach.

It is not surprising that the regulators have leaned towards extra-territorial measures to govern those who bring and use AI Systems in the EU. Limb (1) means that non-EU based organisations who provide AI Systems into the EU will be required to comply with the proposed AI Regulation.

However, the scope of limb (3) extends the reach of this Regulation much further than many would have anticipated. The Commission has justified this broad reach, citing an example scenario where an EU organisation contracts with a non-EU organisation for High-Risk AI Systems. In that circumstance, the non-EU operator of AI Systems

[9] See Section 6 for definition.
[10] See Section 6 for definition.
[11] AI Regulation, Article 2.1.



could process lawfully collected and transferred data from the EU, and provide the EU company with an "output" of that AI System without ever placing such an AI System on the EU Market. Whilst this could be seen as taking aim at cloud-based delivery models, what is most interesting about this broad reach is that its appears to encapsulate **any** output from **any** data source that is later deployed within the EU, not just data originally sourced in the EU.

The Commission has cited the digital nature of AI Systems as the reasoning behind such broad reach,[12] however the scope and extraterritorial nature of the Regulation have been a concern for Big Tech since the initial White Paper in 2020, creating an additional compliance burden for them along geographical lines, that they will no doubt prefer to avoid.

EXCEPTIONS

The Regulation does create some up front exceptions:

1. **No Regulation of Military:** It does not apply to AI Systems produced or used exclusively for military purposes;[13]

2. **Law Enforcement:** It does not apply to any third country government or international organisation who use AI in the pursuit of law enforcement or judicial cooperation with the EU or any Member State;[14] and

3. **Intermediary Service Providers:** The Regulation does not affect the application of the provisions on the liability of intermediary service providers as defined in the e-Commerce Directive.[15]

It should also be noted that Regulation targets primarily 'High-Risk AI System' (as defined in Section 5) and providers of 'non-High-Risk AI' can decide to follow the High-Risk AI rules voluntarily (but this is not mandatory – see Section 11). The Regulation also seeks to avoid cutting across any existing EU legislation already in force, e.g. – for "High-Risk" AI relating to safety components of products or systems and that fall within the scope of various Directive and Regulations governing machinery and vehicles (aviation, marine and others), only Article 84 (*Evaluation and review*) shall apply.[16]

[12] AI Regulation, Recital 11.
[13] AI Regulation, Article 2.3.
[14] AI Regulation, Article 2.4.
[15] AI Regulation, Article 2.5.
[16] AI Regulation, Article 2.2.

4. What is a "prohibited AI practice"?

Having become comfortable with the scope of the Regulation, the next task is to appreciate the distinction drawn by the Commission between the risks presented by the use of an AI System for particular purposes. Importantly, the controls imposed by the Regulation apply to the **use(s)** to which an AI System is put, rather than any particular techniques or technologies.

The Regulation **prohibits** the following practices:[17]

- **Use of subliminal techniques**[18] beyond a person's consciousness in order to "*materially distort a person's behaviour*" in a manner that causes or is likely to cause physical or psychological harm;
- **Targeting and exploitation of vulnerabilities of specific groups**[19] of people due to factors such as age or disability, in order to "*materially distort a person's behaviour*" in a manner that causes or is likely to cause physical or psychological harm;
- **Social scoring practices**[20] by public authorities to evaluate or classify trustworthiness of persons based on social behaviour or personality characteristics that would lead to detrimental or unfavourable treatment of a person in circumstances unrelated to the context in which they were collected; and
- **'Real-time'**[21] **remote biometric surveillance**[22] in publicly accessible places[23] for the purpose of law enforcement, **unless** it is strictly necessary for the purposes of: (i) a targeted search for specific victims of a crime (including missing children); (ii) the prevention of a specific substantial imminent threat to life or physical safety of natural persons (such as in the case of a terrorist attack); or (iii) the detection, localisation, identification, or prosecution of a perpetrator or suspect of certain serious crimes.

Analysis

GENERAL

The Regulation differentiates between AI that creates three types of risk: unacceptable risk, High-Risk, and non-High-Risk (low risk).[24] In doing so, the Commission has determined that there exist a number of use cases for AI Systems where the risk of contravening fundamental rights, significant manipulation, exploitation and/or other harm[25] is simply too great, and have defined these as Prohibited AI Practices, rendering them illegal under Union law.[26]

Crucially here it is the **practice** that is prohibited, not the technical solution. The wording of the AI Regulation here is likely to come under a lot of scrutiny and no doubt some will question whether the prohibitions go far enough.

[17] AI Regulation, Article 5.
[18] AI Regulation, Article 5(1)(a).
[19] AI Regulation, Article 5(1)(b).
[20] AI Regulation, Article 5(1)(c).
[21] For further information, see: AI Regulation, Recital 8.
[22] AI Regulation, Article 5(1)(d).
[23] For further information, see: AI Regulation, Recital 9.
[24] Explanatory Memorandum, paragraph 5.2.2.
[25] Explanatory Memorandum, paragraph 5.2.2.
[26] Explanatory Memorandum, paragraph 5.2.2.

BIOMETRIC SURVEILLANCE

Where the Regulation does permit real-time remote biometric surveillance on a more targeted basis, law enforcement must determine whether such surveillance would be appropriate based on: (i) the nature of the situation; and (ii) the consequences of its use for the rights and freedoms of all persons concerned.[27]

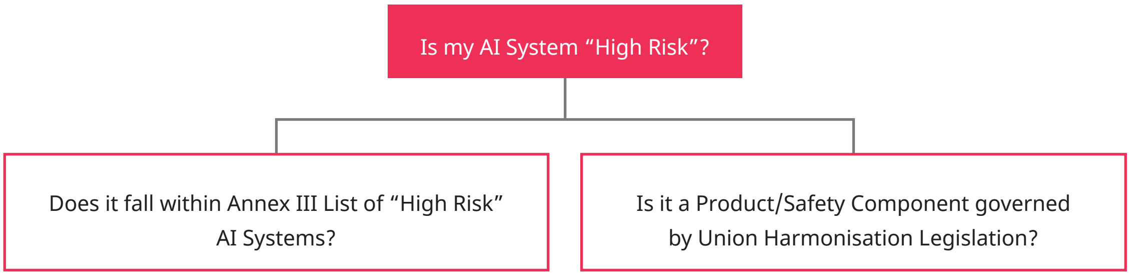
There is also a requirement for necessary and proportionate safeguards where biometric surveillance is used in public, such as limitations around time and geography.[28]

Such considerations and limitations are important so as to strike a balance between the use of this type of surveillance in the protection of citizens, and the potential risk of disproportionately impacting and unfairly restricting the rights and freedoms afforded to citizens under the European Charter for Human Rights.[29] Should the surveillance be deemed necessary, authorities must receive judicial or administrative approval prior to engaging in its use.[30]

[27] AI Regulation, Article 5(2).
[28] AI Regulation, Article 5(2).
[29] AI Regulation, Recital 18.
[30] AI Regulation, Article 5(2) and Article 5(3).

5.
High-risk AI systems

High-Risk AI Systems – are you caught?


Is my AI System "High Risk"?

Does it fall within Annex III List of "High Risk" AI Systems?

Is it a Product/Safety Component governed by Union Harmonisation Legislation?

For those practices which are not prohibited, the Regulation introduces a new conformity regime to regulate the use of High-Risk AI Systems.

An AI System is deemed "High-Risk", and is therefore subject to the compliance regime detailed in this Section, if it falls into either of the following two categories; [31]

1. **The AI System is listed as 'High-Risk' in Annex III (*High-Risk AI Systems*)** - this list deems the following AI Systems are 'de facto' High-Risk whose use may impact on fundamental rights:

1. Biometric identification and categorisation of natural persons	Used for 'real-time'[32] and 'post'[33] remote biometric identification – to the extent not a Prohibited AI Practice;
2. Management and operation of critical infrastructure	AI Systems used as safety components in road traffic and water, gas, heating and electricity supply;
3. Education and vocational training	AI Systems for (i) determining access or assigning people to training institutions; or (ii) assessing students in educational institutions (including for admissions tests);
4. Employment, workers management and access to self-employment	AI Systems for (i) recruitment e.g. job vacancies, screening/filtering, interview/test evaluation; or (ii) decisions on promotion, termination of employment, performance monitoring;
5. Access to and enjoyment of essential private services and public services and benefits	AI Systems used to: (i) determine eligibility for public benefits and services and associated actions; (ii) evaluate creditworthiness or establish credit scores;[34] or (iii) dispatch, or establish priority for dispatching emergency services;

[31] AI Regulation, Articles 6 and 7.

[32] AI Regulation, Article 3- """real-time' remote biometric identification system" means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention.

[33] AI Regulation, Article 3- ""post' remote biometric identification system' means a remote biometric identification system other than a 'real-time' remote biometric identification system;

[34] This excludes AI Systems put into service by small scale providers for their own use.

6. Law enforcement	AI Systems used to (i) assess the risk of a natural person (re)offending or the risk for potential victims of criminal offences; (ii) carry out polygraphs or otherwise to detect the emotional state of a natural person; (iii) detect deep fakes; (iv) evaluate reliability of evidence in investigating/prosecuting criminal offences; (v) predict (re)occurrence of criminal offences as well as the detection, investigation or prosecution of criminal offences based on profiling of natural persons;[35] or (vi) assist with crime analytics and searching datasets to identify patterns/relationships;
7. Migration, asylum and border control management	AI Systems used by public authorities to (i) carry out polygraphs or otherwise detect the emotional state of a person; (ii) assess risks of persons intending to enter a Member State relating to e.g. security, irregular immigration, health; (iii) verify authenticity of travel documents; or (iv) assist in examining asylum, visa and residence permit applications and eligibility; or
8. Administration of justice and democratic processes	AI Systems to assist judicial authorities in researching / interpreting facts and the law, and applying the law to facts.

This list may be **updated** by the Commission to add additional High-Risk AI Systems where the use case is essentially the same as those already listed or where a similar high-risk of harm is present.

2. **The AI System is a safety component of products/products themselves governed by the Union Harmonisation Legislation**

   Certain AI Systems are considered “High-Risk” if they are used as safety components of products (or are a product themselves) and they are required to undergo a third-party conformity assessment before being put onto the market.

   These are listed in Annex II of the Regulation and are focussed on AI Systems on products in the scope of Union Harmonisation Legislation (legislation harmonising the conditions for the marketing of products such as machinery, toys, and medical devices).

Analysis

In line with the original EU White Paper, the Regulation imposes controls upon “High-Risk” uses of AI Systems.[36] However the Regulation diverges from the White Paper approach at a more granular level in defining what constitutes “High-Risk”[37] by focussing on creating a compliance framework for AI Systems that create a High-Risk to the health and safety or fundamental rights of people, rather than determining “High-Risk” based on the sector and intended use of the AI System, as proposed in the White Paper. In classifying something as “High-Risk”, the Regulation focuses on the intended *purpose* for the AI System (aligned to existing product safety legislation), as opposed to just the function performed by the AI System.

Given the broad definition of ‘AI System’, there is a high probability that many systems deployed for the use cases designated as “High-Risk” within the proposed Regulation will be caught by the new regime.

The impact of these broad High-Risk AI System classification rules is that organisations involved in the medical, energy, education, HR, public, financial, insurance, safety, justice and immigration sectors are potentially affected and should act quickly to ensure that they are familiar with the new Regulation and the requirements that must be met, and assess the maturity of their technology roadmaps and business strategies to ensure compliance with the forthcoming regime.

[35] As referred to in Article 3(4) of Directive (EU) 2016/680.

[36] Although see below for voluntary compliance by non-High-Risk AI Systems, which is permitted and encouraged. See Section 11.

[37] In the White Paper, it was proposed that “High-Risk” would be determined based on (i) the sector combined with the intended use; or (ii) an AI System being high-risk “as such” based on a pre-defined list.

Requirements for High-Risk AI Systems

Once it has been established an AI System is 'High-Risk' under the Regulation, Chapter 2 (Articles 8-15) sets out a number of legal requirements with which the high-risk AI System must comply. We will call these the "**High-Risk Requirements**" and they are:

Risk Management	• A risk management system must be established and maintained throughout the AI System's lifecycle, with specified steps covering the identification, analysis, and evaluation of risks and subsequent adoption of suitable risk management measures, taking into account the sophistication of the user and using regular testing. • In real terms, this means establishing a comprehensive record-keeping approach for affected systems.
High Quality Datasets and Data Governance	• For High-Risk AI Systems that use techniques to train models with data, what constitutes a 'quality' data set for training, validation and testing is explicitly specified (e.g. that data sets should be representative, complete, error free). • To the extent strictly necessary for bias monitoring, detection and correction and subject to appropriate safeguards, the processing of special categories of personal data under the GDPR and other related EU law is permitted.
Technical documentation	• Prior to launch of the AI System, technical documentation must be drawn up to evidence compliance with the High-Risk Requirements (and as a minimum, the requirements in Annex IV (*Technical Documentation*)) and must be updated regularly. This highlights the importance for organisations in having comprehensive and auditable documentation.
Record keeping / Automatic logging	• Record keeping and automatic logging capabilities of the AI System, with certain minimum requirements to enable appropriate traceability and (risk) monitoring, are required.
Transparency-by-design	• To address the well-known 'black box' issue, High-Risk AI Systems must be designed to ensure their operation is sufficiently transparent to enable users to interpret the AI System's output and use it appropriately. • AI Systems must include instructions for use containing specified information such as the contact details of the provider and the characteristics, capabilities, limitations (including accuracy) of the AI System, as well as human oversight measures available and measures to facilitate the interpretation of the AI System's outputs.
Human Oversight	• High-risk AI Systems must be developed in a way that enables effective human oversight[38] by natural persons, including the use of appropriate human-machine interface tools, so as to prevent or minimise risks to health, safety or fundamental rights that may arise when using the AI in accordance with its intended purpose or under conditions of reasonably foreseeable misuse.

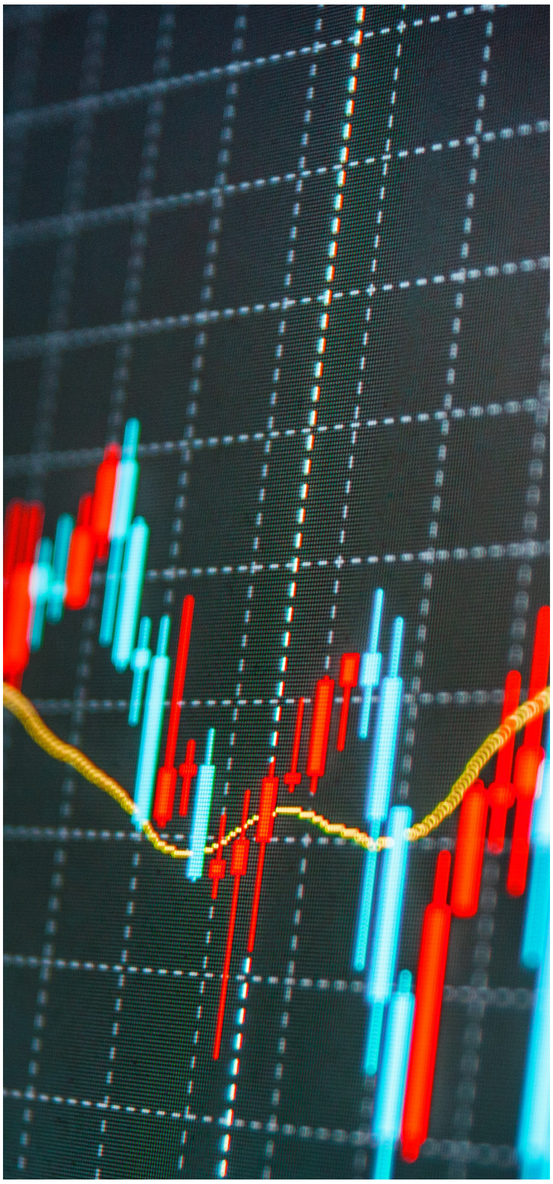
[38] This must include enabling individuals assigned with oversight to be able to: (i) fully understand the capacities and limitations of the High-Risk AI System and monitor its operation to detect anomalies or dysfunctions; (ii) remain aware of 'automation bias', particularly for systems that provide information or recommendations for decisions by natural persons; (iii) correctly interpret the High-Risk AI System's output; (iv) decide not to use the High-Risk AI System or otherwise disregard, override or reverse its output; and (v) intervene on the operation of the High-Risk AI System or interrupt the system through a "stop" button or a similar procedure.

Human Oversight (continued)	• Human oversight must be identified and ensured through either building this into the AI System (if technically feasible) and/or making it possible for the user to implement oversight themselves, in each case prior to the AI System being placed on the market or put into service. Whether this will be technically feasible is open to question, and it may be that we look back at these rules within a short number of years as laudable, but impractical.
Accuracy, Robustness and Security	• AI Systems must be sufficiently accurate, robust and secure throughout their lifecycle, and accuracy metrics must be included in instructions for use. • The AI System should be secure and resilient to errors and faults (whether through interacting with other systems or humans) as well as malicious attempts to exploit vulnerabilities (such as data poisoning[39], adversarial examples[40] or model flaws). • Robustness can be achieved using technical redundancy solutions such as backup or fail-safe plans, and the potential for bias via feedback loops should also be appropriately mitigated.

Analysis

The Regulation seeks to be consistent with other existing international principles, themes and recommendations (such as the OECD Principles on AI) in these requirements. Notably, however, the Regulation deliberately does not go as far as specifying the '*technical solutions*' required to achieve compliance. Rather it acknowledges that allowing providers discretion and flexibility in this area is crucial so that the requirements can be met using a variety of technological solutions, specifications and/or standards that can improve and develop in conjunction with developing science and engineering practices, rather than being stifled by prescriptive and potentially out-of-date standards determined by the Commission.[42]

The impact of this is that there will likely be a flurry of significant, multi-stakeholder activity across all industries, as organisations grapple with how to translate these requirements into practical, technical standards, until 'good industry practice' is established.



[39] i.e. attacks trying to manipulate the training dataset.
[40] i.e. inputs designed to cause the model to make a mistake.
[41] https://www.oecd.org/going-digital/ai/principles/
[42] Explanatory Memorandum, paragraph 5.2.3.

6. The high-risk AI ecosystem: Providers and other operators

The obligations you have under the draft Regulation differ according to what type of Operator you are. These are summarised at a high level, in the table below, and in more detail in the remainder of this Section.

KEY OBLIGATIONS FOR OPERATORS OF HIGH-RISK AI SYSTEMS

Accuracy, Robustness and Security

- The most onerous controls apply to **Providers** - a person or organisation that develops an AI System, or that has an AI System developed, with a view to placing it on the market or putting it into service.[43] These controls include ensuring that the AI System is built in compliance with the Regulation (including the High Risk Requirements), appropriately assessed for conformity and registered with the relevant authorities prior to first use / provision. Providers are also responsible for ongoing post-market monitoring, reporting and corrective actions.
- **Users** are responsible for ongoing use of the AI System, including ensuring that such use remains within the parameters for which it was approved, and monitoring the operation of the system for evidence of damaging effects.[44]
- **Importers**, **Distributors** and **Authorised Representatives** play a secondary role in validating that the appropriate assessments have been undertaken and are responsible for taking steps to rectify issues that may arise in the AI System, aligning to their role.

Other operators / third parties **will be considered a provider for the purposes of the Regulation**, and subject to the obligations of providers, where they:

- place on the market / put into service a High-Risk AI System **under their own name or trade mark**
- **modify the intended purpose** of a High-Risk AI System already placed on the market or put into service, or
- make a **substantial modification** to the High-Risk AI System.

Does this apply to my organisation?

If your business is in the provision of technology services, and elements of those services fall within the high-risk use cases then you, as a **provider**, will need to ensure that you comply with the new requirements.

This means that you will have to:

- **ensure compliance** with the High-Risk Requirements and, upon request of a national competent authority, demonstrate such compliance;[45]
- prior to a High-Risk AI System being placed on the market or put into service, draw up and maintain **technical documentation** demonstrating that the system complies with the High-Risk Requirements;[46]
- have in place a documented, compliant **quality management system** to ensure compliance with the Regulation;[47]

[43] AI Regulation, Article 3.2.

[44] Users are defined in Art 3.4 as any natural or legal person, public authority agency or other authority using an AI System, with the exception of personal, non-professional use of an AI System;

[45] AI Regulation, Article 16.

[46] AI Regulation, Articles 11 and 16.

[47] AI Regulation, Articles 16 and 17.

- ensure the AI System undergoes the relevant **conformity assessment procedure**[48] (discussed in the following Section);
- **register the High-Risk AI System in a new EU database** for stand-alone High-Risk AI Systems,[49] prior to being placed on the market or put into service. This database is publicly accessible;
- draw up an **EU declaration of conformity** – this must contain the information set out in Annex V, be kept up-to-date, and retained for 10 years after the AI System has been placed on the market or put into service;
- affix a **CE marking** to High-Risk AI Systems to indicate conformity with the High-Risk Requirements;[50]
- immediately **take corrective actions** if you consider, or have reason to believe, that a High-Risk AI System placed on the market or put into service is not in conformity with the Regulation (or withdraw or recall it), and inform the national competent authorities of such non-compliance and any corrective actions taken;[51]
- **appoint an authorized representative** by written mandate where no importer can be identified;[52]
- carry out proportionate **post-market monitoring** to actively collect and analyse data provided (e.g. by users) on the performance of High-Risk AI Systems throughout their lifetime and continuously evaluate the compliance of AI Systems with the High-Risk Requirements;[53] and
- **report any serious post-market incident or malfunctioning of the AI System** to the national market surveillance authorities if the incident or malfunctioning constitutes a breach of obligations under Union law intended to protect fundamental rights.[54] This notification must be made immediately after establishing a causal link (or the reasonable likelihood of a causal link) between the AI System and the incident/malfunctioning, and in any event, not later than 15 days after becoming aware of the serious incident/malfunction.

But I'm not a 'provider', so do I have to do anything?

Those in the supply chain as value-added resellers or in other commercial relationships with providers **will also need to take steps** to ascertain what type of Operator they are classed as, and adjust their business processes accordingly to comply with the new requirements, because the Regulation also sets out obligations on **users** and other participants across the AI value chain, including **importers and distributors**.[55]

The obligations on **importers and distributors** are generally focussed on ensuring compliance by **providers** with the Regulation. For example, prior to placing a High-Risk AI System on the market, importers are required to ensure that the provider has carried out the appropriate conformity assessment and drawn up the required technical documentation beforehand.

Users are also subject to a range of obligations, including requirements to: (i) use High-Risk AI Systems in accordance with the instructions of use; (ii) ensure that input data is relevant in view of the intended purpose of the High-Risk AI System; (iii) monitor the operation of the system and inform the provider/distributor of suspected risks and of serious incidents or malfunctioning; and (iv) conserve logs automatically generated by that High-Risk AI System, to the extent such logs are under their control. These new requirements will therefore have implications for procuring bodies in the public sector and customers of outsourced services. One can immediately imagine, for example, that B2B negotiated commercial contracts will feature explicit wording to apportion the obligations to comply with, and pay for these new requirements.

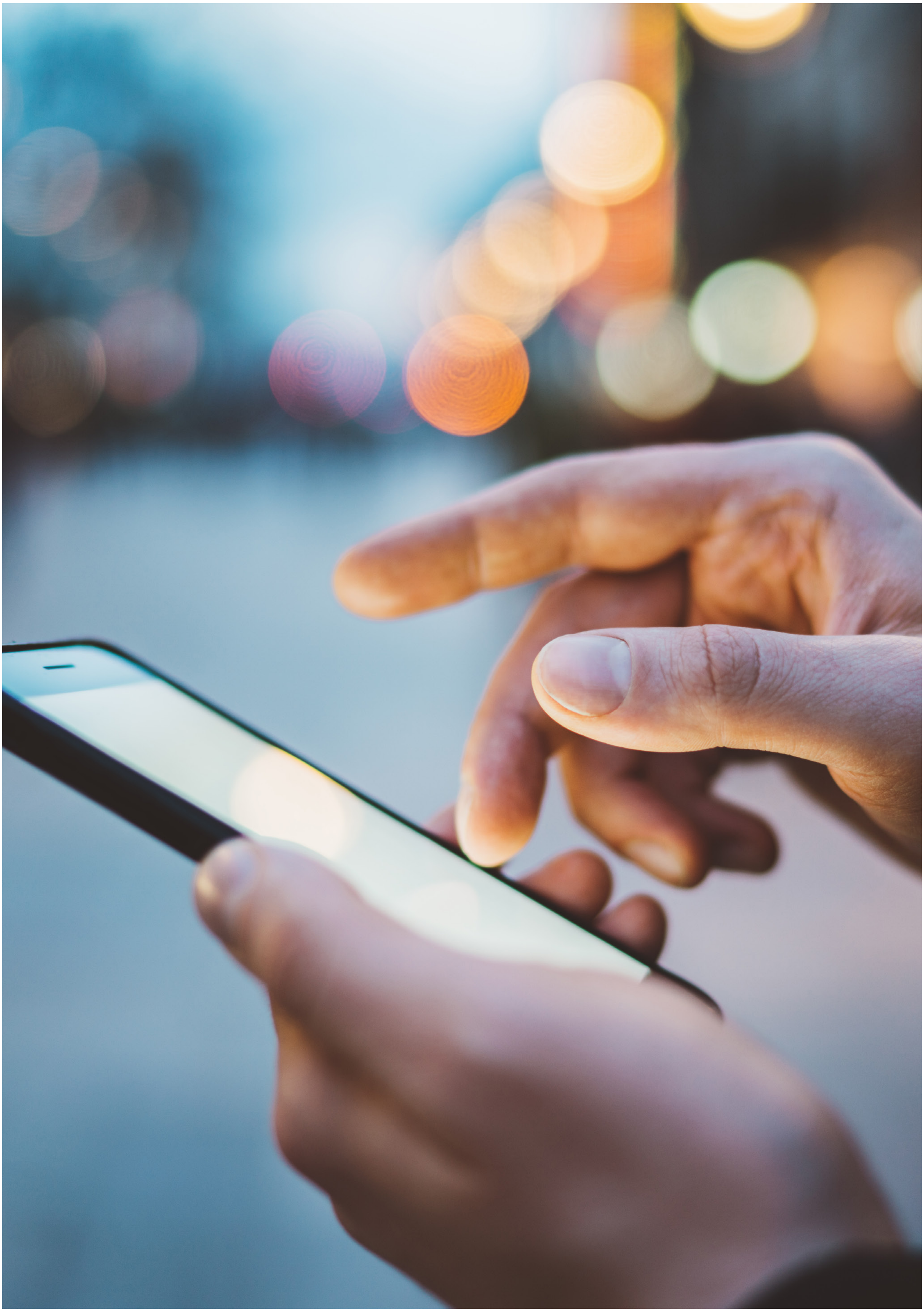
While the obligations placed on other participants are generally less extensive than the obligations placed on providers, such participants should be aware that the **obligations on providers will apply to them where they do certain things**, for example, where they place on the market or put into service a High-Risk AI System under their own name or trade mark, or where they make a substantial modification to a High-Risk AI System.

[48] AI Regulation, Articles 19 and 43.
[49] AI Regulation, Articles 51 and 60.
[50] AI Regulation, Articles 19, 48 and 49.
[51] AI Regulation, Articles 26 and 21.
[52] AI Regulation, Article 25.
[53] AI Regulation, Article 61.
[54] AI Regulation, Article 62.
[55] AI Regulation, Articles 24 to 29.

A more detailed summary of the obligations of each Operator is set out here:

OPERATOR	DESCRIPTION	KEY OBLIGATIONS
Provider	• Natural or legal person, public authority, agency or other body • **Develops** AI System / has AI System **developed** with a view to **placing it on the market** or **putting it into service** under its own name / trademark • Whether for payment or free of charge	• Ensure compliance with the High-Risk Requirements • Maintain the Quality management system • Technical documentation demonstrating compliance with Regulation • Keep logs automatically generated by AI System (where under provider's control) • Conformity assessment • Register AI System in EU database • EU declaration of conformity • Affix CE marking to AI Systems • If provider established outside Union and importer cannot be identified, appoint authorised representative • Implement and maintain post-market monitoring system, to evaluate continuous compliance of AI System with the High-Risk Requirements • Where AI System is non-compliant with Regulation: • Immediately take necessary corrective actions to bring system into conformity, to withdraw it, or to recall it, and • Inform national competent authorities • Inform national market surveillance authorities if incident / malfunctioning of AI System constitutes a breach of obligations under Union law intended to protect fundamental rights • Carry out post-market monitoring and reporting.
Authorised representative	• Natural or legal person established **in the Union** • Has **written mandate from provider** to **perform** and **carry out obligations** and procedures under the Regulation on behalf of provider	• Perform tasks specified in mandate, which shall empower authorised representative to: • Keep a copy of the EU declaration of conformity and technical documentation at disposal of national competent authorities • Upon reasoned request, provide national competent authorities with all necessary information and documentation to demonstrate conformity with the High-Risk Requirements and cooperate with authorities on any action taken.
Importer	• Natural or legal person established in **the Union** • Places on the **market** or puts into **service** an **AI System** that bears **name or trademark** of natural or legal person **established outside Union**	• Before placing AI System on market, ensure: • provider has carried out conformity assessment and drawn up technical documentation • AI System bears conformity marking and is accompanied by required documentation / instructions of use • Not place any non-compliant AI System on the market • Inform provider and market surveillance authorities if AI System presents risk at national level • Indicate address plus name / registered trade name / registered trade mark on AI System or, if not possible, on packaging / accompanying documentation

OPERATOR	DESCRIPTION	KEY OBLIGATIONS
Importer (continued)		• Ensure storage / transport conditions do not jeopardise compliance with the High-Risk Requirements (where under importer's responsibility) • Upon reasoned request, provide national competent authorities with all necessary information and documentation to demonstrate conformity and cooperate with authorities on any action taken.
Distributor	• Natural or legal person in supply chain (other than provider or importer) • Makes AI System **available on the Union market** without affecting its properties	• Before making AI System available on market, ensure: ◦ AI System bears CE conformity marking and is accompanied by required documentation / instructions of use ◦ provider and importer have complied with the Regulation • Not make available on the market any non-compliant AI System • Ensure storage / transport conditions do not jeopardise compliance with the High-Risk Requirements(where under distributor's responsibility) • Where AI System is non-compliant with the High-Risk Requirements: ◦ immediately take necessary corrective actions to bring system into conformity, to withdraw it, or to recall it (or ensure provider, importer or other operator takes such actions), and ◦ immediately inform national competent authorities if AI System presents risk at national level • Upon reasonable request, provide national competent authorities with all necessary information and documentation to demonstrate conformity and cooperate with authorities on any action taken.
User	• Natural or legal person, public authority, agency or other body • **Using an AI System under its authority**, other than for personal non-professional activity	• Use AI Systems in accordance with instructions of use • Ensure input data is relevant in view of intended purpose of AI System (where user exercises control over input data) • Monitor operation of AI System and inform provider / distributor of suspected risks, serious incidents or malfunctioning, and suspend / interrupt use in such cases • Keep logs automatically generated by AI System (where under user's control) • Use information provided under Article 13 to comply with obligation to carry out GDPR data protection impact assessment.



7. Conforming with Conformity Assessments

Do I need to carry out a separate Conformity Assessment?

The Regulation details a myriad of **conformity assessment procedures** to be followed for High-Risk AI Systems, which may be carried out on a stand-alone basis (where the High-Risk AI System is deemed High-Risk 'as such' in Annex III), or as part of wider product conformity assessments governed by existing EU legislation (including where the AI System is a safety component of products/products themselves governed by the Union Harmonisation Legislation).

Where subject to the new conformity assessment regime, providers will, depending on the AI System used, have to comply with either a conformity assessment based on internal controls[56] (most common) or, in more limited cases, a conformity assessment procedure based on assessment of the quality management system and technical documentation, carried out by a newly created notified body. This conformity assessment approach aims to minimize the burden for economic operators as well as for notified bodies and adopt 'presumptions of conformity' where possible.

Can I presume that my AI conforms to the standard?

For certain High-Risk AI Systems that are part governed by existing EU legislation, operators can rely on a 'presumption of conformity'. These include:

- High-risk AI Systems in conformity with "harmonized standards"[58] or parts thereof whose reference have been published in the Official Journal of the EU. These shall be presumed to be in conformity with the High-Risk Requirements.
- If these are not applicable or determined insufficient by the Commission, the Commission may adopt "common specifications"[59] in respect of the High-Risk Requirements. High-risk AI Systems that are in conformity with the common specifications will then be presumed to be in conformity with the High-Risk Requirements.
- There are also presumptions of conformity for other certain High-Risk AI Systems, such as those certified under cybersecurity schemes.[60]

What conformity assessments do I need to carry out if I can't rely on a 'presumption of conformity'?

For operators not able to benefit from a presumption of conformity, the approach to conformity assessments aligns to the classification rules for High-Risk AI Systems listed in Section 5 above.

There are fundamentally two different conformity assessment procedures, which apply in different circumstances:

1. Conformity assessment procedure based on **internal control** (detailed in Annex VI), which does not require any involvement from a notified body; or
2. Conformity **assessment procedure based on assessment of the quality management system and technical documentation** (detailed in Annex VII):
   - This is carried out by a notified body who will issue a certificate to confirm compliance (see below for further detail);
   - An appeal procedure must be introduced for interested parties to appeal against certification decisions made by notified bodies; and

[56] Further detailed in Annex VI of the AI Regulation.
[57] Further detailed in Annex VII of the AI Regulation.
[58] Defined as a European standard as defined in Regulation (EU) No 1025/2012 on European standardization.
[59] 'common specifications' means a document, other than a standard, containing technical solutions providing a means to, comply with certain requirements and obligations established under the Regulation.
[60] See: AI Regulation, Article 42.

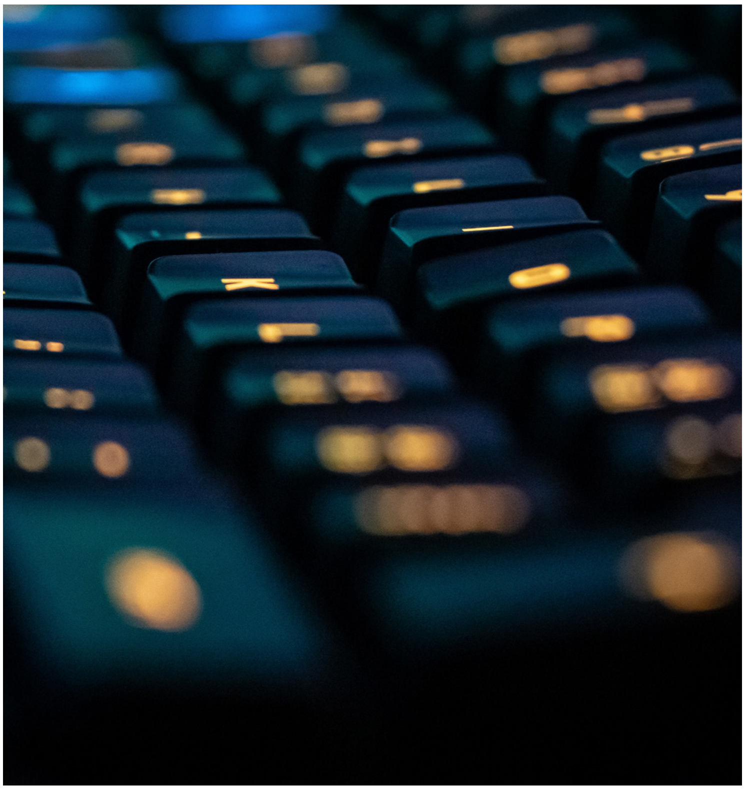
- Certificates are valid for a maximum of 5 years before reassessment is required.

For High-Risk AI Systems, the conformity assessment required is determined by reference to the Annex III list of uses to which the system is put. The rules make a distinction between High-Risk AI Systems that use biometric identification and categorisation of natural persons (point 1 of Annex III) and those that do not (points 2-8 of Annex III), as well as considering High-Risk AI Systems listed in Section A of Annex II (i.e. Union harmonisation legislation based on the New Legislative Framework).

- For High-Risk AI Systems that use **biometric identification and categorisation of natural persons (point 1 of Annex III)**:
  - where harmonised standards or common specifications have been applied, the provider can choose whether to follow: (i) the internal control (without a notified body); or (ii) the assessment of the quality management system and technical documentation (involving a notified body) process; and
  - where harmonised standards have only been applied in part, do not exist, or common specifications are not available, the Annex VII conformity assessment procedure must always be used.
- For High-Risk AI Systems that relate to **critical infrastructure, education, employment, access to essential private and public services, law enforcement, migration/border control and administration of justice and democracy (points 2-8 of Annex III)**, the conformity assessment procedure based on **internal control** (without involving a notified body) should be used in all cases.[61]
- High-Risk AI Systems **used as safety components of products to which the Union harmonisation legislation listed in Section A of Annex II applies** (i.e. systems subject to the New Legislative Framework legislation) must follow the existing conformity assessment required under the relevant legislation. However, the existing conformity assessment must now ensure compliance not only with the requirements established by the relevant legislation it is already are governed by, but also with the High-Risk Requirements.[62] The Commission's intention to align the Regulation with the New Legislative Framework is a helpful one, however it remains to be seen how this will play out in practice with these overlapping regimes.

Analysis

We would recommend that organisations carefully assess which conformity assessment regime may apply, including whether they are subject to an exemption or presumption of conformity and therefore able to avoid carrying out the 'full' conformity assessments detailed here.



[61] However, note the Commission may determine in its discretion that Annex VII assessments should instead apply, having regard to the effectiveness of the existing conformity assessment procedure in preventing/minimizing risks to health and safety, the protection of fundamental rights and the availability of adequate resources of notified bodies, per AI Regulation, Art 43(6).

[62] See AI Regulation, Article 43(3) for further detail.

Regardless of the conformity assessment procedure used, High-Risk AI Systems should undergo new assessments whenever they are substantially modified (regardless of whether the modified system will continue to be used by the existing use or be more widely distributed). In any event, reassessment is required every 5 years for conformity assessments based on the assessment of the quality management system and technical documentation process. There are some exceptions to this for High-Risk AI Systems that continue to learn after being placed on the market/put into service.[63]

What are the exceptions to conformity assessment regime?

There is one notable exception to the conformity assessment regime in respect of any market surveillance authority of a Member State. Such an authority may authorise the placing on the market or putting into service of specific High-Risk AI Systems within a Member State for exceptional reasons **of public security or the protection of life and health of persons, environmental protection, and the protection of key industrial and infrastructural assets**.

The authorisation must be for a limited period of time, can only be issued if the High-Risk AI System meets the High-Risk Requirements, and lasts only while the necessary conformity assessments are conducted, which must be done "without undue delay".[64] The Commission and all other Members States have a right to object within 15 days to any authorisation granted if they view it as being contrary to Union law or the High-Risk AI System not being in compliance with the High-Risk Requirements. If there is an objection, the Commission must consult with the Member State and decide whether the authorisation was justified or not, and is empowered to require the authorisation to be withdrawn if it deems it unjustified. This exception to conformity assessments seeks to balance the emergency actions that a Member State may be required to take with policing and establish some accountability for a Member State who seeks to abuse the exemption by placing on the market/putting into service a High-Risk AI System without good reason for doing so and without compliance with the High-Risk Requirements.

Who are the Notifying Authorities and Notified Bodies?[65]

The Regulation requires the establishment of a number of supervisory bodies within a Member State, known as "**notifying authorities**" and "**notified bodies**" These bodies are required to facilitate the conformity assessment procedure based on assessment of the quality management system and technical documentation (detailed in Annex VII).

NOTIFYING AUTHORITIES:

- These are the national authority/authorities responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring.
- Each Member State must designate or establish a notifying authority, which can include certain national accreditation bodies.
- Notifying authorities must be impartial and independent from notified bodies.

NOTIFIED BODIES:

- These are conformity assessment bodies (bodies that performs third-party conformity assessment activities, including testing, certification and inspection) designated in accordance with the Regulation and other relevant Union harmonisation legislation. We anticipate that being designated as an assessment body will be attractive for those organisations already familiar with the European accreditation infrastructure and European co-operation for Accreditation.
- In order for a conformity assessment body to become a notified body, it must submit an application for notification to the notifying authority of the Member State in which they are established. This application must include details of the conformity assessment activities, the conformity assessment module(s) and the AI technologies for which the conformity assessment body is competent, together with an accreditation certificate (if available) attesting its fulfilment of the Article 33 requirements for notified bodies.[66]
- The notified body will then be assigned an ID number by the Commission, and included in a publicly accessible list of notified bodies. If at any point a notifying authority suspects a notified body no longer meets the Article 33 requirements it can investigate this and potentially restrict, suspend or withdraw its notification.

[63] AI Regulation, Article 43(4).

[64] AI Regulation, Article 46(1).

[65] AI Regulation, Articles 30-38.

[66] AI Regulation, Article 33 requirements include that the notified body is sufficient independent from the High-Risk AI System provider and any other operator with an economic interest in the High-Risk AI System being assessed/any of its competitors.

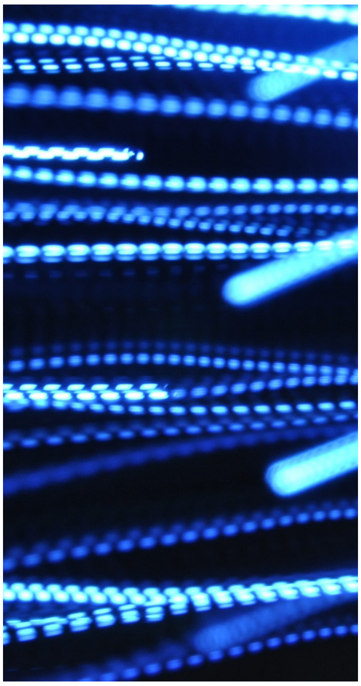
8. Deep fakes and chatbots: Transparency obligations for certain AI systems

Separate and distinct from the High-Risk AI System regime set out in Title III of the Regulation, Title IV (Article 52) sets out specific transparency obligations **for all AI Systems that the Commission has identified as posing manipulation risks** (but that have not been prohibited outright as Prohibited AI Practices). This transparency regime sits alongside the Prohibited AI Practices and High-Risk AI Systems obligations and seeks to ensure that if an AI System is, for example, used to generate or manipulate content that appears authentic, the user is informed that this has been generated using AI, so they can make an informed choice or indeed decide to not engage with the AI System on this basis.

The transparency obligations are as follows but are subject to some exceptions which mostly relate to justifications based on crime detection/prevention (see footnotes for further details):

- **AI Systems intended to interact with natural persons** must be designed so that natural persons are informed they are interacting with an AI System, unless this is obvious from the circumstances/context.[67]
- **Users of emotion recognition systems or biometric categorisation systems** must inform natural persons exposed to this of this aspect of operation of the system.[68]
- **Users of 'deep fakes'**, i.e. AI Systems that generate or manipulate image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful, shall disclose that the content has been artificially generated or manipulated.[69]

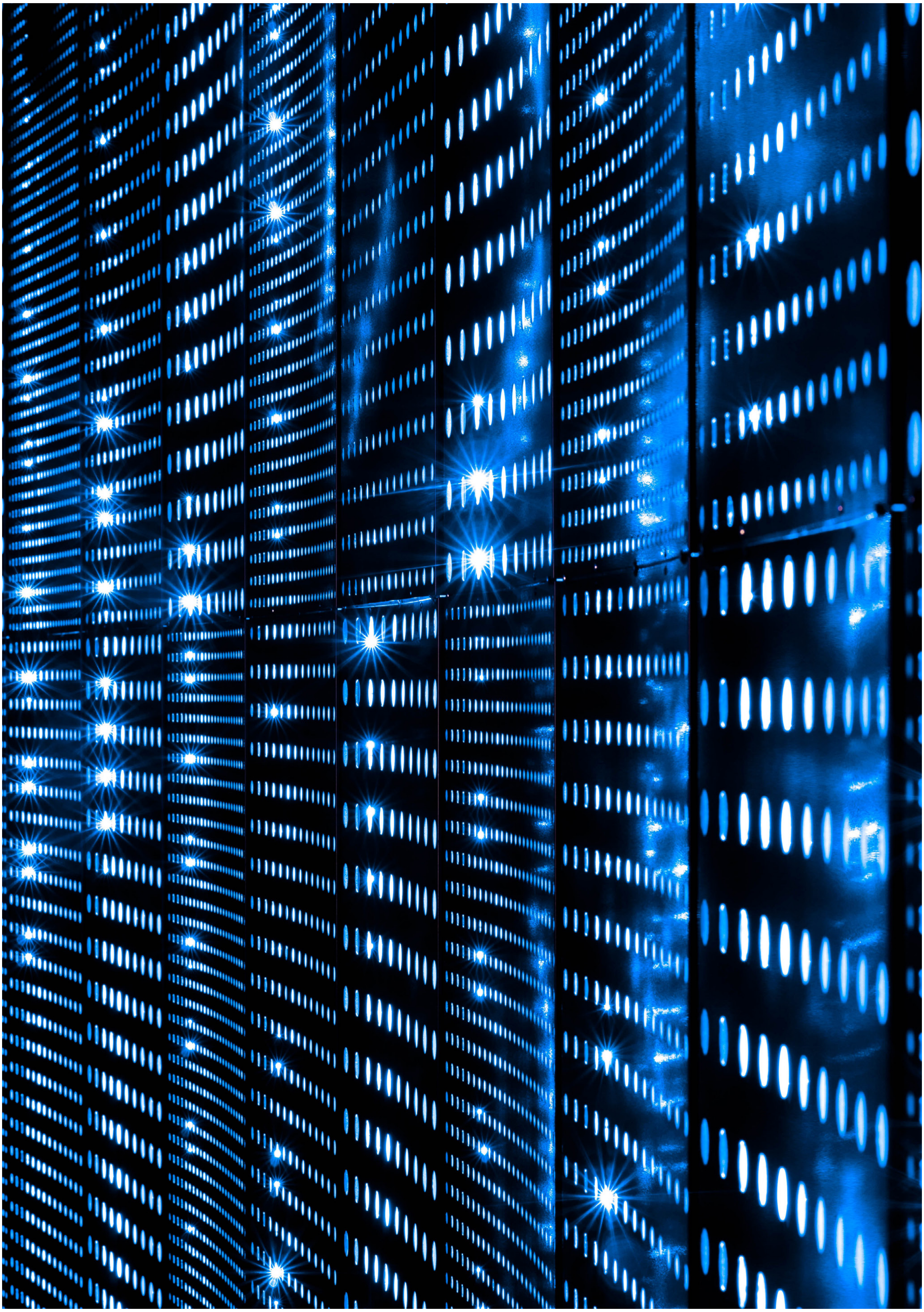
An AI System can be both High-Risk and subject to these Article 52 obligations – they are not mutually exclusive.



[67] Note this does not apply to AI Systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless the systems are available for the public to report a criminal offence.

[68] Note this does not apply to AI Systems used for biometric categorisation which are permitted by law to detect, prevent and investigate criminal offences.

[69] Note this does not apply where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and subject to appropriate safeguards for the rights and freedoms of third parties.



9. Innovation measures

So far, the new requirements appear to add to the administrative burden for commercial organisations. However the proposed Regulation equally acknowledges that in addition to regulatory oversight, AI needs a safe space for development and experimentation in order to encourage innovation.[70] The Regulation proposes three primary methods of creating these spaces: regulatory sandboxes, providing assistance to SMEs, and the involvement of governing authorities and organisations to provide expertise and guidance.

Regulatory Sandboxes

Perhaps the most substantial measure supporting innovation is the creation of regulatory sandboxes. The Regulation encourages Member States to develop and implement regulatory sandboxes[71] to allow a dedicated regime for testing novel AI Systems, while ensuring strict regulatory oversight is maintained prior to their release to the wider market.[72]

The objectives of these sandboxes are:

- to foster AI innovation through controlled experimentation;
- to enhance legal certainty for innovators seeking to test and develop new systems while allowing regulators to understand the emerging risks and impacts these programmes may cause; and
- to accelerate access to markets by removing barriers to entry for those seeking to market new technology.[73]

One of the most notable aspects of these provisions is the permission for participants to re-use personal data collected for other purposes in the training of the sandboxed AI Systems.[74] In order to do so, the AI in development must be created for the purposes of safeguarding certain aspects of substantial public interests,[75] and the data must be processed and administered in accordance with the additional measures of the Regulation.[76] Relevant data protection authorities must be involved in the operation of sandboxes in such circumstances. Participants are also expected to produce a short summary of their research objectives and anticipated results to be published on the website of the appropriate competent authorities.[77]

It should be noted that while the sandboxes allow for innovation, they do not excuse liability of participants should they find themselves in breach of the Regulation or any other applicable national or international legislation.[78] Participants should therefore be wary that while it does permit activities that would otherwise be prohibited, it is not a "*carte blanche*" provision exculpating every action attributed to the advancement of AI.

[70] AI Regulation, Recital 71.
[71] AI Regulation, Article 53(1).
[72] AI Regulation, Recital 71.
[73] AI Regulation, Recital 72.
[74] AI Regulation, Article 54.
[75] AI Regulation, Article 54(1)(a).
[76] AI Regulation, Article 54.
[77] AI Regulation, Article 54(1)(j).
[78] AI Regulation, Article 53(4).

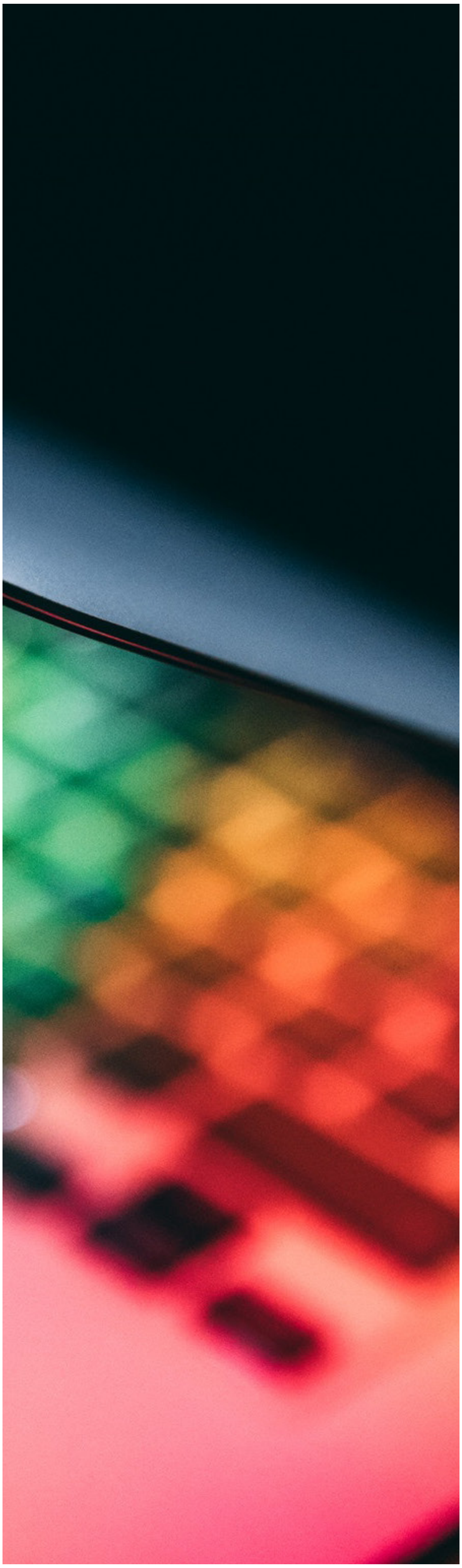
Assistance for SMEs

In recognising the necessity of smaller-scale provider involvement, the Regulation sets out a number of provisions reducing barriers to entry in order to facilitate their contribution.[79] Most notable are the prioritisation of access of small-scale providers and start-ups to the regulatory sandboxes that are due to be created[80] and the requirement that the interests and needs of smaller participants when determining fees for the conformity assessments mandated in the Regulation.[81]

The Regulation also supports innovation through a more soft-touch approach by encouraging Member States to develop initiatives to assist smaller-scale providers and users of AI.[82] Amongst other things, this includes sessions to increase awareness of the regulatory regime[83] and dedicated communication channels for the sharing of information.[84]

Authority Assistance

On a wider scale, the Regulation acknowledges that, in its infancy, the market may lack the necessary expertise to implement the provisions of the Regulation. To minimise the risk of a shortfall in expertise at a national level, the European Digital Innovation Hubs and the Testing and Experimentation Facilities have been considered to assist in implementing the proposed Regulation throughout the Member States.[85] In order to effectively implement many of the newly added conformity provisions, the Commission seeks to, insofar as possible, make available a number of accredited facilities throughout the European Union,[86] and therefore allow a more harmonious approach to certification and approval of AI Systems.



[79] AI Regulation, Recital 73.
[80] AI Regulation, Article 55(1)(a).
[81] AI Regulation, Article 55(2).
[82] AI Regulation, Article 55.
[83] AI Regulation, Article 55(1)(b).
[84] AI Regulation, Article 55(1)(c).
[85] AI Regulation, Recital 74.
[86] AI Regulation, Recital 75.

10.
Penalties and enforcement

Penalties

The Regulation requires Member States to set effective, proportionate, and dissuasive penalties (including administrative fines) for infringements of the Regulation.

The Regulation also specifies the following specific **sanctions**, which are structured in a similar way to the sanctions applicable under the GDPR and are substantial:

BREACH	PENALTY
Non compliance with the prohibition of the **Prohibited AI Practices**[87] Non compliance of a High-Risk AI System with the **Data and Data Governance obligations** (set out in Article 10).	Up to EUR30m **OR** If offender is a company, the higher of: up to EUR30m; or up to 6% of total worldwide annual turnover of preceding financial year.
Non-compliance of AI System with **any other requirements** or obligations under the Regulation (other than the Prohibited AI Practices or Data and Data Governance obligations)	Up to EUR20m **OR** If offender is a company, the higher of: up to EUR20m; or up to 4% of total worldwide annual turnover of preceding financial year.
Supply of incorrect, incomplete or false information to notified bodies and national competent authorities in reply to a request	Up to EUR10m **OR** If offender is a company, the higher of: up to EUR10m; or up to 2% of total worldwide annual turnover of preceding financial year.

The Regulation does not enable individuals to make complaints about AI Systems, meaning that enforcement of will lie solely with the competent authorities. However, nothing precludes individuals petitioning relevant regulatory authorities to undertake enforcement action if they consider a particular AI is being operated in contravention to the Regulation. Similarly, given the large degree of overlap between any likely user interaction with an AI System and processing of personal data that would fall within the ambit of GDPR, it is likely that those aggrieved by particular AI-based processing or decision-making may have direct rights of action against the relevant provider under the GDPR or other overlapping regulatory regimes.

[87] AI Regulation, Article 5.

Governance and the EU Database

At Union level, the Regulation establishes a new European Artificial Intelligence Board ("**EAIB**") which has overall governance oversight and responsibility for ensuring smooth and harmonised implementation of the Regulation. Its specific tasks include: (i) collecting and sharing expertise and best practices among Member States; (ii) contributing to uniform administrative practices in the Member States; and (iii) issuing opinions, recommendations or written contributions on matters related to the implementation of the Regulation.[88] The EAIB will be composed of national supervisory authorities[89] and will advise and assist the Commission on matters relating to the Regulation. As detailed above, a new EU database will also be established for stand-alone High-Risk AI Systems, which will complement the EAIB.

At a national level, each Member State is required to establish or designate national competent authorities for the purpose of ensuring the application and implementation of the Regulation, and to designate a national supervisory authority among the national competent authorities.[90] A framework of notified bodies and notifying authorities must also be designated or established (as further detailed above).

Enforcement

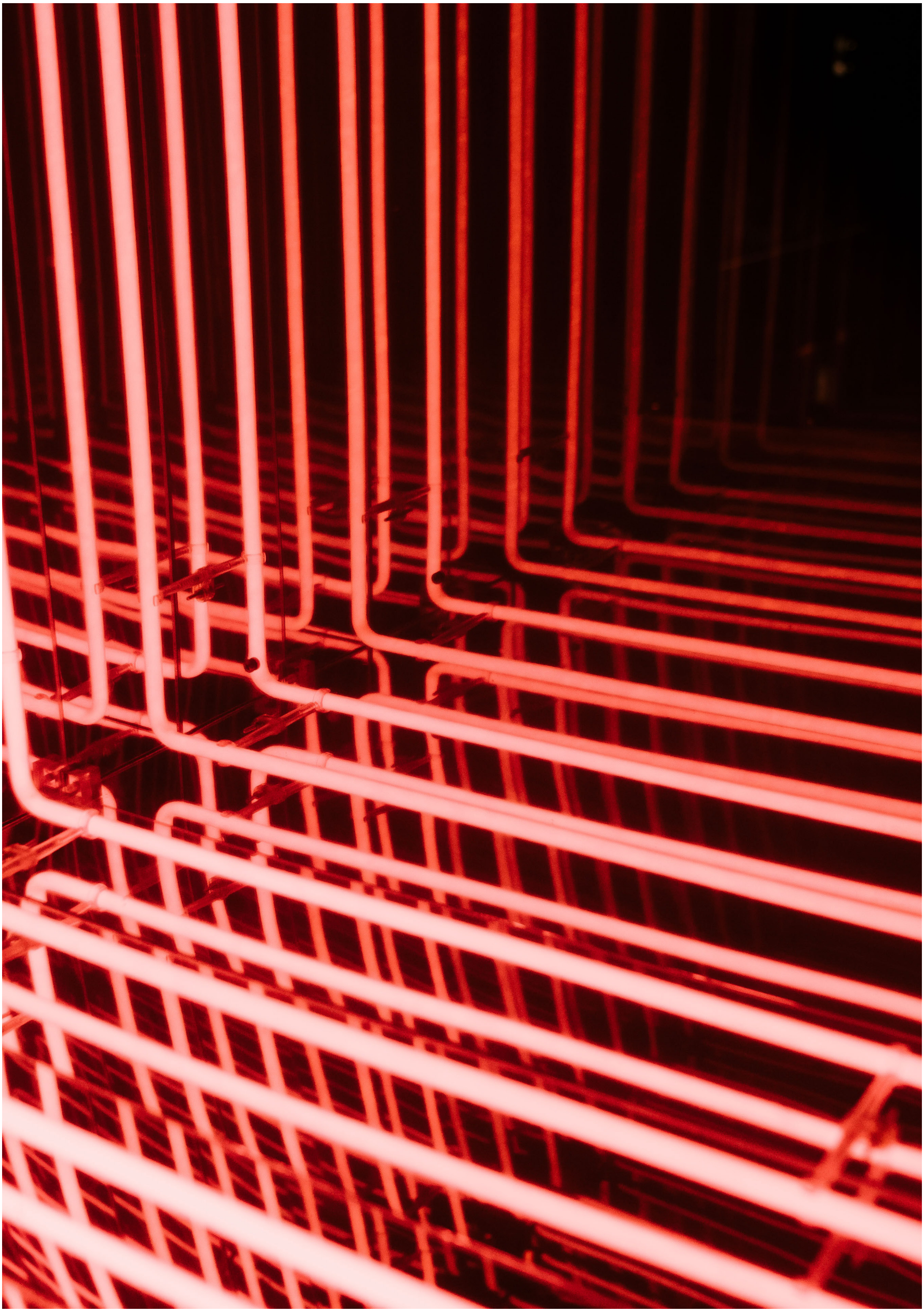
The primary mechanism for enforcing the Regulation is through the use of market surveillance and control of AI Systems in the Union market, in accordance with Regulation (EU) 2019/1020. The Regulation does not envisage the creation of any additional bodies or authorities at Member State level and the intention is that Member States should appoint existing sector authorities who will be entrusted with additional responsibilities of monitoring and enforcement of the Regulation.[91]

The market surveillance authorities will be granted access to data and documentation, including training, validation and testing datasets used by the provider and, where necessary to assess conformity with the High-Risk Requirements, the source code of the AI System.[92] Where the market surveillance authority of a Member State has sufficient reason to believe that an AI System presents a risk to the health or safety or to the protection of fundamental rights of persons, it can choose to evaluate the AI System concerned.[93]

Where the evaluation finds non-compliance with the Regulation, the market surveillance authority can require corrective actions to be taken by the AI System operator in a specified timeframe, with the ability to take all appropriate provisional measures to prohibit or restrict the AI System being made available in its national market, withdraw the product from its market, or recall the product, if corrective actions are not adhered to. There is also a safeguarding/ secondary supervisory procedure which enables other Member States to raise objections to the corrective action measures taken by the Member State in question.[94] Where the evaluation finds that the AI System complies with the Regulation, but still presents a risk to the health, safety or fundamental rights of persons or to any other aspects of public interest protection, the market surveillance authority can require the relevant operator to take all appropriate measures to ensure that the AI System no longer presents that risk, withdraw the AI System from the market, or recall it within a reasonable period.[95]

Market surveillance authorities will therefore have far-reaching audit, inspection and enforcement rights in this regard, and organisations will, to the extent they do not already, need to ensure their AI System can be easily audited by, and be prepared to engage with, existing authorities in the way described in this Section.

[88] AI Regulation, Article 58.
[89] AI Regulation, Article 57.
[90] AI Regulation, Article 59.
[91] Explanatory Memorandum, paragraph 5.2.6.
[92] AI Regulation, Article 64.
[93] AI Regulation, Articles 57 and 65.
[94] AI Regulation, Article 66.
[95] AI Regulation, Article 67.



11. What about non-High-Risk AI?

While not mandatory, the Regulation encourages Member States to have providers of non-High-Risks (i.e. lower-risk) AI create voluntary codes of conduct that would subject their AI to similar principles to those mandated in the Regulation for their High-Risk counterparts (specifically the High-Risk Requirements).[96]

The rationale behind this is that although low-risk AI does not create the same level of risk through its use, it must be deemed safe to place on the market or put into service.[97] These voluntary codes are to: (i) primarily focus on the High-Risk Requirements;[98] and (ii) be created by individual providers themselves, by organisations representing them, or by a combination of the two alongside any other stakeholders they may deem helpful.[99] Should they choose, providers are also encouraged to include provisions that will also assist in the move towards the EU's wider goals, such as environmental sustainability, accessibility, and diversity,[100] and indicates an approach by the EU to continue to develop AI throughout all market sectors.

In recent years, it has become increasingly commonplace for organisations to adopt their own voluntary ethical principles for the use of AI within their organisation, which seek to instil trust and send a message to the external market that the organisation has been responsible in its adoption and development of AI. It remains to be seen, however, whether organisations who are not subject to the Regulation will choose to adopt the codes of conduct envisaged in the AI Regulation in a similar fashion, which, while not mandated by the Regulation, would give similar comfort to customers/suppliers and potentially a competitive advantage to organisations who choose to adopt them, as compared to those who do not.

[96] AI Regulation, Recital 81 and Article 69(1).
[97] AI Regulation, Recital 82.
[98] AI Regulation, Article 69(1).
[99] AI Regulation, Article 69(3).
[100] AI Regulation, Article 69(2).

12. Final analysis

What does this mean in practice?

Any regulation with the potential for fines at the level in the proposed AI Regulation is undoubtedly significant, and the inclusion of penalties akin to the GDPR will certainly put compliance with the Regulation at the forefront of organisations' minds. Since higher-risk AI use cases will almost inevitably also require processing of personal data, providers found breaching one regulation risk the same malfeasance being found to breach the other. In such cases, AI providers are potentially exposed to fines totalling **10% of turnover** (up to 6% under the proposed AI Regulation plus 4% under GDPR). Whilst an eye-watering prospect, these potential fines are only one development to be taken into account by an organisation wishing to "future proof" how it procures, develops and/or use AI solutions. The bigger picture includes existing and proposed hard law as well as increased emphasis on the historically softer ethical considerations and governance.

We looked at some of these developments in more detail in March's alert: Regulating artificial intelligence: Where are we now? Where are we heading? (references to the EU White Paper are, of course, now out of date).

In terms of AI governance, the Regulation now necessitates organisations carry out analysis to determine the answers to key questions such as: (i) if their use of AI Systems falls into the definitions of 'Prohibited AI Practices', High-Risk AI Systems or is subject to the standalone transparency obligations for manipulation risk even if not deemed High-Risk; and (ii) what obligations now fall on them as either providers, users, importers or distributors of AI Systems. Consideration will also be required as to whether any of the Union Harmonisation Legislation is applicable and an organisation can therefore benefit from equivalence in existing obligations elsewhere in Union law.

The sale, import or procurement of complex technology solutions just got harder.

Once identified as relevant, the extensive obligations for High-Risk AI Systems such as conformity assessments (including which type of conformity assessment applies), declarations of conformity, CE markings, and registrations in the EU database will need to be integrated into internal product development and governance processes, as will regular monitoring to ensure compliance after an AI System has been placed on the market or put into service. We are already seeing industry bodies rallying together to address the task of producing robust technical criteria and standards, including certification schemes, that will help support third party conformity assessments and audits of High-Risk AI Systems,[101] as well as AI vendors themselves seeking to include AI governance and transparency as part of their core product offering.[102] New Regulation-compliant record keeping also looks set to become the norm to ensure compliance, and commercial organisations will seek to contractualise these obligations in relevant technology transactions in the future.

But the picture is far from all doom and gloom. As well as the requirement for detailed gap analysis, organisations should also look to make the most of the new opportunities such as regulatory sandboxes and other initiatives to foster innovation in the EU. As with the GDPR before it, there is also the advantage of business certainty and user trust. The proposed AI Regulation brings a framework within which AI developers and providers can develop, deploy and enhance systems in a compliant manner, and use the Regulation to create trusted platforms. Knowing that systems meet the regulatory 'gold standard' in the EU can be a material market advantage.

[101] See https://forhumanity.center/media

[102] For example, https://www.dataiku.com/product/key-capabilities/

The sheer number of documents detailing the current and proposed hard and soft regulation of AI more generally, as well as current best practice, can prove daunting for any responsible organisation to digest and action. Where that organisation is operating in a regulated or sector and/or across many jurisdictions the challenge increases. But in practice, key themes crop up time and time again:

- the governance process around the organisation's decision to use AI at all;
- the quality of the training data used to train the algorithm (be that by the third party supplier, the organisation using the AI tool or a combination of the two);
- the degree of human oversight;
- the accuracy, robustness and security of the IT system; and
- transparency and "explainability" of AI decision making and the ability to challenge the decision.

Comprehensive record keeping is essential which, combined with audit (perhaps in a more continuous mode rather than the traditional static review) can support certification and, ultimately, the broader eco-system of trust, desired by policy makers.

The final, and key, overarching principle common to proposed Regulation around the globe is that it should be risk-based. In other words, flexible enough to apply with only a light touch, if at all, to relatively insignificant use of AI; comprehensive for the critical and/or socially sensitive decision making which incorporates AI. Context is key, not just technology.

In practice, many organisations are able to build upon, and refine, their existing processes rather than start from a blank sheet. A gap analysis can be a useful starting point. It is not unusual for an organisation to be strong on requirements which overlap with GDPR but need to more fully develop its AI governance processes and/or perhaps adapt to the increased significance of using AI ethically and responsibly. The impact assessments will be a familiar step to those who have undertaken GDPR data protection impact assessments (DPIAs) for example – you may already be aware of our set of Data Protection products and services here https://www.dlapiper.com/en/us/focus/data-protection/.

Similarly, the Global AI team at DLA Piper have developed an AI Scorebox which aligns with both the AI Regulation and developing best practice guidance from around the world; enabling organisations to assess their regulatory maturity in advance of the sale, import or deployment of complex technologies, particularly involving AI.

Next steps

The European Parliament and the Member States will need to adopt the Commission's proposals on a European approach for Artificial Intelligence and on Machinery Products in the ordinary legislative procedure.[103] Once adopted, after much anticipated scrutiny and debate, the Regulation will be directly applicable across the EU. It will enter into force on the 20th day after its publication in the Official Journal of the European Union and it will apply from two years after the entering into force,[104] giving organisations two years to prepare for the then final requirements of the Regulation. It is expected that on 'Day 1', it will apply to all AI Systems in the market, which will therefore include AI Systems already launched and developed as well as any new ones.

DLA Piper will be monitoring the progress of the proposed Regulation closely as part of its wider AI Regulation watch, and will provide ongoing commentary, together with advice on how to best prepare your organisation for this ground-breaking new Regulation, as it progresses.

For further analysis from other jurisdictions and perspectives, please see commentary from DLA colleagues on DLA Piper's Technology's Legal Edge Blog.

[103] During the ordinary legislative procedure, proposals move iteratively through the European Parliament and the European Council in a number of readings before an act is adopted as EU law. See https://www.europarl.europa.eu/olp/en/ordinary-legislative-procedure/overview for further details.

[104] AI Regulation, Article 85.

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at dlapiper.com.
This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication. This may qualify as "Lawyer Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.