

# Fundamental Rights Impact Assessment

A Practical Guide – September 2024

## Table of Contents

<b>1. Introduction</b> .....	<b>3</b>
<b>2. AI under the AI Act</b> .....	<b>4</b>
<i>Question 1. Is the system in question an AI system?</i> .....	4
<b>3. What AI systems need to perform a FRIA?</b> .....	<b>5</b>
<i>Question 2. Does your system fall under any of the categories listed below?</i> .....	6
<i>Question 3. Is your AI system subject to any of the exceptions listed below?</i> .....	7
<b>4. Who is responsible for conducting a FRIA?</b> .....	<b>8</b>
<b>5. When should a FRIA be performed?</b> .....	<b>9</b>
<b>6. What should a FRIA include?</b> .....	<b>9</b>
<b>7. Who should you notify?</b> .....	<b>10</b>
<b>8. What about the DPIA?</b> .....	<b>11</b>
<b>9. When do you have to be compliant?</b> .....	<b>11</b>
<b>10. How can WLC support you?</b> .....	<b>12</b>
<b>Annex I - List of Market Surveillance Authorities in Each EU Member State</b> .....	<b>13</b>

# 1. Introduction

The recently adopted Artificial Intelligence (AI) Act is a comprehensive legal framework aimed at fostering the development, deployment, and uptake of AI technologies within the European Union (EU).

A key aspect of the EU's approach is defining the trustworthiness of AI systems based on the acceptability of their risks.

To achieve this, the AI Act employs a clearly defined risk-based approach. Recital 26 states this approach 'should tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate.' In practice, this involves categorising AI systems based on the level of risk they pose to individuals and society. Depending on this categorisation, appropriate measures are implemented to ensure safety and compliance.

By establishing these harmonised rules and guidelines, the AI Act aims to balance the promotion of innovation with the need for safety and ethical considerations. This ensures that AI technologies benefit society while safeguarding public interests such as health, safety, and fundamental rights. Ultimately, the regulation positions the EU as a global leader in the ethical and secure use of AI technologies, fostering a human-centric approach to AI development and deployment.

Given the recent enactment of this legal framework and the growing interest in AI technologies, which are increasingly integrated into numerous industries and workplace operations, businesses must prioritise remaining ahead in ensuring compliance while effectively implementing AI practices.

To assist businesses in navigating this complex legal landscape, we have created this guide on how to conduct a Fundamental Rights Impact Assessment (FRIA), which is a central obligation for high-risk AI systems, evaluating how those systems might affect people's fundamental rights, such as privacy, freedom of expression, and non-discrimination. By reviewing this guide and following our recommendations, you will gain insights into:

- Whether the use of the AI system requires a FRIA,
- Who is responsible for conducting a FRIA,
- When a FRIA should be performed,
- What should be included in a FRIA,
- Whom you should notify,
- How a FRIA compares to other legal requirements under the GDPR, and
- When you should start being compliant.

## 2. AI under the AI Act

### Question 1. Is the system in question an AI system?

The AI Act defines an 'AI system' in Article 3(1) as 'a **machine-based system** that is designed to operate with **varying levels of autonomy** and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, **infers, from the input it receives, how to generate outputs** such as predictions, content, recommendations, or decisions that can **influence physical or virtual environments.**'

The AI Act introduces a **risk-based classification system**, as shown in [Table 1](#), to ensure that AI technologies are developed and deployed in a way that prioritises safety and fundamental rights. This system categorises AI systems into four different risk levels, each with corresponding regulatory requirements:

**Unacceptable Risk:** AI systems in this category pose such a significant threat to fundamental rights and public safety that they are banned from being used within the EU. The EU AI Act establishes a list of AI systems or AI use cases that are forbidden:

- (a) **Social scoring:** AI that rates individuals based on behaviour or characteristics, leading to disproportionate detrimental effects or effects unrelated with the original source of collection,
- (b) **Trait-based crime prediction:** AI predicting a person committing a crime based on personal traits,
- (c) **Biometric ID in public:** Real-time biometric identification in public spaces for law enforcement, with limited exceptions,
- (d) **Subliminal manipulation:** AI that alters behaviour without user awareness, potentially causing harm,
- (e) **Biometric categorisation:** Categorising people based on biometrics traits to infer sensitive attributes like ethnicity, religion or sexual orientation,
- (f) **Emotion recognition:** AI assessing emotions in workplaces or schools, allowed only for safety purposes,
- (g) **Facial image scraping:** Creating databases by scraping facial images from the web,
- (h) **Exploitation of vulnerabilities:** AI exploiting age, disability, social status or vulnerabilities to cause harm.

**High-risk AI systems:** These are AI technologies that, while presenting potential threats to individuals' safety or fundamental rights—especially in critical areas such as healthcare, education, or law enforcement—are not banned. Instead, they are subject to strict regulatory requirements to ensure they operate safely and ethically. This may include performing rigorous **conformity assessments** before deployment (such as FRIA), ensuring the system meets established standards.

**Limited risk AI systems:** These AI applications, like chatbots or AI-generated content, are subject to lighter regulations compared to high-risk AI systems and primarily have transparency obligations. Providers must inform users that they are interacting with AI, ensuring users are aware and can

make informed decisions. While the regulatory requirements are minimal, these systems still need to maintain ethical standards and avoid misleading users.

**Minimal risk AI systems:** These AI systems pose the least threat to users and society, and examples are AI in video games or spam filters. These systems have no mandatory regulatory requirements, but developers are encouraged to follow voluntary codes of conduct to ensure ethical use. The focus is on promoting transparency, fairness, and safety, even though the regulatory burden is minimal.

Deferring from the risk-based classification, it's important to note that the AI Act also addresses General Purpose AI (GPAI). GPAIs are not subject to FRIA requirements but must still meet other transparency obligations.

**Table 1: AI Systems Risk-Based Classification**

	RISK LEVEL	EXAMPLES	COMPLIANCE REQUIREMENTS
1	UNACCEPTABLE RISK	Behaviour manipulation systems, exploitative applications.	Prohibited from develop, use and market.
2	HIGH RISK	Healthcare diagnostics, credit scoring, employee monitoring, student assessing, law enforcement applications.	<ul style="list-style-type: none"> <li>• High-quality datasets to minimise risks and discriminatory outcomes,</li> <li>• High robustness standards,</li> <li>• Transparency,</li> <li>• Human oversight,</li> <li>• Detailed documentation.</li> <li>• Traceability of results,</li> <li>• Risk Management system,</li> <li>• Adequate deployer information.</li> </ul>
3	LIMITED RISK	Chatbots.	Transparency to ensure user awareness.
4	MINIMAL RISK	Spam filters, AI-enabled video games.	Permitted with no restrictions. Good practices like human oversight, non-discrimination or fairness are recommended to ensure ethical operation.

If your system falls under the classification provided above, please proceed to Question number 2.

### 3. What AI systems need to perform a FRIA?

Only some deployers of high-risk AI systems referred to in Article 6(2) of the AI Act and further specified in Annex III are required to conduct a FRIA. As mentioned above, these systems should only be placed on the EU market, put into service, or used if they meet specific mandatory requirements - one of which is the FRIA - ensuring that the deployment of high-risk AI systems does not infringe upon the fundamental rights protected by the EU.

## Question 2. Does your system fall under any of the categories listed below?

Below in [Table 2](#), is a clear list of the in-scope AI systems and related exceptions:

**Table 2. High-Risk AI Systems Subject to FRIA requirement\* \*\***

CATEGORY	INTENDED USE
<b>BIOMETRICS</b>	
(a) Remote biometric identification systems	Not including systems solely for biometric verification to confirm identity.
(b) Biometric categorisation	Used for assigning persons to specific categories based on their biometric data.
(c) Emotion recognition	Used to recognise emotions based on biometrics.
<b>EDUCATION AND VOCATIONAL TRAINING</b>	
(a) Access/admission assignment	Used to determine access or admission to educational and vocational training institutions.
(b) Evaluate learning outcomes	Used to evaluate and steer learning outcomes and processes.
(c) Assessing education level	Used to assess the appropriate level of education that an individual will receive or will be able to access.
(d) Monitoring/detecting prohibited behaviour	Used for monitoring and detecting prohibited behaviour during tests.
<b>EMPLOYMENT, WORKERS MANAGEMENT, AND ACCESS TO SELF-EMPLOYMENT</b>	
(a) Recruitment/selection	Used for recruitment, job advertisements, filtering applications, and evaluating candidates.
(b) Work-related decisions	Used to make decisions about terms, promotion, termination, task allocation, and performance monitoring.
<b>ACCESS TO AND ENJOYMENT OF ESSENTIAL PRIVATE AND PUBLIC SERVICES</b>	
(a) Public assistance evaluation	Used to evaluate eligibility for public assistance benefits and services.
(b) Creditworthiness evaluation	Used to evaluate creditworthiness and establish credit scores, except for detecting financial fraud.
(c) Risk assessment/pricing in insurance	Used for risk assessment and pricing in life and health insurance.
(d) Emergency services evaluation	Used to evaluate and classify emergency calls, dispatch services, and prioritise emergency responses.
<b>LAW ENFORCEMENT</b>	
(a) Risk assessment for crime victims	Used to assess the risk of a person becoming a victim of criminal offenses.
(b) Polygraphs or similar tools	Used to support law enforcement operations as polygraphs or similar tools.
(c) Evidence reliability evaluation	Used to evaluate the reliability of evidence in criminal investigations or prosecutions.
(d) Offending/re-offending risk assessment	Used to assess the risk of offending or re-offending, excluding profiling based solely on certain personal data.
(e) Profiling for crime detection	Used for profiling in the detection, investigation, or prosecution of criminal offenses.

MIGRATION, ASYLUM, AND BORDER CONTROL MANAGEMENT	
(a) Polygraphs or similar tools	Used as polygraphs or similar tools by public authorities.
(b) Risk assessment for entry	Used to assess security, irregular migration, or health risks posed by individuals entering a Member State.
(c) Application examination	Used to assist in examining applications for asylum, visa, or residence permits.
(d) Detection/identification of persons	Used to detect, recognise, or identify persons in migration, asylum, or border control, excluding travel document verification.
ADMINISTRATION OF JUSTICE AND DEMOCRATIC PROCESSES	
(a) Judicial assistance	Used to assist judicial authorities in researching, interpreting facts and law, and applying the law.
(b) Influencing elections	Used to influence election outcomes or voting behaviour, excluding tools not directly exposed to voters.

\*This list is subject to amendments by the European Commission as per Article 7 AI Act.

\*\*Annex III also includes AI systems used for managing and operating critical infrastructure. However, this category is intentionally excluded from the high-risk AI systems required to conduct a FRIA and is, therefore, not included in the above list.

**If your AI system falls under any of the categories listed in Table 2 above, please proceed to the Question number 3.**

### **Question 3. Is your AI system subject to any of the exceptions listed below?**

Even if your AI system is listed in the table above, it may still be exempt from being considered high-risk under Annex III, and therefore not require a FRIA - as described in Article 6(3) of the AI Act. To qualify, ensure **the system poses no significant risks to health, safety, or fundamental rights and meets at least one of the following conditions:**

**1. It performs a narrow procedural task.**

*Example:* An AI system used in law enforcement to automatically categorise crime reports by type (e.g., burglary, assault, fraud).

**2. It improves the results of a previously completed human activity.**

*Example:* An AI system used in the education sector to improve the language quality of a teacher's feedback on student assignments.

**3. It detects decision-making patterns without materially influencing outcomes without human review.**

*Example:* An AI system used to retrospectively determine if a teacher has deviated from the grading pattern to flag potential inconsistencies or anomalies.

**4. It performs preparatory tasks for assessments listed in Annex III.**

*Example:* AI systems used for file handling tasks such as indexing, searching, text and speech processing, or linking data to other sources. These tasks are preparatory to further assessments and thus have a minimal impact on the final decision-making process.

If no exceptions apply to your AI system, then you are required to perform a FRIA. Please refer to the following guidelines for detailed instructions on how to conduct it.

## 4. Who is responsible for conducting a FRIA?

Refer to [Table 3](#) below for a detailed description of who is responsible for conducting a FRIA:

**Table 3. Deployers responsible for conducting a FRIA**

WHO?	DESCRIPTION
Deployers* that are bodies governed by public law.	<p>Although not being defined under the AI Act, according to Directive 2014/24/EU, a body governed by public law is any body established to serve general public interest, possessing legal personality, and being either largely financed, controlled, or managed by the state or other public bodies.</p> <p><i>Example:</i> A municipal government deploying an AI system to manage public transportation schedules and routes.</p>
Deployers* that are private entities providing public services.	<p>Although not explicitly defined under the AI Act, this category broadly refers to private companies or organisations that offer services impacting the welfare, safety, or well-being of the public.</p> <p><i>Example:</i> A private hospital or clinic offering medical services to the public.</p>
Deployers* of high-risk AI systems for evaluating creditworthiness or establishing credit scores.	<p><i>Example:</i> A financial institution deploying an AI system to evaluate loan applicants' credit histories and financial behaviours. The AI analyses past credit card payments, loan repayments, and other financial data to assign a credit score. This score influences the applicant's ability to obtain loans, credit cards, mortgages, and other financial products.</p>
Deployers* of high-risk AI systems for assessing risk and pricing life and health insurance for individuals.	<p><i>Example:</i> An insurance company deploying an AI system to assess the health risks of policy applicants. The AI analyses medical records, lifestyle habits, and family medical history to evaluate the likelihood of future health issues. Based on this assessment, the AI sets insurance premiums that reflect the level of risk associated with insuring the individual.</p>

\*A deployer is: "a natural or legal person, public authority, agency, or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity" (Article 3(4) AI Act).



## 5. When should a FRIA be performed?

Deployers are required to conduct a FRIA before deploying a high-risk AI system for the first time. Once performed, subsequent deployments of the same AI system may rely on previously conducted FRIAs or existing impact assessments if they are relevant to the current deployment context. However, if any aspect of the AI system or its deployment changes significantly or becomes outdated, the deployer must update the FRIA to reflect these changes accurately.

## 6. What should a FRIA include?

The FRIA should evaluate how a high-risk AI system might impact fundamental rights, including privacy and non-discrimination. It should identify risks, outline mitigation strategies, detail human oversight plans, and explain the system's purpose and scope.

To better understand this matter, [Table 4](#) outlines the mandatory requirements for the FRIA, using the example of law enforcement agencies using AI for crime prediction. What factors should be assessed to ensure both compliance and effectiveness?

**Table 4. FRIA Requirements Applied to the Example of Crime Prediction AI System**

REQUIREMENT	EXAMPLE
Explain how the high-risk AI system will be used within the deployer's operations, ensuring it aligns with its intended purpose.	The deployer of the system must detail how the AI system integrates, which units use it, and how predictions guide patrols.
Specify the timeframe during which the AI system will operate and the frequency of its use.	The deployer of the system must define when and how frequently the AI system will analyse crime data and generate predictions to guide policing activities.
Identify the types of individuals or groups who may be impacted by the deployment of the AI system in a specific context.	The deployer of the system must conduct a demographic analysis to identify communities likely targeted by AI-driven policing, considering impacts on civil liberties, privacy, and vulnerable groups.
Assess potential risks and harms that could result from the AI system's deployment, considering the information provided by the AI provider.	The deployer of the system must conduct a risk assessment to identify biases in AI algorithms, risks of increased surveillance, and potential violations of individual rights.
Describe how human oversight will be implemented to monitor and review the AI system's operations and decisions.	The deployer of the system must outline the measures implemented to incorporate human oversight. This includes assigning trained personnel to monitor the AI, conducting regular reviews of predictions for compliance, and establishing protocols for human intervention.
Detail the actions and protocols to be followed in case the identified risks associated with the AI system actually occur.	The deployer of the system must explain the protocols adopted for addressing community concerns about AI policing.

## FRIA Template by the AI Office and other organisations

The AI Act's Article 27(5) specifies that the European AI Office will develop a future FRIA template questionnaire to assist deployers in conducting the FRIA for high-risk AI systems.

This template is intended to simplify compliance by providing a standardised framework and potentially an automated tool to guide deployers through the FRIA process. While the template is not yet available, the AI Office is expected to provide detailed guidelines to ensure deployers can efficiently conduct FRIAs and comply with the AI Act's requirements – possibly in an automated way.

In anticipation of this, various organisations have already developed their own FRIA templates to evaluate the impact of AI systems on fundamental rights.

**White Label Consultancy will also create and distribute, as a follow-up to this White Paper, its own FRIA Template to help organisations navigate the FRIA requirements and prepare for compliance.** This template will provide a practical starting point, and a structured approach designed to align with the forthcoming standards from the European AI Office and support the initial stages of compliance. **Stay updated on our [website](#) to receive notifications of the template's release.**

Nonetheless, while these existing tools can serve as useful preparatory guides for aligning AI systems with compliance standards, the European AI Office's template will be the ultimate authoritative benchmark and assessment tool for ensuring adherence to the AI Act's requirements.

## 7. Who should you notify?

After conducting the FRIA, the deployer must notify the market surveillance authority of the results by submitting the completed template provided by the AI Office. Please refer to [Annex I](#) for a list of the market surveillance authorities in each EU Member State.

### Is there an exemption to the notification requirement?

Deployers may receive temporary authorisation to deploy high-risk AI systems without completing the full conformity assessment under Article 46(1). This exemption applies in urgent situations where there are exceptional reasons, such as:

- **Public security needs,**
- **Protection of life and health,**
- **Environmental protection,**
- **Safeguarding key industrial and infrastructural assets.**

The authorisation is granted for a limited period while the necessary conformity assessment procedures are being completed and a duly justified request must be submitted to the relevant market surveillance authority to obtain this exemption.

If the authorisation is refused after the review, the use of the AI system must stop immediately, and all outputs generated during its use must be discarded. The market surveillance authority must inform the Commission and other Member States of any authorisations issued under these conditions (except for sensitive operational data related to law enforcement activities).

## 8. What about the DPIA?

A Data Protection Impact Assessment (DPIA), as specified under Article 35 of the General Data Protection Regulation (GDPR), is a risk management tool designed to evaluate any data processing activity that could potentially result in a high risk to individuals' rights and freedoms. The DPIA focuses on evaluating how personal data is collected, stored, processed, and shared, ensuring that data protection principles are upheld and that risks such as unauthorised access, data breaches, and privacy violations are minimised.

Although the DPIA and the FRIA both evaluate risks to individuals, they have different focuses. The DPIA specifically addresses personal data processing, while the FRIA may be necessary for both personal and non-personal data. Additionally, the FRIA considers risks related to privacy, non-discrimination, human dignity, and other fundamental rights.

Despite their distinct focuses, DPIAs and FRIAs are closely related and should be used together for comprehensive risk assessments. Article 27(4) of the AI Act acknowledges this relationship and provides guidance on managing it effectively. To streamline the assessment process and prevent unnecessary duplication, organisations deploying high-risk AI systems can draw on previous assessments. Suppose a DPIA has already been completed and encompasses the essential elements of a FRIA. In that case, the FRIA can then focus on broader concerns such as non-discrimination, human dignity, and other fundamental rights. This approach allows organisations to build upon the existing DPIA, ensuring that all relevant risks are addressed while avoiding redundant work.

## 9. When do you have to be compliant?

The AI Act entered into force on the 1<sup>st</sup> of August 2024, but its requirements will be phased in over time. Here's a breakdown of the timeline and key milestones:

- February 2025: Enforcement begins for AI practices deemed prohibited under the Act,
- August 2025: Obligations related to GPAI models will be in force. However, if GPAI models were on the market before this date, these obligations will apply after an additional 24 months,
- August 2026: The majority of the AI Act's requirements will come into effect,
- August 2027: Specific obligations for high-risk AI systems listed in Annex II will be enforced,

Although you have enough time to meet the FRIA requirements, it's important to use this transition period wisely. Start your compliance efforts now to avoid last-minute stress and ensure a smooth transition. By preparing early, you'll manage the requirements more effectively and position your company for successful adaptation to these new compliance requirements.

## 10. How can WLC support you?

Developing a robust compliance strategy is crucial as companies prepare for the new obligations under the AI Act. White Label Consultancy offers expert guidance to help you navigate these requirements effectively. With our extensive expertise in AI, digital services, data protection, and cybersecurity, we provide top-notch advice tailored to your needs.

We assist you in understanding and implementing compliance measures, safeguarding individual rights, and maintaining trust in your AI technologies. Our privacy consultations and ongoing publications, including the forthcoming FRIA Template, will keep you informed and prepared.

Contact us for expert support and stay updated on our resources to ensure your AI systems are deployed responsibly and in accordance with regulatory requirements.

## Annex I - List of Market Surveillance Authorities in Each EU Member State

COUNTRY	MARKET SURVEILLANCE AUTHORITY
Austria	Federal Ministry for Digital and Economic Affairs
Belgium	Federal Public Service Economy, SMEs, Self-Employed and Energy
Bulgaria	State Agency for Metrological and Technical Surveillance
Croatia	Ministry of Economy and Sustainable Development
Cyprus	Ministry of Energy, Commerce, and Industry
Czech Republic	Czech Trade Inspection Authority
Denmark	Danish Safety Technology Authority
Estonia	Consumer Protection and Technical Regulatory Authority
Finland	Finnish Safety and Chemicals Agency
France	Directorate General for Competition, Consumer Affairs, and Fraud Control
Germany	Federal Ministry for Economic Affairs and Energy
Greece	General Secretariat of Industry
Hungary	Hungarian Authority for Consumer Protection
Ireland	Department of Enterprise, Trade and Employment
Italy	Ministry of Economic Development
Latvia	Consumer Rights Protection Centre
Lithuania	State Consumer Rights Protection Authority
Luxemburg	Department of Media, Telecommunications and Digital Policy
Malta	Malta Competition and Consumer Affairs Authority
Netherlands	Netherlands Authority for Consumers and Markets
Poland	Office of Competition and Consumer Protection
Portugal	Directorate-General for Economic Activities
Romania	National Authority for Consumer Protection
Slovakia	Slovak Trade Inspection
Slovenia	Market Inspectorate of the Republic of Slovenia
Spain	Spanish Agency for Consumer Affairs, Food Safety and Nutrition
Sweden	Swedish Consumer Agency

For the official list, refer to the following page [here](#).

# Authors



## **Nicholai Pfeiffer**

Managing Partner

White Label Consultancy

[np@whitelabelconsultancy.com](mailto:np@whitelabelconsultancy.com)



## **Lucrezia Nicosia**

Consultant

White Label Consultancy

[lni@whitelabelconsultancy.com](mailto:lni@whitelabelconsultancy.com)



## **Monika Zięciak**

Associate

White Label Consultancy

[mzi@whitelabelconsultancy.com](mailto:mzi@whitelabelconsultancy.com)

# Contact

hello@whitelabelconsultancy.com

+45 71 74 74 54

## NORWAY


### Main Office Oslo

 +47 4141 2168

 Fjordalléen 16  
0250 Oslo

## DENMARK

### Copenhagen Office

 +45 71 74 74 65

 Dampfærgevej 27  
2100 København Ø

## POLAND

### Warsaw Office

 +48 515 07 99 77

 Ul. Marszałkowska 58/15  
00-545 Warszawa

## UNITED ARAB EMIRATES

### Dubai Office

 +971 50 4536616

 Dubai World Trade Centre  
Dubai

WHITELABELCONSULTANCY.COM

