From Data to Algorithms: The Evolution of Individual Rights in the AI Era

Six years after GDPR transformed data protection, artificial intelligence has emerged as the next frontier requiring regulatory intervention. Enter the AI Act - the world's first comprehensive AI legislation - designed to ensure AI systems respect fundamental rights, human dignity and public safety. But here's the challenge: these two regulatory giants now operate side by side, creating a complex compliance landscape for businesses and new protection paradigms for individuals.

Reality is nuanced. While GDPR focuses on human-centered data protection and the AI Act operates as product safety regulation, they frequently overlap through the "dual compliance principle". When AI systems process personal data—which many do—AI providers and deployers must navigate both frameworks simultaneously. Yet not all AI systems trigger both regulations; some process no personal data at all, while others may handle personal data but still qualify as minimal-risk systems under the AI Act's risk-based approach.

Despite their different approaches, both regulations share a common mission: protecting individual autonomy against unauthorized data processing, while ensuring technology serves humanity, not the reverse. Crucially, when both apply, AI providers often become data controllers under GDPR, creating overlapping responsibilities that demand careful coordination.

Hereinbelow, the core individual's rights, that are recognized both under GDPR and AI Act, are outlined.

Decision making – Participation of the individual

Both legal instruments converge on a shared objective: ensuring human involvement and control over automated decision-making processes. Article 22 of the GDPR establishes an individual's right not to be subject to decisions based solely on automated processing and/or profiling (subject to limited exceptions, including fulfillment of contractual obligations or prior explicit consent), where such decisions produce legal or otherwise significant effects. The data controller must ensure that the data subject can obtain human intervention and contest the decision.

Under the AI Act, Article 14 – applicable to high-risk AI systems – mandates human oversight and imposes transparency obligations on both providers and deployers to ensure meaningful human interaction. Compliance measures vary depending on factors including the risks posed by each AI system and its level of autonomy, and can be categorized as either built-in measures (integrated by the AI provider before market placement or service deployment, where technically feasible) or deployer-implemented measures (identified by the provider but executed by the deployer, such as training protocols and workflow monitoring).

Notably, while the GDPR confers individually enforceable rights upon each data subject, the AI Act imposes transparency obligations directly on providers and deployers, thus creating an additional protective layer to safeguard human oversight in AI-driven decision-making processes.

Documentation requirements at a proactive level

At the preventive risk management level, both regulations emphasize specific documentation requirements that must be met by data controllers under the GDPR and AI providers under the AI Act to identify and mitigate risks related to personal data and fundamental rights. Under Article 35 of the GDPR, when intended personal data processing entails or could entail high risk to fundamental rights and freedoms (e.g. large-scale data processing or processing of genetic data), data controllers are required to conduct a Data Protection Impact Assessment (DPIA) in advance. DPIAs aim to identify, explain the necessity and proportionality of, mitigate, and address the risks of data processing operations, while data controllers may also consult with the competent supervisory authority when drafting DPIAs.

Article 27 of the AI Act provides for a similar assessment applicable to high-risk AI systems, known as the Fundamental Rights Impact Assessment (FRIA). FRIAs must be carried out by AI providers before a high-risk AI system is placed on the market and used for the first time, and shall identify, evaluate and adopt mitigation measures for potential risks relating primarily to safety, bias, and fairness when using a high-risk AI system.

It is worth noting that these assessment studies are cumulative, but when a high-risk AI system processes personal data, the AI provider may proceed with a single document that qualifies as both a DPIA and FRIA, thus addressing both data privacy and AI-related issues.

Right to be informed – Explanation right of the individual/ Transparency obligations

Article 13 of the GDPR requires that comprehensive information is provided to individuals by the controller when personal data are collected from them. Additionally, data subjects must receive adequate information necessary to ensure fair and transparent personal data processing.

Articles 50 and 86 of the AI Act stipulate that providers of AI systems intended to directly interact with individuals shall ensure that users are informed that they are interacting with an AI system and that AI-generated content is clearly marked as such. Similar obligations apply to deployers, who must also ensure that the decision-making procedure in high-risk AI systems - which produce legal effects or significantly affect individuals - is identifiable and can be communicated to the individual, along with clear explanations of the AI system's exact role in the decision-making process.

Both legal instruments aim to enhance transparency, thereby emphasizing the importance of informing individuals in a clear and adequate manner.

Right to redress/ Right to seek remedy

Both the GDPR and the AI Act provide legal safeguards and redress mechanisms for natural persons. Specifically, without prejudice to the right to seek judicial remedy, Article 77 of the GDPR provides that data subjects may lodge a complaint with the competent supervisory authority - in Greece being the Hellenic Data Protection Authority ('HDPA') - in cases of personal data processing that breaches the GDPR and/ or any other applicable national provision. The HDPA is empowered to impose a wide range of administrative sanctions on data processors or controllers, which vary depending on factors including the nature, gravity and duration of the infringement, the number of affected data subjects, any mitigation measures taken, the categories of personal data affected, and any prior infringements. Such administrative sanctions may include warnings, reprimands, administrative fines, orders to comply, erase personal data or rectify data, and temporary or permanent prohibitions on processing operations.

Article 85 of the AI Act introduces the right to file a complaint with the market surveillance authority when a person has grounds to consider that an infringement of the AI Act has taken place, without prejudice to any other judicial remedies. Greece has not yet designated the competent authority for this purpose. Instead, it has only nominated the Hellenic Data Protection Authority, the Greek Ombudsman, the Hellenic Authority for Communication Security and Privacy and the National Commission for Human Rights as competent authorities to monitor the fundamental rights compliance of high-risk AI systems, but none of these authorities holds the mandate of a market surveillance authority. It can be argued that Article 85 of the AI Act mirrors, to some extent, Article 77 of the GDPR, aiming to strengthen the individual's right to redress, pending, however, the official appointment of the competent authority to handle these complaints.

Divergences – Challenges

Nevertheless, the GDPR empowers individuals with additional enforceable rights that significantly strengthen their position against unauthorized disclosure and processing of personal data. These rights include: (i) the right of access (Article 15), granting individuals the right to access their personal data held by the controller, have their data isolated from other individuals' data, and receive precise information on how and why it is being processed; (ii) the right to rectification (Article 16), enabling individuals to demand that controllers rectify any inaccuracies in their personal data without undue delay; (iii) the right to erasure/right to be forgotten (Article 17), allowing individuals to request deletion of their personal data in specific circumstances, including when the data are no longer necessary for the original purposes, when consent is withdrawn, or when data has been processed unlawfully; and (iv) the right to portability (Article 20), granting individuals the right to receive their personal data in a structured, commonly used, and machine-readable format and to transmit such data to another controller without hindrance.

These rights are directly linked to personal data processing and aim to strengthen the individual's position. The AI Act does not provide the same or similar individual legal safeguards, as its primary focus is oriented toward the safety, transparency, and ethical use of AI systems and models, imposing obligations and requirements on AI providers and deployers regardless of whether they obtain and process personal data. Under the dual compliance principle, individuals retain these rights when an AI system involves personal data processing. However, even in such circumstances, the application of individual rights under Articles 15, 16, 17, and 20 of the GDPR is complex and may face practical obstacles due to the technical and structural characteristics of AI systems. Machine learning mechanisms embedded in AI systems make it extremely complicated for AI providers and deployers to provide sufficient and detailed explanations of how personal data are processed. Furthermore, personal data in AI systems are commonly anonymized, aggregated, or transformed into embeddings, making it difficult—if not impossible—for AI providers and deployers to isolate, remove, or erase specific personal data.

Conclusion

The regulatory landscape for individual protection in the digital age has reached a pivotal moment. While GDPR places the individual at the center of its regulatory framework, conferring direct and enforceable rights over personal data to ensure personal control, the AI Act takes a different approach by primarily regulating the development and use of AI systems to align with legal and ethical standards.

These two regulatory giants don't compete - they complement. Operating in parallel without one legislative instrument being fully embedded within the other, the GDPR and the AI Act already provide a comprehensive protection framework for individuals in the digital environment. When AI systems process personal data, individuals benefit from dual protection: GDPR's robust individual rights and the AI Act's safety and transparency requirements.

Yet the road ahead remains challenging. Significant obstacles persist at both practical and legislative levels in addressing the dynamic nature and technical characteristics of AI systems. The anonymization, aggregation, and transformation of personal data in AI systems create real-world barriers to exercising traditional data protection rights. Machine learning's "black box" nature makes it increasingly difficult to provide the detailed explanations individuals deserve.

The ultimate test lies not in the elegance of these regulations on paper, but in their practical implementation. Ensuring that legislative frameworks remain responsive to the continuous evolution of AI technologies, while protecting fundamental rights, will require ongoing collaboration between regulators, technologists, and legal practitioners. As AI continues to reshape our digital landscape, the success of this dual regulatory approach will determine whether technology truly serves humanity - or the reverse.

The framework exists. Now comes the harder task: making it work in practice.

If you have questions or would like additional information, please contact the author:

Sofrini Sideri, Associate

sofrini.sideri@yourlegalpartners.gr