Qubit Privacy

Qubit Privacy Briefings

Briefing #1 / April 2021

THE REGULATION ON A EUROPEAN APPROACH FOR ARTIFICIAL INTELLIGENCE

KEY FINDINGS AND RECOMMENDATIONS

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 HRAIS may be required to comply with it even where they are established outside of the EU.

Infringing certain provisions of the regulation may lead to GDPR-level fines of up to €20M or 4% of annual global turnover

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 may 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

On 14 April 2021, the EU Commission’s draft proposal for the regulation of artificial intelligence (AI) were leaked. The proposal, which are due to be formally announced on 21 April, sets out a comprehensive new legal framework for AI that aims at addressing a broad variety of challenges frequently associated with these technologies.

Acknowledging that AI systems can not only bring social and economic benefits but also produce high risks and harms to the interests and rights of individuals in the EU, the EU Commission drafted a Regulation for AI systems (AIRd). The idea is to foster the development of this new technology while meeting a high level of protection and putting people at the centre.

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. AIRd includes a long list of systems that can be classified as HRAIS (art. 5 AIRd), but from a data protection perspective, the most important use cases are listed in Annex II and they include systems intended to be used for:

- Remote biometric identification of persons in publicly accessible areas
- Determining access or assigning persons to educational and vocations training institutions
- 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
- 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 systems affect individuals in the EU (art. 2(2) AIRd).

Data sets 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. 8 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. 12 AIRd, HRAIS must perform consistently and ensure high levels of:

- Accuracy
- Robustness
- Security

Transparency obligations

Users of HRAIS should be able to **understand** and control how the system produces its outputs (art. 10 AIRd)

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

HRAIS's output must be verified and traced back throughout the system's lifecycle (art. 9 AIRd)

There are special transparency obligations in art. 41 AIRd. According to this provision, individuals must be informed that:

- They are interacting with a HRAIS
- 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 importers, distributors and users

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** (art. 15 and 16 AIRd).

Users must use the HRAIS in accordance with the instructions of the provider. They must **monitor the operation of the system for evident anomalies**. In addition, they must use the information on accuracy, robustness and security to comply with their obligation to carry out a DPIA under art. 35 GDPR (Art. 18 AIRd).

Forbidden AI practices

The AIRd in art. 4 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
- **Indiscriminate surveillance** without differentiation
- **General purpose scoring of individuals**, where the scoring leads to a systematic detrimental treatment of certain persons or groups in social contexts: a) not related to the contexts in which the data was originally obtained; or b) that is disproportionate to the gravity of their social behaviour

Failing to comply with this provision is subject to an administrative **fine of up to €20M or 4% of the total worldwide annual turnover** (art. 63(2)(a) AIRd)

Obligations of providers

Providers are those who develop the AI system 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(1)(2) AIRd)

Providers must:

- Ensure the HRAIS **comply with the AIR**
- Put in place **quality management systems**
- Draw-up Annex IV **technical documentation**
- Undergo **conformity assessments** (art. 45 AIRd) and issue a EU (self)declaration of conformity (Art. 38 AIRd) and affix the CE marking of conformity (Art. 39 AIRd)
- **Keep records** of the logs generated
- **Register the HRAIS** in the EU database (art. 40 and 52 AIRd)
- Take immediate **corrective action** where has reasons to believe that the HRAIS is not in conformity with AIR, informing downstream actors.
- Inform national authorities about any risks
- Optional: Providers established outside the EU may appoint a representative
- Establish a **post-market monitoring system**, proportionate to the nature and the risks of the HRAIS (art. 54 AIRd)
- Report to the authorities any serious incident or any malfunctioning of the HRAIS (art. 55 AIRd)

Conformity assessment

Providers must perform a conformity assessment of the HRAIS to **demonstrate compliance** with the relevant provisions of the AIR, in particular and where applicable arts. 5-40 (art. 35 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. 35(4) AIRd).
- In the case of HRAIS intended to be used for the remote biometric identification of persons in publicly accessible areas, providers may carry out the conformity assessment by themselves if there are applicable harmonised standards. Otherwise, they must follow a special procedure (art. 35(5) 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 which have not been pre-determined and are not part of the technical documentation must be considered a substantial modification (art. 35(6) ARId)

In issuing the EU declaration of conformity, the provider assumes the responsibility for compliance with the AIR and must continuously update it as appropriate (art. 38 AIRd)

Remote biometric identification systems in publicly accessible areas

In addition to the general regulations, the use of remote biometric identification systems in publicly accessible areas (facial recognition technologies) must be authorised only if:

- Authorised by law
- Aims at preventing, detecting or investigating serious crime
- Limited to a temporal and a geographical scope

The authorising decision must be based on a **DPIA** carried out in accordance with the requirements laid down in art. 35(7) GDPR including:

- Evidence of the accuracy for the use of the system for the given purpose, including potential impacts on different groups
- Assessment of the safeguards for the protection of different groups
- Consistency with EU values

Penalties for non-compliance

The AIRd defer the rules on penalties applicable to infringements to EU Member states, provided that they are effective, proportionate and dissuasive.
However, it proposes punishing with administrative **fines up to €20.000.000 or up to 4% of the total worldwide annual turnover** of the preceding financial year for:

- The development, placing on the market or putting into service of prohibited HRAIS (art. 4 AIRd)
- The supply of incorrect, incomplete or false information to notified bodies
- Non-compliance with the obligation to cooperate with the national authorities in the performance of their tasks

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.

Qubit Privacy

Find more

https://qubitprivacy.com/

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 at Data Business Services.
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