Published November 2024

iapp

Leveraging GDPR compliance

By Nils Hullen

The EU AI Act mentions the EU General Data Protection Regulation, Regulation (EU) 2016/679, more than 30 times throughout its recitals and articles, which define the European framework for the development and deployment of high-risk AI systems and general-purpose AI models.

This does not come as a surprise, as many AI models are trained with datasets, including personal data, and most AI systems are used by humans who can be identified by their usernames or other log-in credentials.

In addition, both regulations aim to protect the fundamental rights of individuals and the responsible use of data, as outlined in Recital 10 of the AI Act. The GDPR safeguards the right to the protection of personal data in particular. The AI Act focuses primarily on the health and safety of individuals, as well as other fundamental rights protecting democracy, the rule of law or the environment.

Personal data and AI

The AI Act includes specific rules that cover biometric data, profiling and automated decision-making, which are also within the scope of the GDPR. Furthermore, the AI Act clarifies the GDPR always applies when personal data is processed. These regular processing scenarios are also subject to GDPR rules, when the processing takes place within its territorial scope per Article 2 and when the processed data is personal, meaning it relates to the data subject, an identified or identifiable natural person, per Article 4.

If personal data is used to train an AI model to improve a picture uploaded to an online photo editor, or simply because a user logs onto the AI system with their name and email, the GDPR rules need to be followed as usual. First and foremost, that means processing personal data requires a legal basis, according to GDPR Article 6. In the context of model training and the deployment of AI systems, there are three main legal grounds to consider: the legitimate interests pursued by the controller or by a third party, contractual necessity, and the data subject's consent. Also, other legal grounds can justify processing personal data in specific circumstances, such as when the "vital interests" of a data subject are protected in emergency situations.

The AI Act specifically addresses the use of sensitive personal data or "'special categories of personal data," in the language of GDPR Article 9. Article 10 of the AI Act provides legal grounds for processing these special categories of sensitive data, specifically and exclusively for bias detection and correction in relation to high-risk AI systems. However, this exception only applies if certain conditions are met. Among others, the use of other nonsensitive data, including synthetic or anonymized data, is not sufficient to ensure bias is appropriately addressed in high-risk AI systems. The AI Act also requires sensitive personal data used for bias mitigation to be safeguarded by technical measures, including the pseudonymization of sensitive data, to limit the reuse of the data and, more broadly, to enhance security and privacy protection.

Privacy-enhancing technologies are important tools to solve the potential conflict between the GDPR's data minimization principle and the requirement to process large datasets, which can help ensure AI systems make fair and accurate assumptions. Various PETs, including anonymization, synthetic data, federated learning and fully homomorphic encryption, also available as open source or "as a service," can help unlock the value of personal data in the AI context in compliance with the GDPR rules.

Common principles and approaches

The GDPR kicks in only when personal data is processed, regardless of whether AI is involved. In contrast, the AI Act applies irrespective of whether personal or nonpersonal data is used. Nevertheless, both regulations share some common principles and approaches to implementing their respective provisions, and both are are well known to most privacy professionals. Key principles like accountability, fairness, transparency, accuracy, storage limitation, integrity and confidentiality, which are fundamental for processing personal data under Article 5 of the GDPR, are also enshrined in the AI Act and, as such, are not a novelty to companies processing personal information.

Accountability

The GDPR requires organizations processing personal data to fulfill the applicable requirements of the EU data protection framework and to demonstrate their compliance with the law. To fulfill their accountability obligations under Article 30 of the GDPR, controllers and processors of personal data must keep detailed documentation of their respective processing activities and make them available to data protection authorities upon request, among other things. Accountability is also a fundamental principle of the AI Act, incorporated in various provisions. For example, providers of high-risk AI systems are responsible for ensuring their products adhere to the relevant provisions of the AI Act and for documenting their compliance in "a systematic and orderly manner, in written policies, procedures and instructions" per AI Act Article 17. Furthermore, they are required to keep various technical and organizational documents updated and at hand for requests by authorities per Article 18.

Fairness

Fairness, and with it, nondiscrimination, is one of the fundamental AI ethics principles incorporated into Recital 27 of the AI Act. It is reflected by the obligations of providers to test high-risk AI systems in Article 9, examine datasets for possible biases in Article 10, ensure high-risk AI systems meet an adequate level of accuracy in Article 15 and take corrective actions if necessary in Article 20. Correspondingly, per Article 26, deployers of high-risk AI systems must ensure input data is relevant and sufficiently representative given the intended purpose of the high-risk AI system. They need to ensure they do not over-rely on the output produced by the AI system — automation bias — and conduct, in some instances, fundamental rights impact assessments per Article 27 to avoid unfair decisions involving AI systems in high-risk use cases. Within the realm of the GDPR, fairness, along with lawfulness and transparency, is one of the guiding principles for data processing. It is enshrined in information requirements in GDPR Articles 12-14 and in data subject rights, such as the right to rectify inaccurate data in Article 16 and the right not to be subject to automated decision-making in Article 22.

Human oversight

Human oversight is also one of the fundamental principles of AI ethics and a specific requirement of the AI Act. According to Article 14, high-risk AI systems must be designed to be effectively overseen by "natural persons," i.e., humans. This corresponds with the obligation of the organization deploying the system to assign human oversight to a person who has the competence, training and authority to fulfill this task, as well as the necessary organizational support as outlined in Article 26. This aspect is not new for privacy pros. Under Articles 37-39 of the GDPR, controllers and processors may need to appoint data processing officers. These are dedicated and skilled people with access to sufficient resources who oversee the data processing activities within the organization. Also, if individuals are subject to decisions based solely on automated processing that produce legal effects or similarly significantly affect them, they have the right to contest the decision and to obtain human intervention and oversight from the data controller per GDPR Article 22.

Data subject and AI Act rights

Handling data subject rights requests is an essential part of any privacy compliance program. For example, under the GDPR, data controllers must inform data subjects about the personal data they process, correct and delete data if necessary, or provide them with a copy of the data to transfer them to another controller. All data subject rights apply when personal information is processed in the context of an AI system. Article 85 of the AI Act establishes only a few specific rights related to the nature of product safety law, such as the right for any natural or legal person to lodge a complaint with a market surveillance authority. Downstream providers using general-purpose AI models can lodge a complaint with the European Commission's AI office, which monitors compliance with the rules for such AI models, per Article 89. And, last but not least, AI Act Article 86 contains the right of explanation to individual decision-making. This right only applies to certain high-risk AI use cases. Hence, it is narrower than the comparable data subject right enshrined in Article 22 of the GDPR. It only applies to the extent that the right is not otherwise provided for under European law, including the GDPR.

Impact Assessments

Privacy pros are familiar with privacy impact assessments or, in terms of GDPR Article 35, data protection impact assessments. The AI

Act implements a similar instrument, the fundamental rights impact assessment, in Article 27. The FRIA is limited to specific high-risk AI use cases, such as when public sector entities plan to deploy high-risk AI systems or when AI systems are used to evaluate a person's creditworthiness. Nevertheless, the underlying principle is similar to the DPIA. Hence, the AI Act specifically states the DPIA required by the GDPR can serve as a basis and can be complemented by additional AI-related aspects, which would result in the required FRIA.

Breach and incident notifications

Last but not least, breach notifications are part of any privacy management system to ensure personal data breaches are reported to DPAs within 72 hours, per Article 33 of the GDPR. Following a similar mechanism, details like timelines vary, so providers of high-risk AI systems must report serious incidents to the market surveillance authorities. Providers must implement a communication and investigation process in either case to report data breaches or AI incidents to the competent authorities.

AI and privacy compliance approaches

Compliance with privacy laws requires a systematic approach that stretches across all levels of an organization, large or small. With the applicability of the GDPR and other similar privacy laws, many companies implemented global privacy management systems to cope with the rapidly expanding regulatory landscape and the increasing amount of personal and nonpersonal data utilized in a business context. In many cases, an existing privacy management or, more broadly, a governance, risk and compliance system is the ideal starting point to tackle the AI-related requirements stemming from the AI Act and the other AI-adjacent laws that will emerge over the coming months and years.

A core element of each privacy management system is an inventory of data processing activities, flows and applications using personal data. Organizations can leverage this inventory to include AI models, applications and the data used to develop and operate AI systems. Such an integrated governance system can capture, integrate and make transparent the metadata related to the entire AI life cycle from design to deployment to everyday use, as well as assess and monitor the risks related to the processing of sensitive personal data and the specific risks associated with AI models, such as general purpose AI models with systemic risks, per AI Act Article 51, or high-risk AI systems.

Privacy management systems are often the gateway to relevant documents, such as data processing agreements, vendor contracts, consent forms, records of processing activities and other key performance indicators, like the number of registered inventory assets, response time to data subject requests, number of DPIAs or privacy training completion rates.

For compliance with the AI Act, and AI governance in general, these features can also be used to help create AI fact sheets, establish user information, or collect and analyze the behavior of AI systems, providing relevant information and KPIs in dashboard views.

While existing privacy management approaches are a good starting place, AI governance has unique challenges. The interplay between personal and nonpersonal data, AI models and AI systems is much more dynamic and complex compared to the normal privacy environment. Also, the deep technical expertise of data engineers and data scientists is required to fulfill certain requirements of the AI Act. Automation is a key component in helping manage that complexity and apply technical skills at scale. AI and data governance platforms can provide the tools needed for an integrated and continuous compliance approach, which supports organizations in coping with the plethora of new privacy, data governance and AI regulations, such as the AI Act.

Contact

Joe Jones
Director of Research and Insights, IAPP
jjones@iapp.org

For further inquiries, please reach out to research@iapp.org.

Follow the IAPP on social media

Published November 2024.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this document, including any warranties of accuracy, merchantability, or fitness for a particular purpose. Nothing herein should be construed as legal advice.