VAN BAEL & BELLIS

28 March 2024

Fundamental Rights Impact Assessment in the EU Artificial Intelligence Act

On 13 March 2024, the European Parliament (***EP***) adopted the European Union (***EU***) Artificial Intelligence Act (***AI Act***), one of the first and possibly the most comprehensive regulation of AI in the world.

The AI Act aims to ensure a "*high level of protection of health, safety,* [and] *fundamental rights* [...] *against harmful effects of artificial intelligence systems*" and at the same time "*support innovation*". In pursuit of these goals, the AI Act is built on a risk-based approach: AI systems that pose little to no risk – and there are a lot of these – are subject to minimal requirements. By contrast, AI systems that pose a high risk are subject to a number of requirements addressing the risks associated with such AI systems.

These requirements include several tried and tested measures of risk regulation, ranging from accountability measures such as the requirement to establish a risk management system (used, *inter alia*, in manufacturing and distributing pharmaceutical products) to third-party conformity assessment (leveraging the EU "CE" mark which indicates that a product conforms to certain EU health, safety and environmental protection rules).

In addition, the AI Act introduces a new risk assessment instrument in the form of the Fundamental Rights Impact Assessment (***FRIA***). Not originally foreseen in the 2021 European Commission proposal, the EP added this requirement to "*efficiently ensure that fundamental rights are protected*".

(*At time of writing the AI Act awaits publication in the Official Journal. Our analysis is based on the adopted text published by the EP.*)

What is FRIA?

An FRIA is a type of "impact assessment", i.e., a technical-legal process that helps organisations guide their decisions by providing more clarity on potential negative impacts of their envisaged AI systems in order to protect fundamental rights and to comply with the law. This process ensures accountability, demonstrating that the organisation analysed with due diligence what can go wrong with their project. Other types of impact assessments are used in various areas, including the protection of the natural environment (environmental impact assessment; ***EIA***) or the data protection impact assessment (***DPIA***) for high-risk processing of personal data under the General Data Protection Regulation (***GDPR***).

Deployers that must conduct an FRIA, should – possibly in collaboration with stakeholders – identify, analyse and assess potential future impacts on *all* fundamental rights resulting from AI system usage, and propose actionable steps to mitigate any negative outcomes. The possible scope of an FRIA is broad and covers fundamental rights listed in the Charter of Fundamental Rights of the EU (***CFR***), and possibly other fundamental rights as well. Fundamental rights in the CFR include the right to human dignity, non-discrimination, data protection, the right to education, consumer protection and workers' rights.

For which AI systems will an FRIA be required?

At first sight, it may seem that the obligation to carry out an FRIA does not affect many AI systems. Indeed, the text of the AI Act indicates that an FRIA is "only" required in the following cases:

a. "*deployers that are bodies governed by public law*";

b. deployers that "*are private entities providing public services*"; and

c. deployers of high-risk AI systems for the evaluation of the creditworthiness of natural persons, to establish their credit score or for assessing risks and pricings in the context of life and health insurance.

In addition, high-level AI systems intended to be used as "*safety components*" in critical infrastructure – e.g., in the supply of water, gas, heating and electricity – are exempt from conducting an FRIA.

The scope of this obligation therefore appears to be narrow – and much narrower than the initial EP proposal (June 2023, amendment 413), which intended to cover *all* deployers of *all* high-risk AI systems, with few exceptions.

However, a closer look at the second criterion – "*private entities providing public services*" – reveals that more deployers will be affected by the FRIA requirement than would appear at first sight. In particular, Recital 93 of the AI Act explains that the categories of services "*of* [a] *public nature*" that may be offered by private entities are quite broad, e.g., including services "*in the area of education, healthcare, social services, housing,* [and] *administration of justice*". This criterion is likely to be further explained in future guidance documents. Yet, the recital suggests that any private entity that deploys AI services for "*public services*" in these areas will need to conduct an FRIA as long as the AI system qualifies as high-risk. In many EU Member States, this means that, for example, providers that offer AI systems that fall in the "high risk" category to hospitals will need to conduct an FRIA. We expect that public services will include this requirement in procurement conditions when they procure AI systems.

The AI Act differentiates between various actors within the supply chain of AI systems and outlines distinct requirements for each of them:

Deployers of AI systems are entities that are "*using an AI system under* [their] *authority*", unless for a "*personal non-professional activity*"; and

Providers of AI systems are those who develop an AI system and place it on the market.

When will the obligation to conduct an FRIA apply?

The obligation to carry out an FRIA will be applicable 24 months after entry into force of the AI Act, which will occur 20 days after its publication in the Official Journal. As a general rule, affected deployers must conduct an FRIA prior to the first use of any high-risk AI system and regularly update their FRIA.

Considering the nature of the exercise, which identifies risks and proposes mitigating measures that may affect the design and use of the AI systems, it is strongly recommended that the FRIA exercise is integrated into the developmental phase of the AI system. For that reason, organisations should already consider conducting an FRIA for AI systems under development and that may fall within the scope of the requirement when it will apply within the aforementioned 24 months' time.

What does an FRIA look like?

The AI Act stipulates the minimum mandatory content of an FRIA including the following steps:

a. *Description*: of the high-risk AI system, its intended purpose(s), timeframes and affected people;

b. *Assessment*: of the specific risks of harm likely to impact the affected people; and

c. *Risk treatment*: measures to address such risks, supplemented by a "*description of the implementation of human oversight measures*".

Furthermore, it is recommended that relevant stakeholders be consulted, including the representatives of groups of persons likely to be affected by the AI system, as well as independent experts, and possibly civil society organisations.

Once the FRIA has been performed, the deployer must notify the competent market surveillance authority – which will be designated in each EU Member State – of the results of the assessment (unless the deployer is exempted from the notification requirement).

To aid affected deployers, the newly established EU AI Office is obliged to develop a "*template for a questionnaire, including through an automated tool*" for conducting an FRIA. However, the timeline for its introduction, as well as its quality and completeness, remain unknown at the current time.

How to combine FRIA with related requirements?

FRIA may overlap with related obligations under the AI Act, e.g., conformity assessment, or with the DPIA requirement under the GDPR. Indeed, many high-risk AI systems will also process personal data and therefore have to comply with GDPR. The FRIA and the DPIA processes are analogous, but differ substantially in their scope: while DPIA focuses on rights and freedoms of data subjects affected by the processing of their personal data, FRIA also concerns risks associated with non-personal data.

The AI Act addresses this possible overlap in its Article 27(4) which notes that if some obligations are already met through a DPIA, the FRIA shall "*complement*" that DPIA. Similarly, other prior impact assessments that are relevant can inform an FRIA process. In practice, this will mean that DPIA and FRIA are often conducted together, and may even result in a single integrated report. The possibility to combine an FRIA with a DPIA as well as the promise of a standardised template for an FRIA constitute one of the measures to ease the burden of having to comply with the AI Act and GDPR.

Key takeaways

The AI Act's FRIA is the world's first mandatory impact assessment of AI systems on fundamental rights. While it poses a significant regulatory challenge for deployers of high-risk AI systems, it also provides them with an opportunity to better understand their own AI systems and anticipate their possible negative impacts, and – importantly – document that the organisation acted in an accountable manner when developing its high-risk AI systems. While further clarification as to certain aspects of the FRIA requirement are still necessary, organisations using AI systems that fall within the high-risk category should carefully assess their obligations.

Thibaut D'hulst
Dariusz Kloza
Alexandre Lejeune

Lawyer to contact

Thibaut D'Hulst
Counsel
tdhulst@vbb.com

Brussels office
Glaverbel Building
Chaussée de La Hulpe 166
B-1170 Brussels
Belgium

Phone:+32 (0)2 647 73 50

Geneva office
26, Bd des Philosophes
CH-1205 Geneva
Switzerland

Phone:+41 (0)22 320 90 20

London office
Holborn Gate
330 High Holborn
London
WC1V 7QH
United Kingdom

Phone: +44 (0)20 7406 1471

VAN BAEL & BELLIS

www.vbb.com