EU Digital Laws: Mapping the Interplays with the GDPR

Artificial Intelligence Act: EU General Data Protection Regulation

A topical and consequential intersection is between the Artificial Intelligence Act and the EU General Data Protection Regulation. While they both employ risk-based approaches in some form, the laws are built upon different regulatory logics. The AI Act is a product safety regulation that infuses organizational design responsibilities with a concern for individual rights, while the GDPR directly enshrines fundamental human rights related to personal data protection. The AI Act and the GDPR — as well as their interplay — are likely to see changes as a result of the Digital Omnibus. The European Parliament has produced a report on the interplay between the AI Act and the EU digital legislative framework, including its intersections with the GDPR.

AI Act		GDPR
Article 10(5) and Recital 70 Processing of special categories of personal data is permitted under AI Act Article 10(5) insofar as it is "strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems."	Processing special categories of personal data to monitor, detect and correct bias in high-risk AI systems	**Article 9(1-2)** In general, processing of special categories of personal data is prohibited under the GDPR unless an exception applies. AI Act Recital 70 notes that the GDPR Article 9(2)(g) derogation for "substantial public interest" may be relied upon for the processing of special categories of personal data for bias monitoring.
Article 27 Prior to deploying certain high-risk AI systems, certain deployers must perform a fundamental rights impact assessment prior to their first deployment and notify the competent market surveillance authority of its outcome. The FRIA should complement, not replace, any related data protection impact assessments conducted pursuant to the GDPR.	Fundamental rights and data protection impact assessments	**Articles 35** Where processing is likely to result in a high risk to the rights and freedoms of a natural person, data controllers must conduct a data protection impact assessment.
Article 14 High-risk AI systems must be designed and developed in a way that allows for effective human oversight that prevents or minimizes risks to health, safety or fundamental rights.	Human oversight	**Article 22** GDPR Article 22 provides data subjects with the right not to be subject to a decision based solely on automated processing, including profiling.
Article 26(11) Deployers of high-risk AI systems that make decisions or assist in making decisions related to natural persons must inform them that they are subject to the use of the high-risk AI system.	Transparency	**Articles 13-14, 15(1)(h) and 22** GDPR Articles 13 and 14 require controllers to inform data subjects about the collection and use of their personal data and their rights as data subjects, while Article 15(1)(h) provides data subjects with the right to "meaningful information" about automated decision-making they are subject to under Article 22.
Articles 11-12 and 26(6) AI Act Article 12 mandates that providers of high-risk systems ensure automatic logging; Article 11 requires comprehensive technical documentation to demonstrate conformity. Article 26(6) requires deployers to retain records of use.	Traceability	**Article 30** In mirroring obligations, GDPR Article 30 requires controllers and processors to maintain records of processing activities.
Article 15(5) Providers must ensure robustness, accuracy and cybersecurity throughout the life cycle of high-risk AI systems.	Security	**Article 32** Controllers and processors must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
Article 12 and 26(6) Certain obligations under the AI Act, such as recordkeeping to ensure traceability, may entail personal data being captured and retained in logs that complicate the exercisability of data subject rights (e.g., access, rectification, erasure and objection).	Governance for data subject rights	**Articles 15-22** Data subject rights are guaranteed under GDPR Articles 15-22.
Articles 57-59 and Recital 140 Sandbox testing of AI systems permits experimental processing in a controlled environment, but a legal basis for personal data processing under the GDPR must still be identified. Sandboxes may potentially rely on "substantial public interest" for the use of personal data originally collected for other purposes.	AI sandboxes	**Article 9(2)(g)** GDPR obligations (e.g., lawful bases for processing) still apply to AI sandbox testing. Member states may differ in their interpretations of the validity of the reliance on the GDPR Article 9(2)(g) legal basis of "substantial public interest" for AI sandboxing purposes.
Chapter VII The AI Act decentralizes oversight via member state market surveillance authorities and the AI Office. Data protection authorities may be involved in the enforcement of the AI Act in certain circumstances.	Enforcement	**Chapter VI** The GDPR coordinates oversight of cross-border enforcement via the one-stop-shop mechanism and the European Data Protection Board.

Published April 2026.

iapp.org