QUBIT PRIVACY BRIEFINGS

Qubit Privacy

BRIEFING 3 - APRIL 2021

THE REGULATION ON A EUROPEAN APPROACH FOR ARTIFICIAL INTELLIGENCE

On 21 April 2021, the EU Commission officially released the draft proposal for the Regulation of Artificial Intelligence (AIRd). The proposal sets out a comprehensive new legal framework for AI that aims at addressing a broad variety of challenges frequently associated with these technologies.

KEY FINDINGS

- *The AI Regulation draft radically changes the landscape of a barely regulated area and it imposes stringent obligations to multiple actors in the AI supply chain.*
- *The extra-territorial scope of this regulation means that both providers and users of High-Risk Artificial Intelligence Systems (HRAIS) may be required to comply with it even where they are established outside of the EU.*
- *This regulation may also apply to AI systems already placed in the market or put into service*
- *Infringing certain provisions of the regulation may lead to fines of up to €30M or 6% of annual global turnover*
- *Implications for HRAIS providers*
  - *Developers of HRAIS will need to fully take into account the regulation if enacted*
  - *They have obligations before placing HRAIS on the market (e.g. registering the system) and after the system is operating (e.g. post-market monitoring system)*
  - *If they are established outside the EU, they must appoint a representative in the EU.*
- *For HRAIS users*
  - *Organisations that procure and make use of HRAIS are also under heavy scrutiny*
  - *They must monitor the operation of the system for evident anomalies of the HRAIS*
  - *Foreign users of HRAIS are bounded by this regulation if the systems affect individuals in the EU*
- *For importers and distributors of HRAIS*
  - *While their responsibilities are less burdensome, they must be aware of the regulation and must place on the market only HRAIS that comply with its provisions*

APPLICATION

The AIRd establishes rules for the placing on the market, putting into service and use of high-risk AI systems (HRAIS) in the EU.

From a data protection perspective, the most important HRAIS **use cases** are listed in Annex III and they include systems intended to be used for:

- Remote biometric identification (RBI) of persons in publicly accessible areas
- Determining access or assigning persons to educational and vocations training institutions or assessing students
- Recruitment, making decisions on promotion and termination of work-related contracts, and monitoring work performance
- Evaluation of the creditworthiness of persons
- Evaluation of the eligibility for public assistance benefits and services

https://qubitprivacy.com
federico@qubitprivacy.com

- Making individual risk assessments to use as evidence in law enforcement contexts
- Predicting the occurrence of crimes or events of social unrest
- Processing and examination of asylum and visa applications
- Assisting judges at courts

Importantly, the AIRd has **extraterritorial application**, since it will apply to providers that place on the market or put into service HRAIS in the EU, regardless of whether they are established in the EU or not. Also, to foreign providers and users of HRAIS if the output of the system is used in the EU (art. 2(1)(a) and (c) AIRd).
Additionally, it applies to functioning HRAIS but only if they are subject to significant changes in their design or intended purpose (art. 83(2)AIRd)

FORBIDDEN AI PRACTICES

The AIRd in art. 5 sets out a list of AI prohibited practices, which include AI systems designed or used for:

- Manipulation of human behaviour, opinions or decisions
- Exploiting information about a person or group to target their vulnerabilities
- General-purpose scoring of individuals, where the scoring leads to a systematic detrimental treatment of certain persons or groups in social contexts:
  - not related to the contexts in which the data was originally obtained; or
  - that is disproportionate to the gravity of their social behaviour
- Indiscriminate surveillance (real-time RBI systems) without differentiation. Real-time RBI must be authorised by an independent authority (judicial or administrative) (art. 5(3) AIRd)

Failing to comply with this provision is subject to an administrative fine of up to €30M or 6% of the total worldwide annual turnover (art. 71(3)(a) AIRd)

DATA GOVERNANCE AND HRAIS PERFORMANCE

HRAIS must be trained and tested with high-quality data sets, which must be relevant, representative, free of errors, complete, and statistically adequate. Data sets must consider the features or elements that are particular to a specific geographical, behavioural or functional setting where the HRAIS is planned to be used. High-quality data sets must ensure that the HRAIS performs as intended and does not incorporate any biases or produces unintended adverse outcomes (art. 10 AIRd).
Failing to comply with this provision is subject to an administrative fine of up to €30M or 6% of the total worldwide annual turnover (art. 71(3)(a) AIRd)
Where employed to detect and correct biases, the processing of special categories of data is deemed a reason of substantial public interest (art. 9(2)(g) GDPR)

According to art. 15 AIRd, HRAIS must perform consistently and ensure high levels of:

- Accuracy
- Robustness
- Cybersecurity

TRANSPARENCY OBLIGATIONS

Individuals should be able to understand the HRAIS they are interacting with and control how the system produces its outputs (art. 13 AIRd)

QUBIT PRIVACY BRIEFINGS

BRIEFING 3 - APRIL 2021

Qubit Privacy

HRAIS must be accompanied by the information about:

- The provider
- Its capabilities and limitations, including intended purpose, level of accuracy, robustness and security and factors that may have an impact on these features
- General logic of the system and weighted accorded to different parameters
- Technical and organisational human oversight measures
- Expected lifetime

There are special transparency obligations in art. 52 AIRd. According to this provision, individuals must be informed that:

• They are interacting with an AI system

• Their personal data is being processed by an emotion recognition system or a categorisation system

• Audio-visual content has been artificially created or modified if the HRAIS generates images, audio or video that resembles existing persons, objects or events and falsely appear to be authentic.

OBLIGATIONS OF PROVIDERS

Providers are those who develop the AI system, or has it developed, or places it on the market/puts into service under its own name/trademark or for its own use, whether for payment or free (art. 3(2) AIRd)

Providers must (art. 16 AIRd):

- Ensure the HRAIS comply with the AIR
- Put in place quality management systems (art. 17 AIRd)
- Draw-up Annex IV technical documentation
- Undergo conformity assessments (art. 43 AIRd) and issue a EU (self)declaration of conformity (Art. 48 AIRd) and affix the CE marking of conformity (Art. 49 AIRd)
- Keep records of the logs generated
- Ensure that the HRAIS can be effectively overseen by humans when the system is in use (art. 14 AIRd)
- Register the HRAIS in the EU database (art. 51 and 60 AIRd)
- Take immediate corrective action where has reasons to believe that the HRAIS is not in conformity with AIR
- Inform national authorities about any risks
- Appoint a representative if they are established outside the EU (art. 25(1) AIRd)
- Establish a post-market monitoring system, proportionate to the nature and the risks of the HRAIS (art. 61 AIRd)
- Report to the authorities any serious incident or any malfunctioning of the HRAIS (art. 62 AIRd)

OBLIGATIONS OF USERS

Users are those who use an AI system under their authority, except where it is used for non-professional purposes (art. 3(4) AIRd)

Users must:

- Use the HRAIS in accordance with the instructions of the provider
- Monitor the operation of the system and if they become aware that the system presents a risk or malfunction they must interrupt the use of it and inform the provider
- Keep the logs automatically generated
- Use the information provided by the provider to comply with their obligation to carry out a DPIA under art. 35 GDPR (Art. 29 AIRd).

https://qubitprivacy.com
federico@qubitprivacy.com

QUBIT PRIVACY BRIEFINGS

BRIEFING 3 - APRIL 2021

Qubit Privacy

OBLIGATIONS OF IMPORTERS AND DISTRIBUTORS

Both importers and distributors must place on the market only HRAIS that comply with the AIR. In particular, they must verify that the HRAIS bears the required conformity marking and they are accompanied by the required documentation.
Importantly, where they consider that the HRAIS is not in conformity with AIR, they must not place it or make it available on the market and inform the provider (art. 26 and 27 AIRd).

CONFORMITY ASSESSMENT

Providers must perform a conformity assessment of the HRAIS to demonstrate compliance with the relevant provisions of the AIR (art. 43 AIRd)
The following provisions must be observed:

- Providers must draw up the technical documentation of the HRAIS and carry out a conformity assessment by themselves (self-evaluation). If they consider their HRAIS is compliant with AIR they must declare the conformity and issue an EU declaration of conformity (art. 43(2) AIRd).
- In the case of HRAIS intended to be used for RBI of persons in publicly accessible areas, providers may carry out the conformity assessment by themselves if there are applicable harmonised standards or EC common specifications (arts 40-41 AIRd). Otherwise, they must follow a special procedure (art. 43(1) AIRd)
- Where the HRAIS suffers a substantial modification, a new conformity assessment must be carried out. For the purposes of this evaluation, changes in adaptative (machine learning) HRAIS that have not been pre-determined and are not part of the technical documentation must be considered a substantial modification (art. 43(4) ARId)

Providers must issue the EU declaration of conformity, where they state that the HRAIS meets the AIR requirements. The provider assumes the responsibility for compliance with the AIR and must continuously update it as appropriate (art. 48 AIRd)

GOVERNANCE

It established the European Artificial Intelligence Board (EAIB) to contribute to uniform practices of Member States and to issue opinions and recommendations (art. 58 AIRd)
Member states must designate national competent authorities to ensure the application and implementation of the AIR (art. 59 AIRd)

ENFORCEMENT

Market surveillance authorities (MSA) will have full access to the training, validation and testing datasets used by the provider, including through APIs or other appropriate technical means and tools enabling remote access and, upon reasoned request, they will have access to the source code (art. 64(1)-(2) AIRd)
Where a MSA considers that a AI system presents a risk, it will carry out an evaluation and if the system does not comply with the AIR will require the relevant operator to take measures, including withdrawing the system (art. 65(2) AIRd). The MSA will inform the Commission if the non-compliance affects more than one member state.

https://qubitprivacy.com
federico@qubitprivacy.com

QUBIT PRIVACY BRIEFINGS

Qubit Privacy

BRIEFING 3 - APRIL 2021

PENALTIES FOR NON-COMPLIANCE

The AIRd defer the details concerning the rules on penalties applicable to infringements to EU Member states, provided that they are effective, proportionate and dissuasive (art. 71AIRd)
However, it requires certain infringements to be punished with administrative fines according to the following scale:

- Up to €30.000.000 or up to 6% of the total worldwide annual turnover:
  - For the development, placing on the market or putting into service of prohibited HRAIS (art. 5 AIRd)
  - Non-compliance with the obligations concerning the datasets and data governance (Art. 10AIRd)
- Up to €20.000.000 or up to 4% of the total worldwide annual turnover for non-compliance with any other requirement or obligation under AIR
- Up to €10.000.000 or up to 2% of the total worldwide annual turnover for the supply of incorrect, incomplete or misleading information to the notified bodies (they assess the conformity of certain HRAIS, art. 33 AIRd) and national authorities in reply to a request

This briefing was prepared by Federico Marengo for QUBIT PRIVACY

QUBIT PRIVACY is a consultancy firm established in Italy that provides tailor-made services for individuals and companies to comply with the requirements established in the General Data Protection Regulation.
Federico Marengo is a lawyer, master in public administration (University of Buenos Aires), LLM (University of Manchester), and PhD candidate (Università Bocconi, Milano).
He currently provides data protection consultancy services for Qubit Privacy and also works as of counsel for consultancy firms.
He is the author of "Data Protection Law in Charts. A Visual Guide to the General Data Protection Regulation", e-book released in 2021, and authored several publications on international data transfers and international trade law.
As a PhD researcher, his research deals with the potential and challenges of the General Data Protection Regulation to protect data subjects against the adverse effects of Artificial Intelligence.
He is also teaching assistant at Università Bocconi.

DISCLAIMER
This client briefing is prepared for information purposes only. The information contained therein should not be relied on as legal advice and should, therefore, not be regarded as a substitute for detailed legal advice in the individual case. The advice of a qualified lawyer should always be sought in such cases. In the publishing of this Briefing, we do not accept any liability in individual cases