Council of the European Union
General Secretariat

**Brussels, 25 April 2025**

**WK 5269/2025 INIT**

**LIMITE**

**TELECOM**
**CYBER**
**DATAPROTECT**

*This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.*

**MEETING DOCUMENT**

| | |
|---|---|
| From:<br>To: | General Secretariat of the Council<br>Delegations |
| Subject: | Main takeaways from the debate on the AI Act and the GDPR |

Delegations will find in the annex the main takeaways from the debate on the AI Act and the GDPR.

## Main takeaways from the debate on the AI Act and GDPR

Joint debate of Working Party on Data Protection (WP Data Protection) & Working Party on Telecommunications and Information Society (WP TELECOM)

Polish Presidency of the Council of the EU

### Introduction

On 14 March 2025, the Polish Presidency organised a joint debate on the interplay between the AI Act and GDPR. The debate was held at the meeting of Working Party on Data Protection (WP Data Protection) with the participation of Working Party on Telecommunications and Information Society (WP TELECOM). The debate began with a short contribution from the European Commission (DG CONNECT and DG JUST) on the interplay between the AI Act and GDPR. It was followed by the presentation of Presidency discussion paper (doc. WK 2625/2025) on this topic, and an exchange of views among Member States.

The aim of the debate was to identify challenges that may arise from compliance with both the AI Act and GDPR, from the perspective of both the obliged entities as well as the relevant authorities: market surveillance authorities (MSAs) under the AI Act and data protection authorities (DPAs) under EU data protection law. The discussion also aimed to find best practices in cooperation between these two entities, as well as with other relevant stakeholders.

This presidency paper summarizes key takeaways from the discussion at the joint debate and written contributions shared by Member States.

### Key takeaways

The debate was organised around guiding questions outlined in the Presidency discussion paper. Several takeaways can be drawn from the discussion.

### PART 1 – Main challenges in implementation and compliance with both the GDPR and AI Act & possible actions

***Question 1****: What do you expect to be the main challenges for the competent national authorities under the AI Act and the supervisory data protection authorities regarding the application of both the AI Act and the GDPR?*

***Question 2****: What are the main challenges for providers and deployers of AI systems, regarding compliance with both the AI Act and the GDPR? (i.e. lack of understanding of the provisions and their correlation, complementarity of obligations)? What are ways to minimize* *the burden for providers and deployers of AI systems for obligations which may have similar elements (e.g. the fundamental rights impact assessments)?*

### *1) Differing regulatory approaches between the AI Act and GDPR*

Most Member States notice that GDPR and AI Act follow **different regulatory approaches**. GDPR is focused on the protection of data subjects' personal data (fundamental rights-based approach); its rules apply to all personal data processing activities within the scope of the GDPR following a risk-based approach. By contrast, the AI Act is a market based and product safety legislation that applies to AI systems, regardless of whether they process personal data or not that aims to ensure safety and fundamental rights within the whole AI system's lifecycle, following a risk-based approach with targeted requirements applying to only certain AI systems depending on the level and severity of the risks they pose.

According to some Member States, the difference in the underlying logic between the two acts might lead to different regulatory outcomes (i.e. an AI system is deemed compliant with the AI Act's requirements – but still violates data protection principles, or vice versa) – necessitating a careful case by case approach.

On the other hand, some Member States referred to a risk that an entity deploying an AI system would **infringe both the GDPR and the AI Act** and thus be subject to sanctions under both regulatory frameworks for the same action. To address these scenarios it is crucial that both legal acts are interpreted and enforced coherently.

Moreover, it is important that market surveillance authorities and data protection authorities have a close and continuous dialogue and cooperate on ongoing supervisory and market surveillance activities.

### *2) Interpreting AI Act provisions and their interplay with GDPR*

Many Member States signaled that AI Act poses challenges to interpret due to its complexity, especially when there is a need to interpret it in combination with other laws (such as GDPR). Thus, they see the need that the European Commission provides **clarifying guidelines, including on the interplay between GDPR and AI Act**. The guidelines could explain key concepts, the scope of application of provisions and complementarity of obligations regarding e.g. risk assessment, rights of data subjects, redress mechanisms or safeguards. The guidelines could also help minimize the administrative burden, e.g. by elaborating on how to reuse or share documentation regarding risk assessment and impact assessments relating to both GDPR and the AI Act.

In addition, some Member States proposed organizing **workshops for entrepreneurs** to address outstanding questions, which could further reduce legal uncertainty.

### *3) Using personal data to train AI systems*

Entities that use personal data to train AI systems must be aware of the GDPR's principle of purpose limitation. Where personal data is not collected with the initial intent to train AI systems, any further processing of such data requires compliance with certain rules of the GDPR (e.g. on compatible processing).

### *4) Ensuring coordination and collaboration*

Effective coordination among stakeholders is both a challenge and a necessity for successful implementation. Member States stressed the importance of **establishing a proper national governance structure** that promotes cooperation between the responsible authorities, particularly in cases where AI systems process personal data. They also emphasized that **EU-level exchanges of good practices** and the **development of joint guidelines** (for example guidelines for national authorities responsible for supervision of the AI Act and GDPR, or a common understanding of the technical principles of the respective AI systems) can harmonize interpretations and supervision practices. This exercise could be supported by the AI Board Sub-Group on the AI Act's interplay with other Union legislation, the AI Office and the EDPB. Overall, cooperation should be designed in a way that precludes decisions which contradict one another and taking advantage of all possible synergies. However, such close coordination demands significant **technical expertise** and **sufficient funding**.

### *5) Ensuring the accessibility of a talent pool*

Another challenge is the recruitment of staff with the necessary AI expertise. For effective implementation, regulators, particularly the supervisory authorities, must understand the underlying technology. At the same time, the demand for professionals with such skills exceeds the supply.

### *6) Fundamental rights impact assessment*

Some Member States observed that the fundamental rights impact assessment, as per Article 27 of the AI Act, may require balancing a broad range of rights that could potentially conflict with one another. A suggestion was made to evaluate **to which extent the methodology of the data protection impact assessment is suitable to evaluate all other types of impacts or if providers and deployers of AI will resort to regularly favour data protection interests because they are better known and more strongly emphasised**.

Some Member States noted that while in line with Article 27(4) of the AI Act the fundamental rights impact assessment should complement the data protection impact assessment (Article 35 of the GDPR), the necessity to perform two impact assessments might nevertheless lead to some duplication of efforts. As a solution, Member States suggested developing standardized templates and model cases (possibly with the use of regulatory sandboxes).

### *7) Minimising administrative burden*

Minimizing the administrative burden can be achieved by offering **clear, easy-to-implement advice**, standardized templates (such as a model for a complex impact assessment that meets both GDPR and AI Act requirements) and streamlined reporting mechanisms. Member States underlined that guidelines should focus on clarifying the interplay between the two legal instruments, which would help to avoid legal uncertainty and navigate potentially overlapping compliance obligations.

The European Commission informed Member States that it is currently preparing **guidelines on the relationship of the AI Act with relevant Union law, including GDPR, in line with Article 96(1)(e) of the AI Act. The Commission is also working on a template for the fundamental rights impact assessments (FRIA) as required under Article 27 AI Act**. FRIA should complement and not overlap with the data protection impact assessment and the Commission objective is to provide clear and simple way to implement it with a questionnaire. The Commission also ci that the European Data Protection Board (EDPB) is working on guidelines on the interplay between the data protection law and the AI Act, and that the Commission is discussing with the EDPB opportunities for synergies to ensure consistency in the interpretation, legal certainty and clarity for operators.

## PART 2 – Cooperation between key actors and stakeholders

***Question 3****: Smooth and effective implementation of the AI Act and GDPR with regards to AI systems will require close cooperation of multiple actors representing both the AI and the data protection domains. How do you intend to ensure it at the national level? Please share your best practices and examples of existing cooperation between authorities at the national level, which could be built upon to ensure a consistent implementation of the AI Act and the GDPR in the future.*

***Question 4****: How can the cooperation between the future AI Act market surveillance authorities and GDPR authorities be facilitated (guidelines, collaborative approach in the administration, practical examples, IT tools etc.)? What actions would you see at the EU level?*

### 1) *DPAs as competent authorities within the meaning of AI Act*

Some Member States proposed that data protection authorities should be designated as the enforcers of the AI Act, to strengthen the connection between the two regulatory frameworks. This approach would solidify the role of DPAs and help ensure that both sets of obligations are implemented in a consistent manner.

### 2) *Establishing cooperation mechanisms at national level*

There was broad agreement on the need to establish a **cooperation mechanism for national authorities responsible for both the GDPR and the AI Act at national level**. This mechanism could take the form of joint task forces, technical working groups, coordination bodies, networks, and make use of tools such as conferences, policy forums, or memoranda of understanding. Such structures would **facilitate collaboration** and **provide a platform for experts** from the data protection and AI fields to jointly interpret and apply the regulatory requirements.

In addition to cooperation between national authorities, it would be also beneficial to enhance **broader collaboration** with **diverse stakeholder groups** such as businesses, civil society, trade unions, and academia. **Using IT tools, coordination platforms, and other digital resources** was suggested as a way to enable real-time data exchange in a confidential manner (between a wide range of stakeholders, but also between relevant supervisory authorities) and to reduce administrative burdens while enhancing overall enforcement effectiveness.

### *3) Sharing good practices and harmonized guidelines at national level*

Member States shared examples of effective initiatives, such as coordination platforms and existing memoranda of understanding, which have already been implemented in some countries. They also suggested **to develop common best practices, guidelines, codes of practice,** and even a single auditing framework to ensure that AI systems are assessed holistically. It would be particularly helpful to clarify the interplay between AI compliance requirements and GDPR principles, in areas of intersection and regarding the processing of personal data. The guidance should be coordinated in **a cross-sectoral manner** and **cover several legal areas** so that relevant stakeholders do not have to search for information from several different sources. These actions would not only reduce administrative burden but also would help build regulatory capacity and harmonize enforcement practices across the EU.

### *4) EU-level coordination initiatives*

Lastly, there was a clear call from Member States to the Commission to issue **EU-level guidelines** to address the interplay between the two acts. Some Member States also underlined the importance of **Codes of Conduct** as a tool that can bring clarity on certain points.

Given the interplay between the AI Act and GDPR, it is necessary to **ensure cooperation between relevant EU-level stakeholders**, for example the AI Office, AI Board, European Data Protection Board (EDPB). One Member State also indicated the European Digital Innovation Hubs (EDIHs) could also play a role in supporting private entities with advice. It is also important to ensure that all digital acts should be implemented in a consistent manner. A consistent legal framework and its implementation is crucial to boost the competitiveness and digital sovereignty of the European economy.

The call for coordination is also important considering the likelihood of cross-border cases under the GDPR that might also concern AI systems.

Additionally, the European Commission could support these efforts with **capacity-building initiatives**, for example by **providing dedicated resources and funding for joint training**

**programmes and seminars**, particularly joint sessions for national authorities responsible for both regulations. Overall, reducing bureaucratic inefficiencies through institutional cooperation can help mitigate compliance costs and enhance regulatory effectiveness.

The Commission asked Member States to identify key aspects on which there is a need to provide guidelines. The Commission also announced the upcoming establishment of the AdCo group, which will comprise market supervision authorities designated as competent under the AI Act. The Commission confirmed that under the AI Act each Member States is free to choose the market surveillance authorities for the enforcement of the AI Act which authorities could be different from the data protection authorities.

## PART 3 – Regulatory sandboxes

***Question 5****: How can the AI regulatory sandboxes be implemented in a way that enables collaboration between the AI Act market surveillance authorities and data protection supervisory authorities to bring legal certainty and support AI innovation?*

### *1) Involving relevant national authorities in the establishment of sandboxes*

Member States indicated that the success of regulatory sandboxes depends on the active involvement of both DPAs and MSAs in the creation and management of these sandboxes. Early involvement can help provide clear regulatory guidance and reduce the risk of future non-compliance. Some also suggested involving additional relevant stakeholders, or additionally establishing sectoral sandboxes, dedicated to specific sectors (e.g. healthcare).

Member States also provided **update on the process of establishing such sandboxes**.[1] While some already launched the AI regulatory sandboxes, most Member States are either in the development or preparatory stages of launching such sandboxes. Some Member States referred to experiences with establishing regulatory sandboxes in other domains (like fintech).

For AI regulatory sandboxes, it is essential to **adopt an integrated supervision model**. Firstly, a **national cooperation mechanism** should be established, ensuring that DPAs participate in the testing process from the earliest stage, including in the development of the sandbox plan. This will allow participating entities to obtain clear and early regulatory guidance, reducing the risk of future non-compliance. In addition, **regulatory assessment procedures in the AI sandboxes** could be developed, allowing the impact assessments required by both the AI Act and the GDPR to be harmonised under the guidance and supervision of the relevant market

[1] In line with Article 57(1) of the AI Act, Member States shall ensure that their competent authorities establish at least one AI regulatory sandbox at national level, which shall be operational by 2 August 2026.

surveillance and data protection authorities, minimising administrative burdens, fostering innovation and promoting greater predictability for innovators.

Some Member States also underlined that the creation of a regulatory sandbox requires the use of significant resources.

### *2) Implementing AI sandboxes in accordance with Article 57 (10) of the AI Act*

Member States highlighted it is essential that implementation follows the rules set out in Article 57(10) of the AI Act. This ensures that if innovative AI systems involve personal data or fall under the oversight of additional supervisory regimes, the relevant national data protection authorities will be actively engaged in the sandbox's operation and supervision. This integrated supervision model is intended to provide regulators with early insights into potential compliance challenges, balancing the promotion of innovation with regulatory oversight.

### *3) Offering expertise and guidance*

According to some Member States regulatory sandboxes should provide free access to expertise and guidance on the current legal framework. If needed, other sectoral authorities should also contribute (e.g. in relation to health legislation). This approach would help ensure that participants receive the support needed to navigate the complex regulatory environment. While flexibility is important to accommodate varying needs, the availability of expert guidance remains a critical component.

### *4) Ensuring operational conditions*

Member States stressed that it is crucial to clearly define the operational conditions for sandboxes. AI systems tested in the sandboxes will have an impact on critical infrastructures and digital services, where data protection and cybersecurity are essential. Therefore, the conditions for the AI regulatory sandboxes must be as clear as possible before they are operational. It must be ensured that when tests in the regulatory sandboxes are carried out **under real world conditions**, the safeguards in the AI Act apply and that they incorporate privacy by design measures, guaranteeing that the GDPR is respected in the development phase of AI systems.

### *5) Including mandatory transparency measures*

It has been pointed out by many Member States that the AI regulatory sandboxes should include mandatory transparency measures. AI system providers or prospective providers participating in these environments should be required to document their testing processes and impact assessments, while also maintaining a clear record of algorithmic modifications and compliance measures taken throughout the development phase. Additionally, a summary of each sandbox project, its objectives and expected results should be made publicly available (Article 59(j) of the AI Act), maintaining transparency while also safeguarding commercially sensitive information.

### *6) EU guidelines on sandboxes and other EU level cooperation efforts*

Some Member States recalled that Article 58(1) of the AI Act also requires the Commission to **adopt implementing acts** specifying the detailed arrangements for the establishment, development, implementation, operation and supervision of AI regulatory sandboxes. Moreover, the creation of **joint guidelines** by the AI Office and the European Data Protection Board (EDPB) could help streamline compliance efforts between the AI Act and the GDPR, ensuring that sandboxes promote innovation without compromising the level of protection of fundamental rights.

In addition, **a common digital platform for sandboxes** could facilitate cooperation between national regulators, enabling the sharing of best practices and joint supervision tools, in full respect of each one's remit. The implementation of AI regulatory sandboxes should emphasize integrated collaboration between AI market surveillance and data protection supervisory authorities.

**Transparency through regular publication of sandbox insights, case studies, and success stories** could further assist organizations in understanding compliance requirements, thereby promoting responsible AI innovation.

Some Member States also suggested **closer cooperation within the AI Board subgroup on regulatory sandboxes** where Member States have the opportunity to discuss these issues. Ensuring uniform enforcement across all EU Member States is essential to avoid regulatory fragmentation.

### *Final remark*

By preparing this report Presidency hopes to contribute to the Member States and the European Commission's common efforts to provide clear guidance on the AI Act's application particularly within the context of the GDPR.

The Presidency is convinced that sharing lessons learnt from the current implementation phase and identifying further measures to overcome challenges in the implementation process are essential to facilitate a smooth and simple application of the AI Act. Identifying where regulatory uncertainty creates obstacles to the development and adoption of AI and how the Commission and Member States can support stakeholders better is of key importance if the Union is to turn the concept of Europe as an AI Continent into a reality.