simmons+simmons

Quick guide to the EU draft AI Regulation

APRIL 2021

This quick guide addresses:

- Context to the draft Regulation
- What you should do in light of the draft Regulation
- Key points of the draft Regulation (including hyperlinks to the relevant provisions)
- How we can help

Context

- The EU has now published its eagerly-awaited draft Regulation on AI, which President von der Leyen promised shortly after her appointment.
- This is a significant piece of legislation which will apply to providers, users, importers and distributors of AI systems. It will have a wide territorial reach (eg it will apply to non-EU organisations that supply AI systems into the EU) and there may be significant financial penalties for non-compliance.
- The draft Regulation adopts a risk-based approach. Some AI uses are prohibited; others ("high-risk AI systems" or HRAIS) subject to onerous requirements; and many are not caught by the draft Regulation at all. The focus is on the safety and fundamental rights of EU citizens at its core.
- The majority of the draft Regulation covers the HRAIS requirements. It also seeks to establish and regulate the functioning of various EU and national bodies that will oversee the Regulation.
- The draft Regulation will now go through a detailed legislative process, during which it is likely to be amended. It is unlikely to become binding law for 12-24 months. Even once it becomes binding, there will be a grace period of potentially 24 months before the main requirements will come into force.
- Nevertheless, as we note below, organisations should start thinking now about the potential impact of the draft Regulation on their business.

What should you do in light of the draft Regulation?

- The draft Regulation is likely to change before it is implemented and there will be a grace period to ensure compliance thereafter. However, the risk-based approach and core regulations of the draft Regulation are unlikely to change.
- Given that the draft Regulation contains onerous obligations (and heavy penalties), which will apply to AI systems from the design stage, we think that organisations should start to prepare now for this regulation.
- In particular, we suggest that both providers and users of AI systems:

Familiarise themselves, and ensure that the relevant parts of their organisations (eg procurement and sales teams) are familiar with the key provisions of the draft Regulation.

Undertake an impact assessment of the draft Regulation ie check whether they are using or intend to use any prohibited AI or whether they are likely to be caught by the HRAIS requirements.

If they are developing or intend to develop, or are using or intend to use HRAIS, they should consider what steps they should take now to ensure they are not caught out by the regulation in the future eg by ensuring that any HRAIS is designed with the substantive obligations in mind (particularly around data and record-keeping) and by ensuring that sufficient information is available now to be able to develop risk management and quality management systems in the future.

Consider what contractual changes to make eg to standard terms or to contractual protection / risk-allocation provisions, to future-proof against the regulation.

Key points

Broad definition of "AI system":

The key requirements set out below will apply to any "AI system". This is defined broadly in Article 3(1) as "*software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*". Annex I includes "*logic- and knowledge-based approaches*", which seems to go further than conventional AI systems.

Prohibited AI use (Article 5): The draft Regulation contains a few prohibitions on AI use:

- AI systems or uses that deploy "subliminal techniques" or exploit any vulnerabilities (eg disabilities) to materially distort behaviour and which could cause physical or psychological harm
- Use by public authorities of AI systems used to evaluate or classify trustworthiness of people (eg "social scoring" systems), which results in detrimental treatment
- "Real-time" remote biometric identification systems (eg facial recognition systems) used in public spaces for law enforcement purposes, unless: (i) they are used to target specific potential victims of crime, to prevent imminent threat to life or safety, or to detect criminals whose offences are punishable by a maximum of 3 years' detention, (ii) there are "necessary and proportionate" safeguards in place regarding period and geographical scope of use, and (iii) their use has been approved by the Member State.

High-risk AI systems (HRAIS):

- **What are HRAIS?** Under Article 6, HRAIS are: (i) products or components covered by the EU legislation listed in Annex II (eg medical devices), or (ii) the AI systems listed in Annex III, including those used:
    - to identify people using remote biometric identification (whether real-time or not) eg facial recognition systems
    - as safety components in the management and operation of essential public infrastructure eg AI used in public utilities services utilities
    - to determinate access to education institutions or in assessing students in education eg AI systems used to grade exams
    - in recruitment processes eg AI systems used to score candidates or review job applications
    - in employment promotion or termination decisions or in reviewing work performance or behaviour
    - in migration, asylum and border control management
    - in various law enforcement and judicial contexts

Key points

- **Distinction between providers and users:** the HRAIS obligations summarised below apply principally to "providers" of AI systems, rather than "users":
    - "Providers" are those who develop or have developed an AI system with a view to placing it on the market or putting it into service under their own name
    - "Users" are those under whose authority an AI system is deployed

    These definitions are not as clear as they could be, and note that a user will be considered to be a provider if they: (i) deploy the HRAIS in their own name or trademark, (ii) modify the intended purpose of a HRAIS that is already on the market, or (iii) make a "substantial modification" to the HRAIS (Article 28).

- **Substantive obligations for HRAIS providers:** HRAIS providers are subject to extensive and onerous obligations, including:
    - Risk management system: implementing process for entire lifecycle of HRAIS to identify, analyse and mitigate risks (Article 9)
    - Data and data governance measures: training and testing of HRAIS using data shall be undertaken in accordance with Article 10
    - Technical documentation: drafting comprehensive "manual" for HRAIS which contains, at a minimum, the Annex IV information (Article 11)
    - Record-keeping: HRAIS must be designed to ensure automatic logging of events eg period of use and input data reviewed (Article 12) and providers must keep these logs (Article 20)
    - Transparency: HRAIS must be accompanied by instructions for use which include detailed information including their characteristics, capabilities and limitations (Article 13)
    - Human oversight: HRAIS must be designed so they can be overseen by humans, who should meet various requirements eg being able to understand the HRAIS and to stop its use (Article 14)
    - Accuracy, robustness and cybersecurity: HRAIS must be accurate (with accuracy metrics included in instructions for use), resilient to errors or inconsistencies (eg through fail-safe plans) and resilient to cyber-attacks (Article 15)
    - Quality management system: HRAIS providers must put in place a comprehensive quality management system which includes at least the extensive Article 17 information requirements.
    - Post-market monitoring: HRAIS providers must document a system to collect and analyse data provided by users on the performance of the HRAIS throughout its lifetime (Article 61).

Key points

- **Procedural obligations for HRAIS providers**: HRAIS providers are also subject to various procedural obligations before they supply any HRAIS:
    - Conformity assessment: providers must ensure their HRAIS undergoes a "conformity assessment procedure" before the HRAIS is supplied (Article 19), although conformity can be presumed in certain circumstances (see Article 40, Article 41 and Article 42). For biometric identification systems, conformity must be assessed by the relevant "notified body" using the Annex VII procedure. For all other HRAIS, the Provider can undertake a self-assessment following Annex VI.
    - Conformity declaration, CE marking and registration: If the HRAIS passes the conformity assessment, the provider must draw up a written EU declaration of conformity (Article 48), affix a CE Marking to the HRAIS documentation (Article 49) and register the HRAIS in the EU database (Article 51).
    - Reporting obligations: HRAIS providers must report to the relevant authority within 15 days any "serious incident" or "malfunctioning" of the HRAIS which constitutes a breach of EU obligations intended to protect fundamental rights (Article 62).

- **Obligations for HRAIS Users:** HRAIS Users are subject to only limited obligations; notably, to ensure they use the HRAIS in accordance with its instructions of use, to monitor the operation of the HRAIS and to keep a record of the logs generated by the HRAIS (if under their control) (Article 29).

Other AI systems: AI systems or use which are not prohibited or HRAIS are subject to very little regulation:

- Save for two specific circumstances, the only general requirement is a limited obligation of transparency: providers must ensure that AI systems that are intended to interact with individuals are designed and developed to ensure that those individuals are aware that they are interacting with an AI system (Article 52).

- Member States are encouraged to facilitate codes of conduct being drawn up (by organisations or individual providers) to "foster the voluntary application" to non-high-risk AI systems of the substantive HRAIS obligations noted above (Article 69).

Financial penalties (Article 71):

- Fine of up to 6% of total worldwide revenue for non-compliance with: (i) prohibited AI uses, and (ii) data and data governance measures for HRAIS in Article 10.

- Fine of up to 4% of total worldwide revenue for non-compliance with any other requirement or obligation.

How we can help

Want to find out more about how our team can help with your AI legal issues? Get in touch.

We can help in the following ways:

- Providing advice on the potential application of the draft Regulation
- Assist with an impact or risk assessment to assess how the draft Regulation might affect your business
- Assist in ensuring compliance with the requirements of the draft Regulation to future-proof your AI systems e.g. by advising on the design of your AI systems, creating protocols or checklists for your AI systems, assisting in the drafting and collating of the required information
- Assist with other legal issues relating to AI and/or the draft Regulation e.g. assisting with AI explainability, advising on AI-related contractual issues and advising on data-related issues (including with data protection impact assessments).

Simmons + Wavelength

Simmons has a dedicated AI Group comprising lawyers across practice areas who can help you to navigate and manage AI-related legal, ethical and regulatory risks.

In 2019, we acquired Wavelength – the world's first regulated legal engineering business. Simmons Wavelength's team comprises technology experts and data scientists, with a deep experience of AI and data science.

Together, we can help you with legal and technical issues relating to AI. Please get in touch.

Minesh Tanna
AI Lead
Solicitor-Advocate
T +44 20 7825 4259
E minesh.tanna@simmons-simmons.com

simmons-simmons.com.