SQUIRE PATTON BOGGS

The Proposed New EU Regulatory Regime for Artificial Intelligence (AI)

EU – September 2021

Introduction

In April 2021, the EU Commission (EC) proposed a suite of new legislative and non-legislative proposals related to artificial intelligence (AI): in a proposed Regulation laying down rules on Artificial Intelligence ("Artificial Intelligence Act – AIA"), the EC attempts the **first-ever comprehensive legal framework** for this highly debated and fast-developing **family of technologies**. We set out below a high-level summary of the key policy considerations and proposed new restrictions, risk-classifications and related obligations for AI providers and users stemming from this landmark proposal.

The proposed AIA is accompanied by a **revised AI Coordination Plan** with member states (Plan), which aims to "accelerate, act and align AI policy priorities and investments across Europe" in order to allow Europe to obtain global leadership in the development of **human-centric, sustainable, secure, inclusive and trustworthy AI**. The Plan also lays out the existing/planned projects related to AI at the EU level, as well as the various funding opportunities, including via the new Recovery and Resilience Facility, which foresees a 20% digital expenditure target at member state level.

Furthermore, the EC has proposed a **revised machinery regulatory framework** in order to cater for AI technologies embedded in a broad range of consumer and professional products. The proposed new Machinery Regulation, which will replace the existing Machinery Directive (Directive 2006/42/EC), seeks to ensure safety, and established an EU-wide conformity assessment when putting such AI-enhanced products on the EU market.

Status Quo of the EU Policy Debate

The AIA proposal follows the **standard EU lawmaking procedure** (i.e. the "ordinary legislative procedure") and is, thus, now debated in parallel in the European Parliament (EP) and Council. The complex and far-reaching nature of the proposed AIA will undoubtedly lead to lengthy negotiations that are likely to continue well into 2022.

The **EP has been particularly vocal** about the need to create a regulatory framework establishing the limitations for AI technologies and robotics, especially under a well-defined civil liability regime for AI products and services. Even though the Civil Liberties, Justice and Home Affairs (LIBE) and the Legal Affairs (JURI) committees have been more involved in the early phases of the AI policy debate, the **Internal Market and Consumer Protection (IMCO) Committee has been named as the leading committee for the proposed AIA**. Nevertheless, the LIBE and JURI committees are keen to maintain a competence on the legislative file as Associated Committee, alongside the Industry, Research and Energy (ITRE) Committee.

The IMCO Committee Rapporteur Brando Benifei (S&D Group, Italy) hopes that the EU Parliament would be in a position to adopt its negotiating mandate by the end of 2021 – which seems very ambitious given the complexity of the AIA proposal.

The EP is expected to pursue an aggressive stance on provisions that would impact citizens' fundamental rights, for instance in the area of remote biometric recognition. The EP is expected to suggest additional AI practices that shall be banned in the EU, and we also expect the EP to challenge the possibility to self-certify high-risk AI systems by their providers.

The **Council of the EU** has debated the proposed AIA at the technical level. The Council of Ministers already held a first exchange of views on the AIA proposal in June. The proposed AIA is a top priority for the Slovenian Presidency, which aims to reach a **General Approach** by the end of its mandate in December 2021.[1] However, we expect these complex deliberations to last well into 2022, leaving it up to the French or maybe even the Czech Council Presidency to continue and possibly conclude the Council's General Approach.

While some voices among EU member states pick up on industry concerns about the potential impact of the AIA on competitiveness and innovation, a principal concern for a number of member states lies in more narrowly defined concerns about the potential for AI systems to support law enforcement, counterterrorism, etc.

The New Artificial Intelligence Act (AIA)

From a policy perspective, the EC recognises the **benefits** that AI can play in society, from improved medical care to better education. However, as **some AI systems create risks**, the EC considers that a new regulatory regime is necessary in order to protect users, including from a fundamental rights and user safety perspective without constraining the technological development. The EC also hopes to provide more clarity and legal certainty around AI in order to **establish trust and excellence in AI solutions**, to fuel their uptake and expansion in Europe, but also to prevent fragmentation in the European regulatory regime for AI systems.

Together with the fact that various AI-enhanced products and services are already in the EU market, the EC has proposed the **first comprehensive regulatory regime for AI worldwide**. The AIA proposal incorporates feedback from external stakeholders and expert groups.[2]

[1] The Slovenian Council Presidency will host a High-Level Conference on AI on 13 to 14 September 2021.

[2] E.g. the High-Level Expert Group on Artificial Intelligence; the High Level Expert Group on the Impact of the Digital Transformation on EU Labor Markets; or the Expert Group on Liability and New Technologies.

Scope

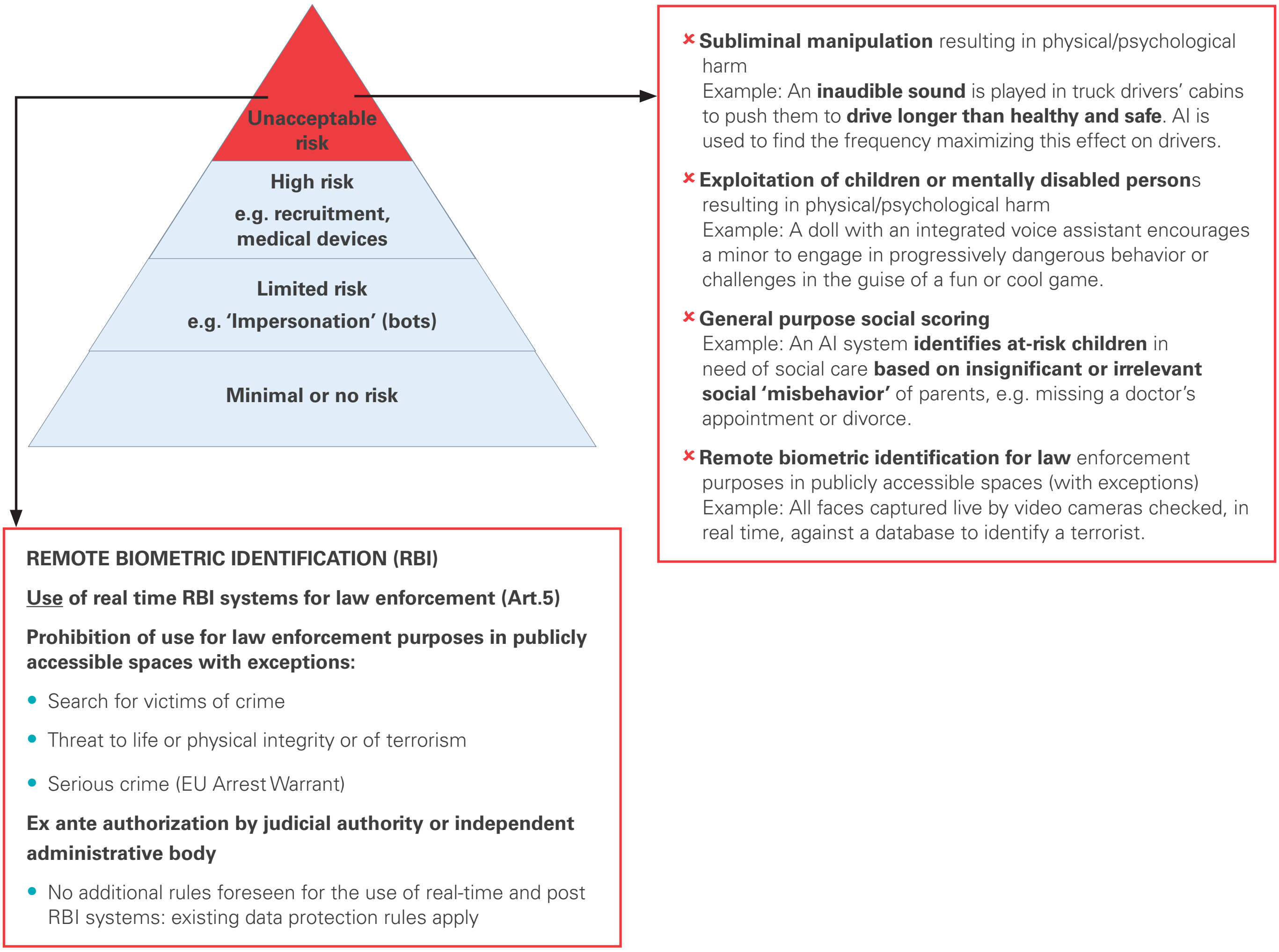
The **scope** of the proposed AIA[3] (Title I) covers providers that place AI systems on the market, or put them into service, irrespective of whether those providers are established within or outside the EU. Users of AI systems are covered by the new rules if they are located in the EU. The AIA will even apply if the provider and user is established outside the EU, but the output produced by those systems is used in the EU. AIA will, thus, apply to providers of AI systems (e.g. a developer of a CV-screening tool), as well as users of such AI systems (e.g. a bank buying this CV-screening tool). It will not apply to private, non-professional use. In addition, AI systems exclusively developed and used for military purposes are exempt.

Risk Categorisation

The EC proposes a **risk-based categorisation** of AI systems with **four levels of risk and related regulatory obligations and restrictions**:

(i) Unacceptable Risk (Title II)

A very limited number of particularly harmful AI practices that contravene EU values are **prohibited** because they violate fundamental rights.[4] These prohibited practices include "**social scoring**" by governments, the **exploitation of vulnerabilities** of children or otherwise disabled persons, the use of **subliminal techniques** that can cause physical and psychological harm and – subject to narrow exceptions – **live remote biometric identification** systems in publicly accessible spaces used for law enforcement purposes.


Unacceptable risk
High risk
e.g. recruitment, medical devices
Limited risk
e.g. 'Impersonation' (bots)
Minimal or no risk

- ✗ **Subliminal manipulation** resulting in physical/psychological harm
  Example: An **inaudible sound** is played in truck drivers' cabins to push them to **drive longer than healthy and safe**. AI is used to find the frequency maximizing this effect on drivers.
- ✗ **Exploitation of children or mentally disabled person**s resulting in physical/psychological harm
  Example: A doll with an integrated voice assistant encourages a minor to engage in progressively dangerous behavior or challenges in the guise of a fun or cool game.
- ✗ **General purpose social scoring**
  Example: An AI system **identifies at-risk children** in need of social care **based on insignificant or irrelevant social 'misbehavior'** of parents, e.g. missing a doctor's appointment or divorce.
- ✗ **Remote biometric identification for law** enforcement purposes in publicly accessible spaces (with exceptions)
  Example: All faces captured live by video cameras checked, in real time, against a database to identify a terrorist.

REMOTE BIOMETRIC IDENTIFICATION (RBI)

Use of real time RBI systems for law enforcement (Art.5)

Prohibition of use for law enforcement purposes in publicly accessible spaces with exceptions:

- Search for victims of crime
- Threat to life or physical integrity or of terrorism
- Serious crime (EU Arrest Warrant)

Ex ante authorization by judicial authority or independent administrative body

- No additional rules foreseen for the use of real-time and post RBI systems: existing data protection rules apply

Source:
DG CNECT Presentation 8 June 2021, edited by Squire Patton Boggs

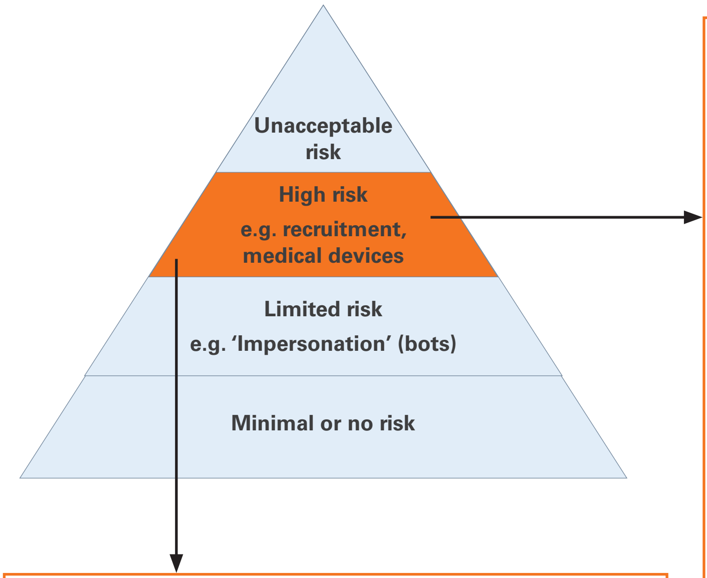
[3] A regulation is an EU legal instrument that will directly apply in all EU member states and, thus, needs to additional step at the national level to become applicable law.

[4] E.g. EU Charter of Fundamental Rights.

(ii) High Risk (Title III, Annex III)

Article 6 defines **"high-risk" AI systems** as those where the AI system is intended to be used as a safety component of a product, or is itself a product, **and** this product is **subject to an existing third-party conformity assessment** (e.g. engine-powered vehicles, trains and planes).

In addition, the **EC has the power to directly designate an AI system as high risk** by adding it to Annex III of the AIA, subject to certain criteria. Given the fast evolution of high-risk AI use cases, the EC proposes to review the list of covered systems on an annual basis. The EC would adopt delegated acts to change the list of high-risk AI systems in Annex III.


Unacceptable risk
High risk
e.g. recruitment, medical devices
Limited risk
e.g. 'Impersonation' (bots)
Minimal or no risk

1. **Safety components of regulated products** (e.g. medical devices, machinery) which are subject to third-party assessment under the relevant sectorial legislation
2. **Certain (stand-alone) AI systems in the following areas**
   - Biometric identification and categorization of natural persons
   - Management and operation of critical infrastructure
   - Education and vocational training
   - Employment and workers management, access to self-employment
   - Access to and enjoyment of essential private services and public services and benefits
   - Law enforcement
   - Migration, asylum and border control management
   - Administration of justice and democratic processes
3. Establish and implement **risk management** processes & in light of the **intended purpose** of the AI system
   - Use high quality **training, validation and testing data** (relevant, representative, etc.)
   - Establish **documentation** and design logging features (traceability and auditability)
   - Ensure appropriate certain degree of **transparency** and provide users with **information** (on how to use the system)
   - Ensure **human oversight** (measures built into the system and/or to be implemented by users)
   - Ensure **robustness, accuracy** and **cybersecurity**

REMOTE BIOMETRIC IDENTIFICATION (RBI)

Putting on the market of RBI systems (real time and ex-post)

- **Ex ante third party conformity assessment**
- Enhanced logging requirements
- ''Four eyes'' principle
  - No additional rules foreseen for the use of real-time and post RBI systems: existing data protection rules apply

Annex III contains a number of AI uses cases that could (potentially) adversely affect people's health, safety or their fundamental rights, and are, therefore, deemed "high risk". These high-risk use cases include AI systems that, for instance, (i) use **biometric identification**, (ii) manage or operate **critical infrastructure**, (iii) are used in **educational or vocational training**, (iv) are used for **recruiting or HR/employment-related** tasks, (v) determine the **access to essential private and public services, including benefits**, (vi) are used in a **law enforcement** context, (vii) are used in a **migration, asylum or border management** context or (viii) are used in the **administration of justice** or **democratic processes**.[5]

High-risk AI systems can only be placed on the EU market, or put into service, if they comply with **certain minimum requirements**. Before placing a high-risk AI system on the EU market, or otherwise putting it into service, providers must subject it to an **ex-ante conformity assessment**. Such a conformity assessment has to be repeated if there are substantial modifications made to the system. In certain cases, an **independent notified body** needs to be involved in that assessment process.

Providers of high-risk AI systems will also have to implement quality and risk management systems to ensure their compliance with the new requirements and to minimise risk for users and affected persons, even after the product has been placed on the market. **Market surveillance authorities** will support the post-market monitoring via audits.

For **high-risk AI systems**, the EC proposes a range of **new mandatory requirements (Title III)**, including:

The establishment of a **risk management system** (Art. 9), which in a continuous and iterative process manages the risks associated with the AI system

- **Quality criteria** regarding the training, validation and testing data sets used (Art. 10)
- Technical documentation describing, *inter alia*, the compliance of the AI system with applicable rules, including for law enforcement purposes (Art. 11)

[5] See AIA, Annex III, for details.

- **Record-keeping requirements** to ensure an appropriate level of traceability of the AI system's functioning (Art. 12)
- **Transparency and provision of information** to enable users to interpret the system's output and use appropriately (Art. 13)
- Systems are **effectively overseen by humans** (Art. 14)
- Systems need to achieve appropriate levels of **accuracy, robustness and cybersecurity** throughout their life cycle (Art. 15)

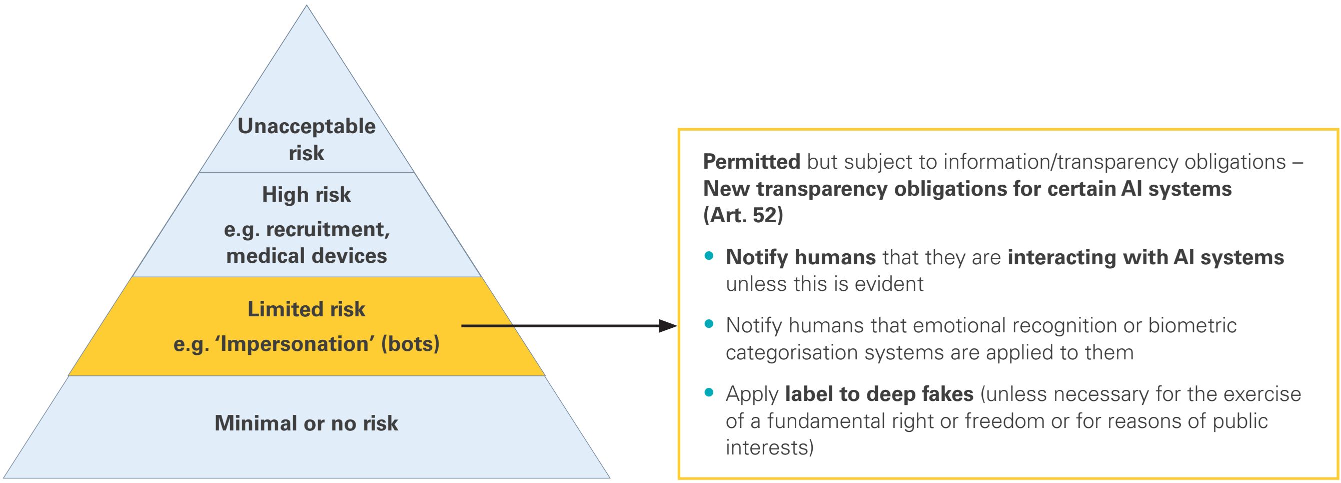
For the **providers of high-risk AI systems**, new obligations include:

- General obligation to observe the abovementioned list of requirements
- Maintain a **quality management system** (Art. 17)
- Ensure their systems undergo the relevant **conformity assessment procedure** (Art. 19)
- Keep **automatically generated logs** (Art. 20)
- Obligation to **take corrective action** when the AI system is not in conformity with the AIA (Art. 21), **duty to notify** serious incidents or any malfunctions to national competent authorities (Art. 22) and **need to cooperate** with these authorities (Art. 23)
- Specific rules apply to **importers** of high-risk AI systems (Art. 26), as well as **distributors** (Art. 27) and **users** (Art. 29)

The EC will establish a publicly **accessible register of high-risk AI applications** and systems (Art. 60).

(iii) Limited Risk (Title IV)

Certain AI systems will only be subject to **new transparency requirements** (Title IV), for instance, where there is a risk of manipulation (e.g. chatbots) or deceit (e.g. deep fakes). Natural persons should be aware that they are interacting with an AI system, unless this is obvious from the circumstances and the context of the use. Law enforcement exceptions exist.

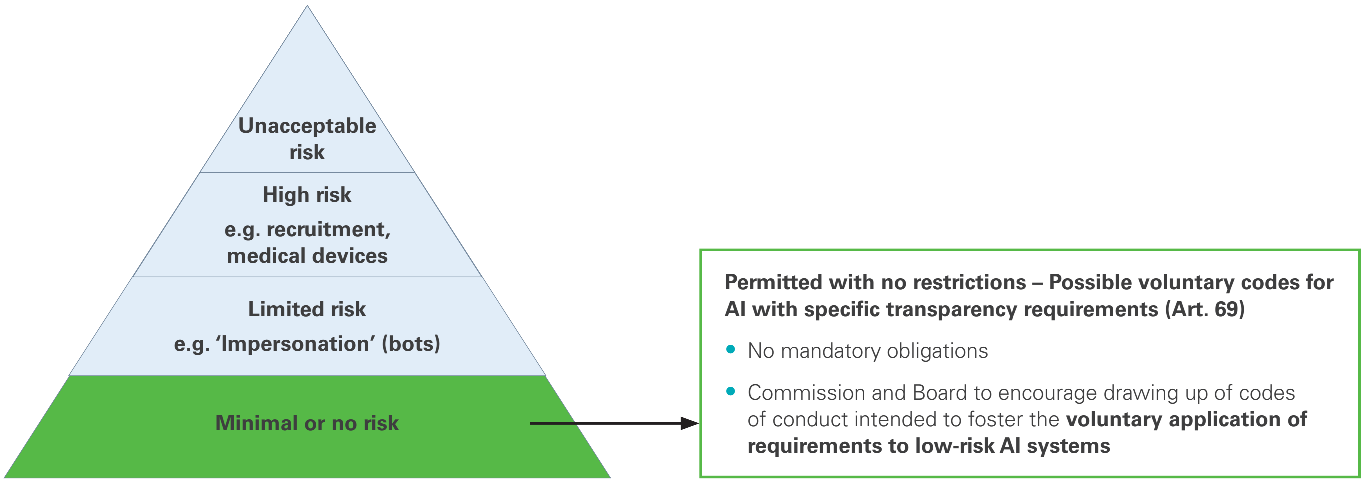

Unacceptable risk
High risk
e.g. recruitment, medical devices
Limited risk
e.g. 'Impersonation' (bots)
Minimal or no risk

Permitted but subject to information/transparency obligations – **New transparency obligations for certain AI systems (Art. 52)**

- **Notify humans** that they are **interacting with AI systems** unless this is evident
- Notify humans that emotional recognition or biometric categorisation systems are applied to them
- Apply **label to deep fakes** (unless necessary for the exercise of a fundamental right or freedom or for reasons of public interests)

(iv) Minimal Risk

All other AI systems can be developed and used subject to the existing legislation without any new legal obligations via the AIA. According to the EC, a large number of AI systems currently in use in the EU fall into this category. The EC is recommending **voluntary codes of conduct** for providers of such AI systems.


Unacceptable risk
High risk
e.g. recruitment, medical devices
Limited risk
e.g. 'Impersonation' (bots)
Minimal or no risk

Permitted with no restrictions – Possible voluntary codes for AI with specific transparency requirements (Art. 69)

- No mandatory obligations
- Commission and Board to encourage drawing up of codes of conduct intended to foster the **voluntary application of requirements to low-risk AI systems**

Oversight/Enforcement (Title VI)

The proposed **enforcement** measures foresee **penalties of up to €30 million or 6% of global revenue (whichever is higher) for the most serious infringements** of the new regime, making the penalty regime even more draconic than those incurred by violations of the General Data Protection Regulation (GDPR). Such is the case related to the use of prohibited AI systems and the violation of the data-governance provisions when using high-risk AI systems.

All **other cases of non-compliance** with the AIA are subject to a **penalty of up to €20 million or 4% of global revenue (whichever is higher)**. The mere supply of **incorrect, incomplete or misleading information to competent authorities** already carries a **potential penalty payment of up to €10 million or 2% of global revenue**.

Member state authorities will play a key role in the application and enforcement of the new AI regulatory regime. Newly designated **national AI supervisory authorities** shall supervise the AIA application, as well as carry out market surveillance activities. At the EU level, a new **European Artificial Intelligence Board** shall be established and will support and guide the EC and national authorities in their related activities.

Although enforcement rests with member states, as is the case for GDPR, one can expect that the penalties will be phased-in, with the initial enforcement efforts concentrating on those who are not attempting to comply with the regulation. One can also expect to see ample material on how to comply with the regulation, as well as interpretive notes.

Potential Implications for Industry

Somewhat similar to the GDPR, the AIA proposal as proposed will have an extraterritorial reach and, thus, potentially affect a large number of firms with customers based in the EU. While the regime is not yet set in stone, but in the midst of the EU lawmaking process, the direction of travel suggested by the EC is clear.

Given that the proposed AI regulatory regime is the first of its kind worldwide, many experts expect it to have a major influence on other regions in the world – this is dubbed the "Brussels effect"[6] – similar to what was experienced following the adoption of the GDPR. This makes it all the more important for all interested stakeholders to engage in the debate now in order to secure an adequate EU regime for AI.

While engaging in the current regulatory and policy debate is key, many organisations will also need to start preparing for the new AIA, and address the risks associated with the new AI rules more broadly.

What Is Next?

The legislative process on the AIA proposal will continue to develop in the months to come, with the debate to continue through 2022. Next to the current legislative debates, the EC will, in 2022, come forward with additional legislative measures regarding AI, focused on **adapting the liability framework** to be applied to emerging technologies.
This will likely include a revision of the **Product Liability Directive**, and a legislative proposal related to the **liability of AI systems**. Similarly, the EC envisages proceeding with adaptations to existing sectorial safety legislation, including the **General Product Safety Directive** or the **Radio-Equipment Directive**.

Importantly, the EC will, in 2021, publish a **Policy Program** to implement **Europe's Digital Compass**, which encompasses a broader range of policies relevant to align the EU's 2030 digital ambitions. It will set out a road map on the general principles and commitments that member states will be advised to follow and concrete actions needed to address the policy objectives. Usage of AI systems is listed as one of the main areas to be developed to reach the EU's 2030 digital ambitions, which include 75% of European enterprises having taken up cloud computing services, big data and AI solutions.

How We Can Help

The EU envisages setting the standards that will pave the way for ethical technology worldwide while simultaneously ensuring the EU remains competitive. As evidenced by the responses to the public consultation on the proposed AIA, the **industry has voiced strong concerns** in relation to the far-reaching implications the future law would entail for their business. Many argue that the AIA would create unnecessary and burdensome compliance obligations, which will also be very costly for companies. On the other side of the spectrum, the civil society, trade unions and data protection authorities share the belief that the proposed law does not go far enough and should impose stronger restrictions for high-risk AI usage and compliance obligations for AI systems. Whether the **proposed AIA becomes a *de facto* global standard setter**, as for GDPR, or drives AI innovation to other jurisdictions with less intrusive legislation remains an **open question**.

However, what seems beyond doubt is that the EU legislative process will work its way towards the **first major regulation of AI systems globally**, and that any company seeking to do business in or with the EU will have to comply. The legislative proposal constitutes the foundation upon which the EC will continue formulating its future policies around the various facets of AI. The ever-evolving nature of AI systems makes it difficult to ensure the legislative framework will be future-proof. However, at this stage of the legislative process, where the technical elements of the proposed law will be deliberated, this will be the ideal time to understand the direction of the negotiations. The **current legislative phase provides ample opportunities to engage with policymakers** in order to influence this critically important new AI regulatory regime.

[6] "The Brussels Effect – how the European Union rules the world", by Anu Bradford, Oxford Press.

With us as your trusted advisors on your side, you will be able to spot, assess and understand the risk and opportunities for your organisation from the AIA proposal and the broader policy and political context that keeps developing alongside the legislative debate. We will support you in devising and executing successful strategies to shape the policy debate.

We have decades of experience in shaping technology related laws and regulations in Brussels, and our team has an unrivalled network of contacts within EU policymakers and other relevant stakeholders.

Additionally, we can help you think through what the new AI regulatory regime may mean for your organisation, and which steps can already now be taken in order to anticipate and manage the new regime. Such steps may include, inter alia, the following:

- An inventory of all AI systems used by the organisation
- A risk-classification system
- Risk-mitigation measures
- Independent audits
- Data risk-management processes
- An AI governance structure

In addition, we can track all of the above against the evolving policy context as the legislative debates continue. We stand ready to assist you with this crucial step.

As a full-service global law firm, we provide insight at the point where law, business and government meet, giving our clients a voice, supporting their ambitions and achieving successful outcomes. Our multidisciplinary team of more than 1,500 lawyers and public policy experts in 45 offices across 20 countries provides unrivalled access to expertise and invaluable connections on the ground. It is a seamless service that operates on any scale – locally or globally. It encompasses virtually every matter, jurisdiction and market – and we place our clients at the centre.

We combine sound legal counsel with a deep knowledge of our clients' businesses to resolve their legal, public policy and political challenges. We care about the quality of our services, the success of our clients and the relationships that are forged through those successes. Our client base spans every type of business, both private and public, worldwide. We advise a diverse mix of clients, from Fortune 100 and FTSE 100 corporations to emerging companies, and from individuals to local and national governments. Leveraging local connections, while exerting global influence, we are commercial, connected and committed.

Our Public Policy Practice Group works with clients to make sure they are heard, at the right time, by the right people, with the right message in Washington DC, Brussels, London, Canberra and other major capitals around the world.

Visit our European Public Policy and International Policy webpages for more information on our team and capabilities.

Contacts

Wolfgang Maschek
Partner, Chair of European Public Policy Practice, Brussels
T +32 2 627 1104
E wolfgang.maschek@squirepb.com

Rosa Barcelo
Partner, Co-Chair, Global Data Privacy, Cybersecurity & Digital Assets Practice, Brussels
T +322 627 1107
E rosa.barcelo@squirepb.com

Matthew Kirk
International Affairs Advisor, London
T +44 20 7655 1389
E matthew.kirk@squirepb.com

Georg Serentschy
Senior Advisor, Brussels
T +32 2 627 1111
E georg.serentschy@squirepb.com

Christina Economides
Public Policy Advisor, Brussels
T +32 2 627 1105
E christina.economides@squirepb.com

Francesca Zuccarello Cimino
Associate, Brussels
T +32 2 627 1108
E francesca.zuccarellocimino@squirepb.com

The opinions expressed in this update are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.