A W O

Opinion

Ensuring consideration of fundamental rights in the EU AI Act

Alex Lawrence-Archer

August 2023

Opinion: sufficiency of Data Protection Impact Assessments and certain draft articles of the AI Act to ensure consideration of fundamental rights

A. Summary of opinion, background, and instructions

I. Summary of opinion

1. In our view neither the GDPR[1] requirement for data protection impact assessments ('**DPIAs**') nor the provisions of Articles 9, 62 or 63 of the draft EU AI Act (the '**AI Act**') mandate a comprehensive and prospective consideration and mitigation of risks to fundamental rights from high-risk AI systems, the objective pursued by including in the AI Act mandatory fundamental rights impact assessments ('**FRIAs**'):

   i. **DPIAs are not required in some situations** in which the use of AI systems could cause significant risks to fundamental rights.

   ii. Whilst it is arguable that DPIAs should consider fundamental rights, *in practice* it is likely that DPIAs **emphasise risks to data security and confidentiality, as opposed to broad risks to fundamental rights**.

   iii. **There are limitations to the DPIA regime** which could be improved upon in a regime mandating FRIAs in the AI Act.

   iv. **Article 9 AI Act places obligations on *providers* of AI systems, not *deployers*.** Providers of AI systems cannot fully assess how AI systems may imperil to fundamental rights once they are in deployment. The Article 9 risk management system for providers in fact *complements* FRIAs by deployers.

   v. **Articles 61-63 AI Act mandate only *ex post* reporting and market surveillance where risks from AI systems manifest**; this needs to be complemented by prospective assessment and planning in order to keep risks to fundamental rights at a socially acceptable (low) level.

2. **Proposals for FRIAs in the AI Act would meaningfully add to protections for fundamental rights from the impact of AI systems**. Where FRIAs overlap with existing DPIA requirements, this is readily resolved by requiring the two assessments to be conducted together.

[1] Regulation (EU) 2016/679

II. Background and instructions

3. The AI Act[2] will regulate AI systems[3]. It places obligations on both the:

   i. Provider of an AI system (i.e. developers): "*a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service*"; and

   ii. To some extent, the user or 'deployer' of an AI system: "*any 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.*"[4]

4. Whilst the European Commission ('**Commission**')'s proposal uses the term 'user', the European Parliament ('**EP**')'s proposal uses the term deployer, with the same definition. We adopt the latter term in this Opinion.

5. The AI Act is promulgated with a view to:

   > *"laying down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values."* (Recital 1 AI Act)

6. Broadly speaking, the AI Act (i) prohibits certain AI systems (Article 5), and (ii) classifies some other AI systems as 'high risk' (Article 6). A classification of an AI system as high risk brings with it a range of obligations – primarily for the provider – contained in Chapter 2 AI Act.

7. In this context, many have highlighted the potential for AI systems to interfere with individuals' fundamental rights[5] (see detail in section B.I) below. Indeed, the Commission has stated that one of its objectives for the AI Act is to:

---

[2] All references to Articles and Recitals are to the text proposed by the European Commission - https://artificialintelligenceact.eu/the-act/ - unless otherwise stated.

[3] Broadly defined in Article 3 as *"software that is developed with one or more of the techniques and approaches listed in Annex I* [machine learning, logic-based and statistical approaches] *and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."*

[4] Both Article 3 AI Act. The majority of the regulatory burdens created by the AI Act are placed on providers of AI systems. However, the precise distribution of responsibilities between providers and deployers is a matter of ongoing legislative debate.

[5] Typically thought of as encompassing – at a minimum – the rights set out in the European Union Charter of Fundamental Rights.

"ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values."

8. This has led to proposals for the AI Act to mandate FRIAs: that is, to require deployers of high-risk AI systems to carry out a comprehensive and prospective assessment of how high-risk AI systems may impact fundamental rights, and to mitigate those risks. These proposals have resulted in a proposed new Article 29a of the AI Act, promulgated by the EP (included at Annex 1 for reference).

9. We are instructed that others have argued against the inclusion of mandatory FRIAs in the AI Act, on the basis that they would be duplicative of requirements elsewhere in the AI Act, or in the GDPR (see section B.III below).

10. We are therefore asked to give an opinion on whether the DPIA requirements of the GDPR or certain existing Articles of the AI Act mandate the consideration and protection of fundamental rights, such that FRIAs are not required to be included in the Act.

B. Fundamental Rights Impact Assessments

I. Rationale and objectives

11. A full assessment of how AI systems can imperil fundamental rights is unnecessary and beyond the scope of this Opinion. We are instructed that advocates for FRIAs have identified various ways in which AI systems can (among other things) exacerbate bias, facilitate repression and surveillance, promote the spread of disinformation, and undermine the integrity of democratic institutions[6].

12. Research[7] has also shown that European citizens themselves are concerned about the impact that AI systems may have on fundamental rights.

13. FRIAs are posited as a means to ensure that prior to deployment, the ways in which a high risk AI system might interfere with fundamental rights are assessed, enabling the deployer to plan to mitigate risks to fundamental rights as far as possible (i.e. by modifying plans for deployment of the AI system). This would reduce the incidence of interference with fundamental rights from AI systems, contributing to a socially acceptable and proportionate level of protection for those rights.

[6] https://avaazimages.avaaz.org/Avaaz_From_Harms_to_Hope_Jun_2023.pdf sets out examples of the ways in which AI systems have interfered with fundamental rights in the recent past.
[7] https://secure.avaaz.org/campaign/en/from_harms_to_hope/#report-section-02

14. What constitutes a sufficient level of protection for fundamental rights from AI systems is of course subjective. Based on the wording of draft Article 29a, the objective pursued in requiring FRIAs through the AI Act (the '**FRIA Objective**') appears to be to ensure that risks to fundamental rights are comprehensively prospectively assessed in the context of specific deployments of AI systems, and that deployers plan to mitigate those risks, or do not deploy if mitigation is not possible.

15. In providing this Opinion we assess whether the FRIA Objective is already achieved by other means, since those advocating against FRIAs in the AI Act suggest that Article 29a is redundant, since the FRIA Objective is met by the DPIA regime and other AI Act requirements (see further section III below).

II. What is proposed?

16. In summary, the EP's draft Article 29a requires deployers of high-risk AI systems to:

    i. Assess the AI system in-context, including:

    > *"(e) the reasonably foreseeable impact on fundamental rights of putting the high-risk AI system into use; (f) specific risks of harm likely to impact marginalised persons or vulnerable groups; (g) the reasonably foreseeable adverse impact of the use of the system on the environment; (h) a detailed plan as to how the harms and the negative impact on fundamental rights identified will be mitigated."*

    ii. Not deploy the system if the risks cannot be mitigated.

    iii. (Excluding SMEs)[8] inform the supervisory authority of the FRIA and *"to the best extent possible"* consult with representatives of those likely to be affected, as well as (e.g.) consumer protection and equality bodies.

    iv. (For public authorities and 'gatekeeper' undertakings under the EU Digital Markets Act) publish a summary of the FRIA.

III. Counterarguments against the inclusion of FRIAs in the AI Act

17. We are instructed that arguments against the inclusion of FRIAs in the AI Act have focused on their redundancy in light of other provisions. That is, it is claimed that existing

[8] For the avoidance of doubt, SMEs are only excluded from this specific aspect of the FRIA requirement in Article 29a.

law – or other proposed Articles of the AI Act – already achieve the FRIA Objective without the provisions of Article 29a being necessary. Specifically, it is claimed that:

i. DPIAs required under the GDPR will cover risks to fundamental rights from high-risk AI systems.

ii. The Article 9 AI Act duty for providers of AI systems to establish risk management frameworks for high-risk AI systems will ensure that any risks to fundamental rights are monitored and documented (and therefore mitigated against).

iii. The requirements in Articles 61-63 AI Act for incidents of interference with fundamental rights from AI systems to be reported to and monitored by supervisory authorities negates the need to prospectively assess the risk of such incidents.

C. Data Protection Impact Assessments

I. What the GDPR requires

18. Article 35(1) GDPR states:

> *"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."*

19. The Article goes on to provide examples of when processing will *'in particular'* be considered to be high risk and therefore require a DPIA, and in Article 35(7) to set out the contents required in a DPIA:

> *"The assessment shall contain at least:*
> *(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
> *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
> *(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."

20. The 'controller' is "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*"[9], which is analogous to the deployer of an AI system.

21. 'Processing' and 'personal data' are very broadly defined in the GDPR.[10] Often, the deployment of an AI system will involve the processing of personal data. Where that processing is '*likely to result in a high risk to the rights and freedoms of natural persons'*, the controller/deployer will be obliged by the GDPR to carry out a DPIA assessing that risk and, per Article 35(7), plan to mitigate it.

22. Where a DPIA is required, its structure is relatively similar to that envisaged for FRIAs[11]. As set out at para 19 a DPIA involves a description of the processing and its purpose, an assessment of its proportionality, an assessment of risks to individuals (data subjects) and a plan for measures to address those risks. These elements correspond to the requirements for FRIAs in Article 29a:

    i. Description of processing, purpose and proportionality: requirements (1)(a), (b) and (in part) (d) from Article 29a.

    ii. Assessment of risks: requirements (1)(c), (e) and (f) from Article 29a.

    iii. Plan for measures to address risks: requirements (1)(h) and (i) from Article 29a.

II. <u>Gaps in ensuring comprehensive prospective consideration of fundamental rights</u>

23. Several features of the DPIA regime mean that while DPIAs overlap in some respects with FRIAs, that overlap is not complete, leaving gaps in pursuing the FRIA Objective.

    a) <u>Only applicable where there is processing of personal data</u>

24. A DPIA is only required where there is processing of personal data (that is, information relating to an identifiable individual). As stated above, often the deployment of a high-

[9] Article 4 GDPR
[10] *Ibid*
[11] We do not consider in detail the territorial application of the GDPR vs the AI Act, but in most respects they are identical such that the deployer of an AI system caught by the AI Act will also be caught by the GDPR to the extent that the deployment involves the processing of personal data.

risk AI system will involve the processing of personal data (e.g. where an AI system is used to determine eligibility for social benefits). However, many situations can be envisaged where AI systems present risks to fundamental rights – which need to be assessed and mitigated – despite not involving the processing of personal data of those affected.

Example 1: A deployer of navigation technology incorporated into partly self-driving cars uses an AI system to direct motor traffic to the routes that safely minimise travel time for users of the app. This results in an increase in 'rat-running' whereby drivers take more complex, but less congested routes through quieter neighbourhood streets. The resulting increase in air pollution, decrease in air quality and increased risk of road accidents interfere with residents' right to life and to environmental protection, but their personal data is not processed by the navigation technology deployer, meaning any DPIA (if required) would not consider this interference with their fundamental rights.

Example 2: The authorities use fully anonymised statistics on previously reported crimes to determine the allocation of physical police patrols to certain neighbourhoods through an AI system. The deployed system results in increased allocations of patrols where arrests leading to convictions for small-scale drug possession have historically been highest, which also happen to be areas with a higher proportion of ethnic minority residents than the national average. Such a system – and the consequent over-policing of historically over-policed communities poses a risk to rights to life, dignity, liberty (among others) as well as rights to non-discrimination. This is despite the AI system processing no personal data, meaning a DPIA is not required.

Example 3: The semi-privatised national railway authority deploys an AI system to dynamically determine rail fares to 'smooth out' demand by predicting and responding to peaks and troughs through 'surge pricing'. The system only uses fully anonymised, aggregated data on rail route capacity and use. The resulting price rises for those living further from their work and who are unable to work from home could interfere with rights to non-discrimination and to access to services of general economic interest, despite the deployment of the AI system involving no personal data and therefore not requiring a DPIA.

Example 4: A border agency deploys an AI system to assess the likely appearance of unseaworthy boats transporting irregular migrants who may be in need of assistance in order to prioritise patrols. The system uses only 'boat-level' data on the routes of previously intercepted boats. It achieves significant efficiencies, subject to the deployers of the system setting a level of 'risk tolerance' for false negatives (i.e. areas in which no boats are anticipated, and therefore no patrols despatched). The consequent failure to rescue migrants could interfere with their right to life, despite the system using no personal data and therefore not requiring a DPIA.

b) Unclear whether high-risk AI systems are high risk for the purposes of the GDPR

25. A DPIA is required where processing is '*likely to result in a high risk to the rights and freedoms of natural persons'.* Under Article 29a, a FRIA would be required for *all* deployments of high-risk AI systems (as defined in Article 6 AI Act). Despite the similar terminology, these definitions are distinct. It is not clear that every deployment of a high-risk AI system will meet the criteria triggering a DPIA under Article 35 GDPR. The version of Article 29 proposed by the Commission recognises this:

> *"Users* [deployers] *of high-risk AI systems shall use the information provided under Article 13 to comply with their obligation to carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680,* ***where applicable.****"* (emphasis added)

26. For example, an AI system will be high-risk for the AI Act if it is '*intended to be used for recruitment or selection of natural persons'* (Article 6 and Annex III). That is, intended to be used in any way for recruitment. An AI system used to optimise the scheduling of interviews would meet this definition and therefore be a high-risk AI system, but the processing of setting appointment times would likely not be likely to result in a '*high risk to the rights and freedoms of natural persons*'. Similarly, an AI system for use as a safety component in personal watercraft may process the personal data of craft testers. This would be a high-risk AI system under the AI Act (Article 6 and Annex II) but the *processing of personal data* involved (as opposed to the testing activities and operation of the craft) would not be high-risk in the sense requiring a DPIA.

c) In practice, DPIAs may be more focused on risks to privacy and data security

27. The language of Article 35 GDPR is general: it requires an assessment of the risks to data subjects' *'rights and freedoms'*. It is well arguable that this should include an

assessment of risks to fundamental rights, which could suggest that a FRIA requirement in the AI Act is unnecessary.

28. Recital 91 to the GDPR provides some support for this proposition, as does some guidance from the Article 29 Working Party:

> *"the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion."*[12]

29. Some academic commentators have argued that the DPIA regime requires a consideration of impacts on fundamental rights, whilst also acknowledging the significant uncertainty faced by data controllers in interpreting GDPR requirements[13].

30. Others have instead highlighted approaches to DPIA compliance in practice, including by reference to guidance and enforcement from data protection authorities:

> *"Existing data protection regulations are still focused on the traditional pillars of the so called fourth generation of data protection law: the purpose specification principle, the use limitation principle and the notice and consent model (i.e. an informed, freely given and specific consent)."*[14]

31. Guidance from regulators in the Union does indeed appear to prioritise risks to data security. By way of example:

    i. Guidance from the Commission nationale de l'informatique et des libertés (the French data protection authority) states in its guidance on DPIAs:

    > *"A risk is a hypothetical scenario that describes a feared event and all the threats that would allow it to occur. More specifically, it describes:*
    > - *how sources of risk (e.g., an employee bribed by a competitor) could exploit the vulnerabilities of data carriers (e.g., the file management system, which allows* ***manipulation of data****)*

---

[12] *Guidelines on Data Protection Impact Assessments*, 2017: https://ec.europa.eu/newsroom/article29/items/611236

[13] Janssen, Heleen, *Detecting New Approaches for a Fundamental Rights Impact Assessment to Automated Decision-Making* (2020). International Data Privacy Law 10:1, https://doi.org/10.1093/idpl/ipz028

[14] Mantelero, *Beyond Data, Human Rights, Ethical and Social Impact Assessment in AI* (2022) Open Access

- *in the context of threats (e.g.: **hijacking by sending e-mails)** and allowing feared events to occur (e.g.: **illegitimate access** to data) [in relation to] personal data (e.g.: customer files)*
- *causing impacts on the privacy of the persons concerned (eg: unwanted solicitations, feeling of invasion of privacy, personal or professional problems).”*[15]

ii. Guidance from the Dutch Government on DPIAs[16] states:

> *“A DPIA will also show you what measures you should take to prevent or minimise the risk of a privacy breach.”*[17]

iii. The Irish data protection commission in its guidance on DPIAs provides several examples of risks which should be covered, including ‘*inappropriate disclosure of personal data*’, ‘*disclosure of personal information to third parties’*, and ‘*data may be kept longer than required in the absence of appropriate policies*’*,* but not mentioning any risks relating to (for example) discrimination due to algorithmic bias.

32. Although a full survey of guidance from data protection authorities across the Union is not possible, these examples from leading authorities give a sense – through official guidance on which data controllers are likely to rely – of the emphasis in the DPIA regime that tends to be placed on particular types of risk. That is, risks to data security and confidentiality, as opposed to broader risks to fundamental rights.

33. Structurally, DPIAs may be less likely than FRIAs to take risks to fundamental rights into account. For example, there is no requirement to consult with the individuals affected or their representatives (or indeed with anyone else)[18]. This contrasts with draft Article 29a which requires consultation (by non-SME deployers) of representatives of those affected as well as equality, consumer protection, and social partner bodies. This underlines the focus of FRIAs – as distinct from DPIAs – on ensuring that deployers come to a broad understanding of the various ways in which an AI system might affect people.

---

[15] https://www.cnil.fr/en/privacy-impact-assessment-pia; translated from French
[16] https://business.gov.nl/regulation/data-protection-impact-assesment-dpia/
[17] The Dutch Government’s development of an FRIA framework further suggests that it considers fundamental rights not to fall squarely within the existing DPIA regime: https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms
[18] This is only required by Article 35 of the GDPR ‘where appropriate’, which is not further defined, stripping the requirement of any practically enforceable meaning.

34. There is no requirement to publish DPIAs and there is no central repository of DPIAs carried out by controllers across the Union. Further, enforcement or litigation relating to the *content* of DPIAs (as opposed to whether or not a DPIA was carried out prior to processing) has been rare. In the scope of this Opinion therefore it is not possible to conclusively demonstrate that DPIAs *do not* consider risks to fundamental rights.

35. An expansive interpretation of the GDPR would view fundamental rights as being required content in a DPIA. A highly conscientious controller would perhaps follow this approach, but we are instructed that it is not common practice. This is not surprising, given the tension between the Recitals to the GDPR and Working Party Guidance on the one hand, and 'working level' guidance from data protection authorities on the other.

36. **In practice the DPIA regime does not appear to reliably *require* the consideration of risks to fundamental rights. This is unsatisfactory in light of the clear risks which AI systems do present. The FRIA regime under Article 29a – in strong contrast – places a prominent, explicit, and readily enforceable emphasis on the need to consider risks to fundamental rights.**

d) Limitations of the DPIA regime: transparency and supervisory authority role

37. There is no requirement to publish DPIAs and indeed it is very rare for them to be published, despite encouragement from data protection authorities (since doing so could be damaging for the controller carrying out the DPIA)[19].

38. This contracts with Article 29a:

> *The deployer that is a public authority or an undertaking referred to in Article 51(1a)* [a gatekeeper undertaking for the Digital Markets Act] *(b) shall publish a summary of the results of the impact assessment as part of the registration of use pursuant to their obligation under Article 51(2).*

39. Likewise, under the GDPR, a controller carrying out a DPIA only needs to consult with the supervisory authority in certain circumstances:

> *"The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would*

[19] Although note that Article 29 AI Act as proposed by the EP would require any DPIA associated with the deployment of a high-risk AI system to be published in summary form.

result in a high risk in the absence of measures taken by the controller to mitigate the risk."

40. This contrasts with Article 29a which requires consultation (except for SMEs) in all cases where a high-risk AI system is deployed.

41. Finally, the DPIA regime places the burden on the supervisory authority to intervene where risks cannot be adequately managed: processing is only prevented where the supervisory authority does so under Article 36 GDPR. By contrast, Article 29a requires the system not to be put into deployment if sufficient mitigation measures cannot be identified. That is, it places a much clearer obligation on the deployer (or data controller by analogy) not to deploy risky AI systems than the DPIA requirements of the GDPR.

42. These three factors demonstrate **some weaknesses in the DPIA regime** – less transparency, less involvement from the supervisory authority, and weaker requirements not to engage in risky activities – **which would be addressed by the FRIA regime**[20] proposed in Article 29a, promoting the FRIA Objective.

e) Summary

43. **Taken together, key aspects of the DPIA regime show that it cannot be relied upon to deliver the FRIA Objectives.** The below summary table shows that**:**

i. A DPIA will not always be required where AI systems imperil fundamental rights.

ii. Even where required, the DPIAs do not in practice place an explicit and readily enforceable emphasis on the consideration of fundamental rights.

iii. The DPIA regime lacks transparency and a firm requirement on deployers not to deploy unacceptably risky systems.

44. **FRIAs as proposed in Article 29a promote the FRIA objective above and beyond what is already required by the DPIA regime in the GDPR**. This is not to say that FRIAs and DPIAs are completely distinct. As set out in para C.I, in some cases a DPIA and FRIA will cover related or overlapping issues. The downsides of this are limited though, since Article 29a(6) provides for the two assessments to be carried out '*in conjunction*'.

[20] Albeit that this is dependent on precisely how Article 29a is drafted, which is still to be confirmed.

Summary comparison table; DPIAs vs FRIAs

Features	DPIAs/GDPR	FRIAs/AI Act
Responsible entity	Controller in relation to processing	Deployer of an AI system (generally analogous to controller)
When an assessment might be required	Where personal data is processed	Where a high-risk AI system is deployed (only in *some* cases will this involve processing of personal data)
Risk level triggering requirement	'Likely to result in a high risk to the rights and freedoms of natural persons'	Always required where an AI system is high-risk as defined by Article 6 AI Act
Risks covered	Statutory language is neutral; practice suggests focus is on data security and confidentiality and on data subjects	All risks to fundamental rights. Broad consultation required.
Shared with supervisory authority?	Only where risk to rights and freedoms is high in the absence of mitigations	Yes (except SMEs)
Published?	No	Yes, for public bodies and gatekeepers
Obligation not to deploy/process?	No: burden is on supervisory authority to intervene	Yes: deployer must not deploy if risks cannot be mitigated

D. Articles 9 and 61-63 AI Act

I. Article 9

45. Article 9 AI Act provides *"A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems."* Article 9(2) clarifies that the risk management system should identify and evaluate risks of the AI system and put in place measures to address them so that:

> *"any residual risk associated with each hazard as well as the overall residual risk of the high-risk AI systems is judged acceptable, provided that the high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse."*

46. Article 16 AI Act makes the *provider* of the high-risk AI system responsible for putting in place and implementing this risk management system.

47. Amendments proposed by the EP tend to broaden the scope of the requirements of Article 9, requiring emergent risks to be considered, and explicitly directing the attention of the provider of the AI system to risks to fundamental rights (which are not mentioned in the texts proposed by the Commission or Council).

48. The wording of Article 9 is broad, covering 'risks' in general, which may be interpreted to cover risks to fundamental rights (particularly in light of the preamble and recitals to the AI Act), although fundamental rights are not named in the Commission text. The EP version makes it clear that fundamental rights must be considered by providers of AI systems to the extent possible. **Thus the risk management system makes some contribution to the FRIA Objective.**

49. **However, this does not mean that Article 9 makes FRIAs under Article 29a redundant**. Article 9 envisages risk management being carried out by providers, not deployers of AI systems. In practice – even taking into account the testing requirements of Article 9 – providers will have only limited information and insight into how their systems might interfere with fundamental rights. Without the context of one or more specific deployments of a system, providers cannot be expected to assess and manage all the ways in which fundamental rights may be affected. Consider for example:

AI System	**Potential Deployments**
Example 1: An AI system which aims to efficiently and quickly predict an individual's problem-solving skill level	To set the starting level for a new user in an online game: **low fundamental rights impact.**
	To stream applicants for employment in public administration: **high fundamental rights impact.**

AI System	**Potential Deployments**
Example 2: AI system which plots the most efficient path for a vehicle which needs to make a number of predefined stops in complex terrain	To control an agricultural vehicle used to carry out a mix of tasks on a farm staffed by a small number of skilled workers: **low fundamental rights impact.**
	To control a self-driving ambulance which needs to visit a number of emergency situations of varying priority levels: **high fundamental rights impact.**

AI System	Potential Deployments
Example 3: AI system which generates convincingly human-like written output in response to prompts from users, which can be refined through 'conversation' between the user and the system.	To help people write speeches for social situations such as weddings: **low fundamental rights impact.**
	To reduce primary mental healthcare costs by engaging users in crisis in conversation and suggesting self-help solutions: **high fundamental rights impact.**

50. These examples demonstrate that the impact of a high-risk AI system is dependent on the context in which it is deployed, which can only be judged by the deployer. Indeed, requiring providers to predict all the different ways in which a general purpose AI system might affect fundamental rights in use by different deployers throughout the Union would place an unacceptable and completely unrealistic burden on them, seriously undermining the Article 9 risk management system.

51. **Rather than overlapping with the requirement for FRIAs in Article 29a, the risk management system in Article 9 would complement FRIAs, providing a starting point of assessment of potential issues from a more technical perspective for deployers to consider when conducting FRIAs, contributing to the FRIA Objective.**

II. Articles 61-63

52. Article 61 provides:

> *"1. Providers shall establish and document a post-market monitoring system in a manner that is proportionate to the nature of the artificial intelligence technologies and the risks of the high-risk AI system.*
>
> *2. The post-market monitoring system shall actively and systematically collect, document, and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2."*

53. Article 62 provides:

> *"Providers and, where deployers have identified a serious incident, deployers of high-risk AI systems placed on the Union market shall report any serious incident of those*

systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the national supervisory authority of the Member States where that incident or breach occurred."

54. The Article goes on to provide for the sharing of information on incidents reported between supervisory authorities and – in the EP's version – for appropriate measures or corrective actions to be taken by supervisory authorities or deployers respectively.

55. Article 63 provides for surveillance by supervisory authorities of the compliance of AI systems with parts of the AI Act.

56. Taken together, these Articles concern *ex post* activities only where risks to fundamental rights have actually manifested. They may play a role in ensuring that, where things do go wrong, lessons are learned for future deployments.

57. The FRIA Objective is different: its focus is on preventing – as far as possible – fundamental rights from being infringed in the first place, through comprehensive and prospective assessment of risks. This reflects the importance of fundamental rights in the European legal order, and the fact that it is far from straightforward for individuals to get redress when their fundamental rights are breached, making strict measures to prevent breaches proportionate.

58. **By definition therefore, since Articles 61-63 only address interferences with fundamental rights retrospectively, they cannot make a significant contribution to the FRIA Objective**, although as more information from post-market monitoring by providers and market surveillance becomes available, the quality of FRIAs conducted under Article 29a is likely to increase.

Annex 1: Text of EP Proposed Article 29a[21]

1. Prior to putting a high-risk AI system as defined in Article 6(2) into use, with the exception of AI systems intended to be used in area 2 of Annex III, deployers shall conduct an assessment of the systems' impact in the specific context of use. This assessment shall include, at a minimum, the following elements: (a) a clear outline of the intended purpose for which the system will be used; (b) a clear outline of the intended geographic and temporal scope of the system's use; (c) categories of natural persons and groups likely to be affected by the use of the system; (d) verification that the use of the system is compliant with relevant Union and national law on fundamental rights; (e) the reasonably foreseeable impact on fundamental rights of putting the high-risk AI system into use; (f) specific risks of harm likely to impact marginalised persons or vulnerable groups; (g) the reasonably foreseeable adverse impact of the use of the system on the environment; (h) a detailed plan as to how the harms and the negative impact on fundamental rights identified will be mitigated. (j) the governance system the deployer will put in place, including human oversight, complaint-handling and redress.

2. If a detailed plan to mitigate the risks outlined in the course of the assessment outlined in paragraph 1 cannot be identified, the deployer shall refrain from putting the high-risk AI system into use and inform the provider and the National supervisory authority without undue delay. National supervisory authorities, pursuant to Articles 65 and 67, shall take this information into account when investigating systems which present a risk at national level.

3. The obligation outlined under paragraph 1 applies for the first use of the high-risk AI system. The deployer may, in similar cases, draw back on previously conducted fundamental rights impact assessment or existing assessment carried out by providers. If, during the use of the high-risk AI system, the deployer considers that the criteria listed in paragraph 1 are not longer met, it shall conduct a new fundamental rights impact assessment.

4. In the course of the impact assessment, the deployer, with the exception of SMEs, shall notify national supervisory authority and relevant stakeholders and shall, to best extent possible, involve representatives of the persons or groups of persons that are likely to be affected by the high-risk AI system, as identified in paragraph 1, including but not limited to: equality bodies, consumer protection agencies, social partners and

[21] As at June 2023

data protection agencies, with a view to receiving input into the impact assessment. The deployer shall allow a period of six weeks for bodies to respond. SMEs may voluntarily apply the provisions laid down in this paragraph. In the case referred to in Article 47(1), public authorities may be exempted from this obligations.

5. The deployer that is a public authority or an undertaking referred to in Article 51(1a)(b) shall publish a summary of the results of the impact assessment as part of the registration of use pursuant to their obligation under Article 51(2).

6. Where the deployer is already required to carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 shall be conducted in conjunction with the data protection impact assessment. The data protection impact assessment shall be published as an addendum.