IP, IT, DATA PROTECTION
European Service Line

ANDERSEN

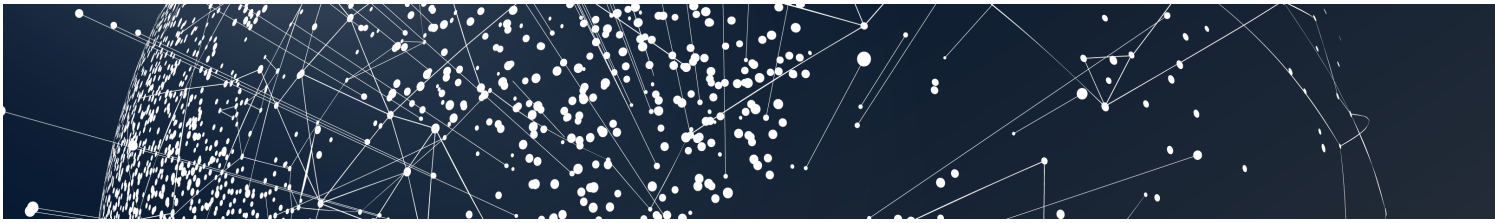
EU Artificial Intelligence Act: Key Considerations for Data Protection Officers

> According to Article 4 of the AI Act, providers and deployers of AI systems shall take measures to ensure a sufficient level of AI literacy for their staff and other persons dealing with the operation and use of AI systems on their behalf.

Paraphrasing the words of European Commission officials, it is the first time that the need to regulate the use of a technology emerges. The complex text of the proposed EU Regulation on Artificial Intelligence ("AI Act") vividly reflects the challenges of regulating a -currently developing- technology with untapped potential. With the AI Act anticipated to become an official legal text soon, the exploration of the challenges it will pose gradually unfolds.

The relationship between Artificial Intelligence and personal data is undoubtedly a major topic these days. As elucidated in Article 2, as well as, indicatively, recitals number 10, 27, and 45, of the newly introduced AI Act, both EU and national laws concerning the protection of personal data and the confidentiality of communications remain applicable, as more specific sets of rules; thus, the respective obligations they create remain in force.

In view of the challenges posed by the use of AI systems, the AI Act goes a step further and introduces a number of new obligations aimed at safeguarding the processing of any personal data. The designated Data Protection Officer ("DPO") within an entity must ensure adherence to these obligations. Notably, the following aim to shed light on their significance, as well as their impact with regard to data protection measures:



Data Protection by design and by default

The assurance of privacy rights and personal data protection remains paramount throughout the entire lifecycle of an AI system. Article 10 of the AI Act specifies that data governance and management practices suitable for the specific purpose of each high-risk AI system must govern the training, validation, and testing of datasets. Thus, the active involvement of the DPO in this process is deemed crucial to upholding these standards.

Drafting of policies, procedures and instructions

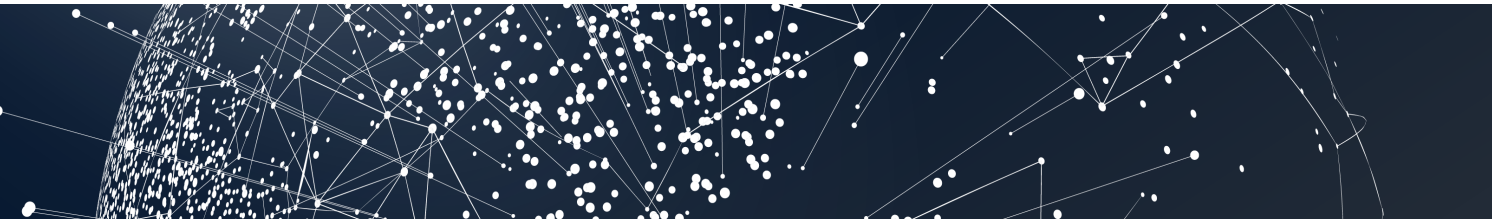
Providers of high-risk AI systems are required to implement a quality management system (Article 17), so that they can ensure compliance with the AI Act. This system must be documented in detail through written policies, procedures, and instructions. The provider's DPO should be actively involved in drafting this documentation, as the later shall -among others- incorporate provisions governing data management, and the protocols for the communication with the competent National Data Protection Authority (NDPA). Additionally, this documentation must be kept for a period ending 10 years after the AI system has been on the market or into service, in case the national competent authorities need to be informed (Article 18).

Information to the deployers

The term 'deployer' refers to the natural or legal person, public authority, agency, or other body using an AI system under its authority, during its professional activities. The AI Act aligns with the fundamental principles of the General Data Protection Regulation ("GDPR") concerning transparency and the provision of information to data subjects about the processing of their personal data. The AI Act stipulates that providers shall give to deployers precise information and instructions, encompassing details such as specifications for input data and any other pertinent information related to training, validation, and testing of the datasets utilized, all while considering the intended purpose of the AI system (Articles 13, 50 etc.). The provider's DPO should ensure that the deployers are properly and fully informed in accordance with the GDPR.

Participation in the staff's training

According to Article 4 of the AI Act, providers and deployers of AI systems shall take measures to ensure a sufficient level of AI literacy for their staff and other persons



dealing with the operation and use of AI systems on their behalf. It is obvious that this AI training should focus, among others, on the protection of personal data and on means and methods to ensure the highest possible level of protection when using AI systems, adding to the DPO's pertinent obligations pursuant to the GDPR.

Notifications to the competent National Data Protection Authority (NDPA)

The AI Act provides for the obligation of notifying the competent NDPA in a series of cases, such as the use of a "real-time" remote biometric identification system in publicly accessible spaces (Article 5 paragraph 4), as well as in the case of a post-remote biometric identification system during the targeted research of a person convicted or suspected of having committed a criminal offence (Article 26 paragraph 10). The DPO should ensure that the competent NDPA is promptly and fully informed in such cases, where required.

Evaluation of the risks for personal data

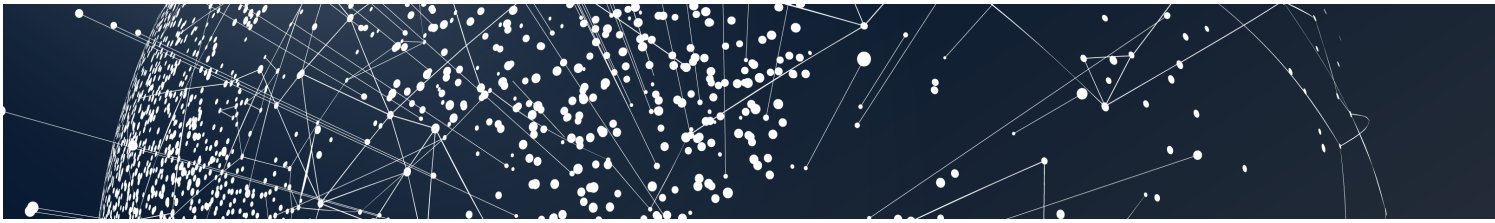
Pursuant to Article 9 of the AI Act, a risk management system (RMS) shall be established, implemented, documented and maintained by providers in relation to high-risk AI systems. One of the main steps to be followed for the creation and use of the RMS is the evaluation of the possible risks, based on the analysis of data gathered from the post-market monitoring system, as clarified in Article 72.

Carrying out Data Protection Impact Assessments (DPIAs)

According to Article 26 paragraph 9 of the AI Act, deployers of high-risk AI systems shall use the information provided to them for transparency reasons to comply with their obligation to carry out a DPIA under Article 35 of the GDPR, where applicable. The deployers' DPOs should therefore assess the obligation to carry out a DPIA each time and undertake to carry it out where required. Moreover, the AI Act introduces an obligation to carry out a fundamental rights impact assessment (Article 27), providing that where a DPIA has been carried out, it has to be complemented by the required content of this fundamental rights impact assessment.

Participation in the development of AI systems in the AI regulatory sandbox

Another innovation introduced by the AI Act is the concept of AI regulatory sandboxes (Article 57), which provide a controlled environment that promotes innovation and



facilitates the development, training, testing and validation of innovative AI systems for a limited period of time before they are placed on the market or put into operation.

Under said article, personal data lawfully collected for other purposes may be processed solely for the purposes of developing, training, and testing certain AI systems in the public interest under certain conditions. Within such context and in light of point 1 ("Data Protection by design and by default"), the DPO's participation is indispensable, so that full compliance with the requirements set, not only by the AI Act, but also by EU legislation, is ensured.

Reporting of serious incidents

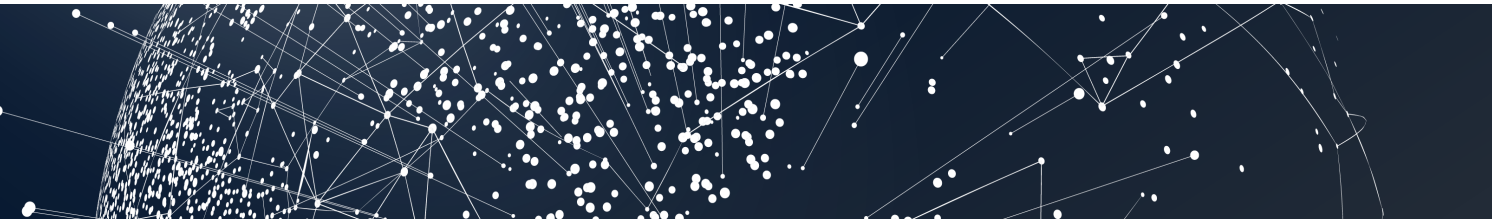
As per the AI Act, a "serious incident" refers to any occurrence or malfunctioning of an AI system that results, directly or indirectly, in a violation of obligations outlined in Union law designed to safeguard fundamental rights, such as the right to privacy and personal data protection. Any serious incidents must be promptly reported to the market surveillance authorities of the Member States where the incidents occurred (Article 73). Consequently, if the serious incident involves a breach of the right to privacy and personal data, it is imperative for the DPO of the high-risk AI system provider to be involved in the procedure for the lawful disclosure of the incident to the competent authorities and overall compliance with data protection legislation.

Reviewing whether an AI Practice is prohibited

Article 5 of the AI Act lists the cases of prohibited AI Practices. These include practices forbidden, due to the excessive processing of biometric data that they perform. In the event that an AI system involves processing of personal data that may be considered unlawful under both the AI Act and the GDPR, the DPO's insight, contribution, and subsequent guidance to ensure the lawfulness of the processing in question are required.

Testing in real world conditions outside AI regulatory sandboxes

Article 60 of the AI Act provides for the possibility to test high-risk AI systems under real-life conditions outside the above-mentioned regulatory sandboxes, provided that certain strict conditions are met. One of these conditions is to properly inform the data subjects, in accordance with Article 61, and obtain their informed consent. It is also stipulated that those subjects should be given the possibility to withdraw their



consent, without any harm and without having to provide any justification, as well as the possibility to permanently delete their personal data. Of course, similarly to the GDPR, the withdrawal of informed consent does not affect activities already carried out. It is therefore evident that the DPO of any provider wishing to test high-risk AI systems outside of regulatory sandboxes, should ensure that proper informed consent is obtained from the subjects and is properly recorded. Additionally, the DPO will be required to assess and determine specific time periods for the retention of the personal data that will be used during testing, and decide upon their proper and secure deletion, destruction, anonymization or pseudonymization.

In light of the above, it can be assumed that the new legislation's objective is particularly demanding: achieving a delicate balance between, on the one hand, effectively safeguarding the rights and freedoms of citizens and, on the other hand, boosting innovation and investment in the European Union in the important and complex field of AI. In this way, the new AI Act could serve as a means for enhancing safety, transparency, and accountability in the quest for the protection of personal data.

Contact information:

Themistoklis Giannakopoulos |
European IP, IT, Data Protection Service Line Coordinator
Andersen Legal in Greece
themistoklis.giannakopoulos@gr.AndersenLegal.com

Alexandra Athitaki | Junior Associate
Andersen Legal in Greece
alexandra.athitaki@gr.AndersenLegal.com