ASK·Q

A GAME CHANGER FOR
IN-HOUSE LEGAL TEAMS

AI Act and GDPR: Birds of a feather flock together

WHITE PAPER

Laurine Delforge

DATA PROTECTION LAB LEAD

Hi there,

In recent years, AI technologies have exploded, transforming industries and changing how we collect, process, and use data. But with this rapid growth comes a new set of challenges around data privacy, transparency, and accountability.

This white paper is here to cut through the complexity, giving you a straightforward look at data protection and the ins and outs of developing and implementing AI systems. We break down the relationship between the GDPR and the AI Act, showing how they work together to ensure that personal data in AI systems is processed legally, fairly, and transparently.

This is the second in a series of five white papers, created to help you navigate data protection regulations that can sometimes feel overwhelming. Our aim is to simplify this complexity, making it straightforward for you to understand and apply these regulations in your work. With our practical GDPR roadmap, we take the hassle out of compliance, so you can focus on what you do best.

Enjoy the read,

Laurine

This white paper will help you understand the interplay between the AI Act and the GDPR and make you reflect on how the things you already do in your role as DPO or Compliance Officer can be translated into AI Act compliance.

Takeaways:

- Alignment of AI Act and GDPR: The EU AI Act and the GDPR aim to protect individuals' rights and privacy. While the GDPR focuses on personal data protection, the AI Act regulates the broader use of AI, especially for high-risk AI systems.
- Both require assessments (DPIA, CA and FRIA) for systems processing personal data and emphasize transparency and reporting obligations.
- Compliance for High-Risk AI Systems: High-risk AI systems must undergo a Conformity Assessment (CA) before entering the market and, in some cases, a Fundamental Rights Impact Assessment (FRIA) before being deployed, ensuring they meet safety and transparency requirements. A Data Protection Impact Assessment (DPIA) is also required if personal data is involved, aligning these obligations with GDPR requirements.

An Information Note For Compliance Officers and DPOs:

The EU Artificial Intelligence Act (AI Act) is a comprehensive legal framework that regulates the development, deployment, and use of artificial intelligence (AI) within the European Union. The AI Act's uniqueness is its risk-based tier-system approach, which ensures that AI systems are used to protect the end-user's fundamental rights and safety. The AI Act categorizes AI systems into different risk levels, each with corresponding obligations for each category of stakeholders (providers, deployers, distributors, and importers of AI systems).

The AI Act is designed to complement the GDPR. While the GDPR focuses on protecting personal data, the AI Act addresses broader concerns about the safe and ethical use of AI systems. The AI Act establishes specific rules for high-risk AI systems, including those involving the processing of personal data.

Many have already noticed the similarities between the AI Act and the GDPR. Both require an EU representative in case the operations are not conducted in the EU, incidents need to be recorded and reported, and technology that can result in a risk to people's rights and freedoms needs to be assessed.

This white paper will help you understand the interplay between the AI Act and the GDPR and make you reflect on how the things you already do in your role as DPO or Compliance Officer can be translated into AI Act compliance.

AI Conformity Assessment and FRIA: DPIA 2.0?

Before a high-risk AI system can be brought to market, a Conformity Assessment (CA) is required to ensure compliance with the AI Act. This mandatory assessment must be carried out by the AI provider (or a 'notified body') and approved by a regulatory authority before the system's market launch. On the other hand, although required by the GDPR, DPIA is not checked by default by a Data Protection Authority and is conducted solely at the discretion of the data controller.

The provider, intending to market the high-risk AI system, is responsible for performing the CA. This includes evaluating whether the system meets the AI Act's requirements, which cover aspects such as data quality, technical documentation, and transparency.

The CA must be conducted before the AI system is introduced to the EU market or put into service. Significant modifications to the AI system also necessitate an updated CA. In this regard, it is pretty similar to the DPIA: it should also be conducted before the processing of personal data takes place and must also be re-evaluated once there are significant changes to this processing.

Both assessments involve evaluating risks associated with high-risk AI systems that process personal data. The CA can form the foundation for the DPIA and vice versa, especially if the provider also acts as the controller. This alignment ensures that both assessments reinforce each other, promoting compliance and risk mitigation. Many examples can be given of when both of these assessments would need to be performed: AI systems used in employment or education contexts, connected medical devices, automated border control, and administration of justice.

While the CA obligation only applies to providers of AI systems, which is a relatively limited number of companies, carrying out a Fundamental Rights Impact Assessment will be an obligation of deployers. It is safe to assume that many entities will be (and already are) acting as deployers of AI systems.

FRIAs must be conducted before deploying a high-risk AI system. Although the AI Act does not specify a set procedure for conducting a FRIA, it requires deployers to assess various elements, such as the AI system's purpose and usage, affected individuals, potential risks, human oversight measures, and internal governance structures.

A FRIA complements DPIAs under the GDPR, although it addresses additional requirements specific to the AI Act.

Transparency is critical to success

The AI Act introduces measures to ensure transparency and disclosure, mainly when AI systems interact with individuals or process their personal data. The transparency requirements align closely with the GDPR's emphasis on data subject rights and the principles of transparency, fairness, and accountability.

A core component of the AI Act is the obligation to notify individuals when interacting with an AI system, especially when the presence of AI is not immediately apparent to the user. This ensures that users are aware of the nature of their interaction and can make informed decisions about their engagement with the system. For instance, situations are common when consumers chat with customer support on a website, and only after minutes of receiving unhelpful, repetitive answers do they realize that they have not been talking to a human this whole time and would have been helped faster if they had called the helpline.

> **“While the AI Act requires that individuals are informed about their interaction with AI and the system’s capabilities, the detailed obligation to notify users about the specific purposes of data processing still comes from GDPR.”**

This transparency requirement reflects the GDPR's principles by ensuring individuals retain control over their personal data and are fully informed about its use. The GDPR mandates that data controllers provide clear and accessible information about data processing activities, including the controller's identity, processing purposes, and the data subjects' rights. The AI Act builds on these principles by adding specific obligations for AI systems, thereby enhancing the overall framework for data protection and user rights in the context of AI.

Personal Data Protection in Regulatory Sandboxes

Regulatory sandboxes play a critical role in balancing innovation with compliance.

> **“By operating within these controlled settings, developers can test AI systems in real-world scenarios before being placed on the market while adhering to stringent data protection regulations and receiving guidance and support from the competent authority.”**

This is particularly important when personal data is involved, as it allows for the development of AI systems that respect individuals' privacy and data protection rights from the outset – a concept similar to the GDPR's ‘data protection by design’, by which companies are required to implement technical and organizational measures which guarantee the protection of personal data from the initial phase of the design of a data processing activity.

A vital aspect of these sandboxes is the involvement of national data protection authorities (DPAs). The AI Act mandates that DPAs oversee sandbox activities to ensure that any processing of personal data is done in compliance with GDPR principles. This includes ensuring that data processing activities are transparent, that consent is obtained where necessary, and that data minimization principles are strictly followed. Data minimization requires only the data essential for the AI system's function to be collected and processed, thereby reducing the risk of unnecessary data exposure.

Incident Reporting

The processes for reporting an AI incident under the AI Act and a data breach under the GDPR share several similarities.

> **“They reflect a common underlying goal of protecting individuals' rights and maintaining trust in digital systems.”**

Both frameworks emphasize timely notification, thorough documentation, and accountability.

The AI Act and the GDPR require that incidents be reported promptly to relevant authorities. Under the GDPR, data breaches that risk individuals' rights and freedoms must be reported to the supervisory authority within 72 hours of becoming aware of the breach. Similarly, the AI Act mandates that incidents involving high-risk AI systems be reported immediately to the appropriate regulatory body (and, in any case, no later than 15 days after the provider became aware of the incident).

Documentation plays a critical role in both AI incident and data breach reporting. The GDPR requires organizations to document all data breaches, regardless of whether they need to be reported to the supervisory authority, including details of the breach, its impact, and the remedial actions taken. Comprehensive record-keeping of AI incidents, detailing the nature of the incident, the AI system involved, the impact on individuals, and the steps taken to address the issue, can help authorities understand the scope and implications of the incident and ensure accountability.

Conclusion

Undoubtedly, the AI Act and GDPR serve complementary purposes in regulating AI systems and data protection. High-risk AI systems require a mandatory CA before market entry, and if personal data is processed, a DPIA is also necessary. This dual requirement ensures robust protection of individuals' rights and fosters a comprehensive regulatory environment for AI technologies within the EU.

Need help navigating this new and exciting regulatory landscape? Contact Ask Q to chat with our AI and data protection experts—together, we can find an efficient and practical solution for your business!

Unlock the knowledge of Ask Q.

WWW.LETSASKQ.COM

Get in touch

laurine.delforge@letsaskq.com

Love them or hate them, the GDPR and other data protection laws are here to stay. We're there to help legal teams tackle the huge volume of work and bottlenecks in compliance workstreams.

VISIT:

https://letsaskq.com/data-protection-lab

ASK Q

A GAME CHANGER FOR
IN-HOUSE LEGAL TEAMS