Bonn, Bucharest, Dublin, Lisbon, Madrid, Milan, Paris, The Hague, Vienna, Warsaw

Fundamental Rights Impact Assessments: What are they? How do they work?

CEDPO AI and Data Working Group
Micro-Insights Series
January 2025

Authors:
Thomas Ajoodha
Jared Browne

Contact information:
https://cedpo.eu
info@cedpo.eu

About the Micro-Insights Series

The Micro-Insights Series is a publishing initiative by the CEDPO AI and Data Working Group. It will provide digestible, definitive, short-form papers on key areas of interest at the intersection between data and artificial intelligence. With a practical focus, keeping one eye on explaining complex topics and the other on implementation, it will outline the significance of key areas and advise practitioners on impact, and next steps. With the EU Artificial Intelligence Act (the 'AI Act') coming into law in 2024, the scene is now set for all practitioners, and it is possible to discuss the regulation of data and AI with much greater clarity.

The Micro-Insights Series will follow the evolution of AI and data over the coming years, and as the clock winds down on the crucial implementation period for the AI Act, and as AI technologies evolve in ever-more novel and unexpected ways, the Series will respond with up-to-date, authoritative guidance on the core areas of concern.

Amongst others, the series will include papers on:

- Regulation of General-Purpose Artificial Intelligence under the AI Act
- Explaining the AI Pact.
- Educating practitioners on how to conduct Fundamental Rights Impact Assessments under the AI Act.
- Outlining the role that data protection regulators will have in AI regulation.
- Examining whether or not the data protection officer is the right person to be the AI officer.
- The lawful basis for using training data in machine learning.
- Readiness toolkit for the AI Act.

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Table of Contents

1. Introduction: What is a fundamental rights impact assessment?

Fundamental rights impact assessments (FRIAs) are a requirement under Article 27 of the EU Artificial Intelligence Act ('the AI Act', 'the Act'), and must be conducted in certain circumstances for high-risk AI systems.

At its simplest, an FRIA is an assessment of the potential impact of an AI system on the rights of any individual that might be affected by the operation of that system. An FRIA is a risk assessment, so it does not focus on risk elimination, but rather on risk management. The point of an FRIA is to identify risks to affected individuals, assess their likelihood and severity, propose mitigants to control those risks, and then set out a comprehensive plan as to how those risks will be properly managed.

Although risk assessments are not new, AI risk assessments, in the context of fundamental rights, will be a new phenomenon for many data protection and privacy professionals. Although data protection and privacy professionals will be familiar with assessing risks to personal data, and sometimes even in the context of AI systems, what is novel about FRIAs is the need to specifically understand risks that are uniquely AI-based, and which may lead to direct or indirect adverse effects.

Broadly, AI has a number of unique risks such as opacity, complexity, autonomy, bias, and discrimination, from which many sub-risks flow. To give a concrete example, autonomous, algorithmic systems that make significant independent decisions about human beings lives, such as AI-based loan-decision engines that decide on creditworthiness, would most likely require a FRIA.

As the name suggests, not all rights are in scope, but only fundamental ones. In the context of EU law, this should be understood to refer primarily to AI's potential negative impact on the numerous rights enshrined in The Charter of Fundamental Rights of the European Union (the **'EU Charter'**).

The EU's AI Office is committed under Article 27 (5) of the Act to develop a template for a FRIA questionnaire, as well as an automated tool to facilitate compliance.

The below table outlines the rights protected in The EU Charter, categorised by domain:

Domain	Rights Protected
Dignity	Human dignity (1), Right to life (2), Right to the integrity of the person (3), Prohibition of torture and inhuman or degrading treatment or punishment (4), Prohibition of slavery and forced labour (5)
Freedoms	Right to liberty and security (6), Respect for private and family life (7), Protection of personal data (8), Right to marry and right to found a family (9), Freedom of thought, conscience and religion (10), Freedom of expression and information (11), Freedom of assembly and of association (12), Freedom of the arts and sciences (13), Right to education (14), Freedom to choose an occupation and right to engage in work (15), Freedom to conduct a business (16), Right to property (17), Right to asylum (18), Protection in the event of removal, expulsion or extradition (19)
Equality	Equality before the law (20), Non-discrimination (21), Cultural, religious and linguistic diversity (22), Equality between women and men (23), The rights of the child (24), The rights of the elderly (25), Integration of persons with disabilities (26)
Solidarity	Workers' right to information and consultation within the undertaking (27), Right of collective bargaining and action (28), Right of access to placement services (29), Protection in the event of unjustified dismissal (30), Fair and just working conditions (31), Prohibition of child labour and protection of young people at work (32), Family and professional life (33), Social security and social assistance (34), Health care (35), Access to services of general economic interest (36), Environmental protection (37), Consumer protection (38)
Citizens' Rights	Right to vote and to stand as a candidate at elections to the European Parliament (39), Right to vote and to stand as a candidate at municipal elections (40), Right to good administration (41), Right of access to documents (42), European Ombudsman (43), Right to petition (44), Freedom of movement and of residence (45), Diplomatic and consular protection (46)
Justice	Right to an effective remedy and to a fair trial (47), Presumption of innocence and right of defence (48), Principles of legality and proportionality of criminal offences and penalties (49), Right not to be tried or punished twice in criminal proceedings for the same criminal offence (50)

2. Who needs to complete fundamental rights impact assessments?

FRIAs must be completed by deployers of high-risk AI systems. Under the hierarchy of responsible parties designated by the Act, deployers have significantly less responsibility than providers, given that they have not developed the high-risk system. However, they do put it into use for their own specific use case, so this brings with it obligations to safeguard the fundamental rights of ultimate end-users.

However, not all deployers are obliged to carry out FRIAs. Only deployers that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III, are under this obligation.

3. When should a fundamental rights impact assessment be conducted?

FRIAs must be completed by deployers of high-risk AI systems *before* the deployment of those systems. Although providers of the relevant high-risk system will have already conducted detailed risk assessments before the system has reached the hands of the deployer, the logic of a deployer needing to also carry out a risk assessment is that many risks only materialise downstream in specific use cases, - hence the need to capture these kinds of potential harms at the deployment phase of the life cycle.

Specifically, the high-risk systems in scope are those outlined in Article 6(2) of the Act, with the exception of high-risk AI systems intended to be used in the area listed in point 2 of Annex III, more details of which will be explained at Section 4, below.

4. What are the specific requirements of fundamental rights impact assessments?

Article 27 of the AI Act outlines a comprehensive framework for conducting Fundamental Rights Impact Assessments (FRIA) for high-risk AI systems. This framework is designed to ensure that AI deployments do not infringe upon fundamental rights. The article mandates that before deploying such systems, deployers must undertake a meticulous assessment covering several key dimensions:

- **Deployment context and intended purpose:** Deployers must provide a detailed description of the processes in which the high-risk AI system will be used. This

includes clearly defining the intended purpose of the AI system within the specific operational context. Understanding the deployment context is crucial for identifying potential risks associated with the system's use.

- **Operational duration and usage frequency:** This requires a description of the period and frequency of the AI system's intended use. This helps in evaluating the system's long-term impact on fundamental rights and ensures that the assessment is not limited to a short-term perspective.

- **Affected natural persons and groups:** Deployers must identify the categories of individuals and groups likely to be affected by the AI system. This involves analysing the specific context in which the system will operate and recognising those who might be impacted by its deployment.

- **Specific risks of harm:** An essential part of the assessment is identifying the specific risks of harm that the AI system might pose to the identified individuals or groups. This includes evaluating the potential adverse effects and considering the information provided by the AI system's provider.

- **Human oversight measures:** The implementation of human oversight measures is crucial for mitigating risks associated with AI systems. Deployers must describe the oversight mechanisms that will be put in place, following the instructions for use, to ensure that the system operates within safe and ethical boundaries.

- **Risk mitigation measures:** Deployers are also required to outline the measures to be taken if the identified risks materialise. This includes internal governance arrangements and complaint mechanisms, ensuring that there are robust procedures to address any issues that arise during the system's operation.

This structured approach ensures that FRIAs are thorough and cover all necessary aspects to protect fundamental rights. By detailing each requirement, deployers can comprehensively assess and mitigate potential risks, thereby preventing rights violations before they occur.

5. How does a fundamental rights impact assessment interact with a data protection impact assessment and other regulatory frameworks?

The advent of the digital age has ushered in an array of transformative technologies, among which AI stands out for its profound implications on society. With this rapid technological advancement, regulatory frameworks have evolved to address the myriad of impacts on fundamental rights. A notable trend in digital regulation is the increasing prevalence of impact

assessments designed to pre-emptively gauge the effects of technology deployment. For instance, the General Data Protection Regulation (GDPR) mandates a Data Protection Impact Assessment (DPIA) for processing operations likely to result in high risks to individuals' rights and freedoms. Similarly, the Digital Services Act (DSA) introduces systemic risk assessments for providers of very large online platforms and of very large online search engines; while these assessments focus primarily on addressing broad societal and systemic risks beyond fundamental rights alone, they nonetheless emphasise the protection of these core rights as a critical component. The AI Act aligns with this regulatory trajectory, mandating FRIAs for high-risk AI systems, thereby embedding a thorough consideration of fundamental rights into the fabric of AI governance.

The interplay between the FRIA under the AI Act and other impact assessments, notably the DPIA under the GDPR, offers a multifaceted view of regulatory compliance. While the DPIA focuses on data protection and privacy risks, the FRIA encompasses a broader range of fundamental rights concerns. This complementary relationship ensures a holistic approach to safeguarding rights and freedoms in the digital sphere. For instance, a DPIA conducted under the GDPR may already cover certain aspects required for a FRIA, such as data privacy and security measures. In such cases, the FRIA complements the DPIA by addressing additional fundamental rights issues, ensuring comprehensive coverage without unnecessary duplication. In fact, Ar.27 (4) of the Act specifically allows for this, saying 'If any of the obligations laid down in this Article is already met through the data protection impact assessment … the fundamental rights impact assessment … shall complement that data protection impact assessment.'

Moreover, the systemic risk assessments mandated by the DSA for large online platforms align with the objectives of the FRIA. Both frameworks aim to identify and mitigate risks to fundamental rights, fostering a safe and ethical digital environment. By integrating these assessments, deployers can achieve a cohesive strategy for protecting fundamental rights across various technological domains.

6. Conclusion: The role of fundamental rights impact assessments in responsible AI

Owing to their knowledge and experience of assessing impact to fundamental rights there is a compelling argument for data protection officers having a significant role in conducting or overseeing the completion of the fundamental rights impact assessment. However, although data protection officers do have a native knowledge of such assessments it should be remembered that their experience with data protection impact assessments will not have exposed them to the full range of rights that AI systems are likely to impact. In practical terms, this means that data protection officers will have to gain an understanding of technology impacts to, for example, the right to freedom of expression, the right to work, the right to a fair trial, the right to asylum and considerably more.