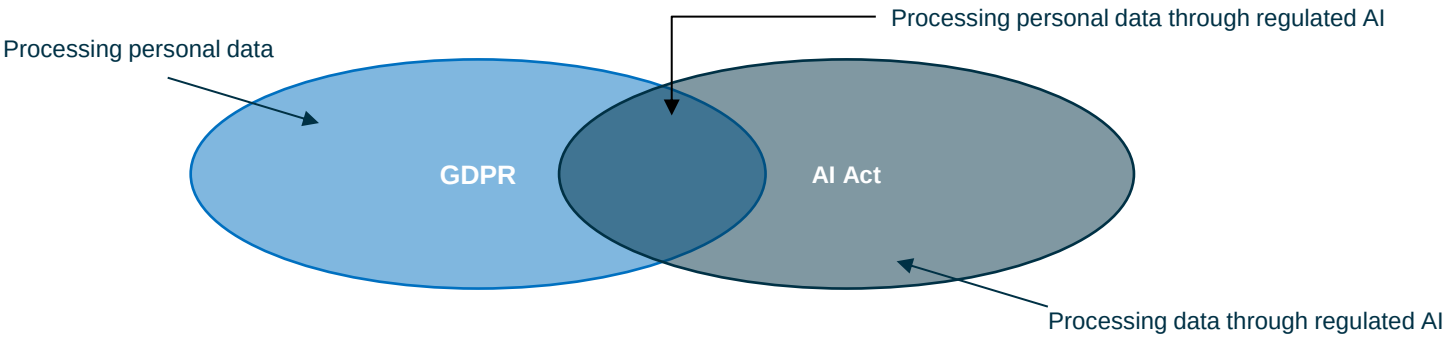
Interplay of the EU AI Act and GDPR

What this document is about

- In certain scenarios, there will be an overlap between the EU Artificial Intelligence Act ("**AI Act**") and the EU General Data Protection Regulation ("**GDPR**") when personal data is processed through regulated AI systems.
- To illustrate such overlaps in these scenarios, the table below gives an overview of the key requirements under the AI Act applicable to **Providers*** and **Deployers***[1] relating to **high-risk AI systems*** and links each of those requirements to a correlating requirement under GDPR.
- This overview shall support organizations to identify synergies through existing processes and protocols that possibly could be leveraged for AI compliance measures, to align internal workstreams, and to enable the internal privacy organization to identify relevant touchpoints with the AI compliance organization.
- This document does not address any interplays of the AI Act with other areas of law, such as product regulator, IP, cyber security, digital regulation, commercial, or labor & employment.

[1] Non-public bodies and institutions only.

Areas of overlap between GDPR and AI Act



Key Definitions

***Provider**	means an organization that develops an AI system (or has an AI system developed) and places it on the EU market or puts the AI system into service under its own name or trademark, whether for payment or free of charge
***Deployer**	means and organization using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity
***High-risk AI systems**	may include AI systems intended to be used (i) for emotion recognition, (ii) for recruitment or selection of individuals, in particular to place targeted job advertisements, to analyze and filter job applications, and to evaluate candidates, or (iii) to make decisions affecting employees (e.g., term, termination of employment, promotions, task allocation, performance and behavior evaluation)

Interplay AI Act and GDPR

AI Act Requirements relating to high-risk AI systems	Interplay with GDPR requirements	Responsible actor under the AI Act	
		Provider	Deployer
Extraterritorial application (Art. 2 AI Act): ▪ Providers (irrespective of their place of establishment) placing on the market or putting into service an AI system in the EU ▪ Deployers with place of establishment in the EU ▪ Providers or Deployers of AI systems where the output of the AI system is used in the EU	▪ Extraterritorial application (Art. 3 GDPR)	●	●
AI literacy (Art. 4 AI Act) ▪ Ensure a sufficient level of AI literacy of staff and service providers dealing with the development, operation and use of AI systems	▪ Accountability, Art. 5 (2) GDPR ▪ Organizational measures for compliance, including privacy policies, Art 24 (2) and 32 (4) GDPR ▪ Training by DPO, Art. 39 (1) lit. b) GDPR	●	●
Risk management system (Art. 9 AI Act) ▪ Implement a continuous iterative process for the entire lifecycle of a high-risk AI system to identify risks and to adopt risk management measures	▪ Privacy by design, Art 25 (1) GDPR ▪ Data protection impact assessment, Art. 35 GDPR	●	
Data and Data Governance (Art. 10, 26 (3) AI Act) ▪ Training, validation and testing data: consider original purpose of personal data collection; ensure relevant and sufficiently representative data ▪ Input data: ensure relevant and sufficiently representative input data	▪ Fair processing, Art. 5 (1) a) GDPR ▪ Purpose limitation, Art. 5 (1) b) GDPR ▪ Adequate, relevant and limited data (data minimization), Art. 5 (1) c) GDPR ▪ Accurate and up-to-date data (accuracy), Art. 5 (1) d) GDPR ▪ Legal basis in Art. 10 (5) AI Act for the processing of sensitive data for training purposes	●	●

AI Act Requirements relating to high-risk AI systems	Interplay with GDPR requirements	Responsible actor under the AI Act	
		Provider	Deployer
Transparency towards deployer (Art. 13 AI Act) ▪ Provide instructions to Deployer with information on characteristics, capabilities and limitations of performance, any known or foreseeable circumstances which may lead to risks or misuse, guidance on the interpretation of output, human oversight measures etc.	▪ Deployer to use such information for DPIAs (Art. 26 (9) AI Act and 35 GDPR)	●	
Transparency towards affected individuals (Art. 50, 26 (11), 86 AI Act) ▪ Providers of AI systems intended to interact directly with individuals shall inform individuals that they interact with an AI system; ▪ Mark AI-generated synthetic content as AI generated; ▪ Deployers to identify deep fakes and text generated by AI system (if used to inform the public on matter of public interest); ▪ Deployers of AI systems that make decisions or assist in making decisions related to individuals shall inform the individual that they are subject to the use of an AI system. ▪ Deployers using AI systems for decision-making shall inform the individual about the decision-making process	▪ Transparency, Art 13 and 14 GDPR ▪ Information about automated decision making, Art. 13 (2) f) GDPR	●	●
Human Oversight (Art. 14, 26 AI Act) ▪ Ensure human oversight to prevent or minimize risks	▪ Right of data subject to obtain human intervention in case of automated decision making (Art. 22 GDPR)	●	●

AI Act Requirements relating to high-risk AI systems	Interplay with GDPR requirements	Responsible actor under the AI Act	
		Provider	Deployer
Accuracy, robustness and cybersecurity (Art. 15 AI Act) ▪ Design high-risk AI systems in a way to achieve accuracy, robustness and cybersecurity with consistency and to eliminate biased outputs	▪ Technical and organizational security measures, Art. 24 and 32 GDPR	●	
Quality management system (Art. 17 AI Act) ▪ Ensure compliance with the AI Act through policies, procedures and instructions	▪ Accountability, Art. 5 (2) GDPR ▪ Organizational measures for compliance, including privacy policies, Art 24 (2) and 32 (4) GDPR	●	
Recording of log-files (Art. 12 AI Act) ▪ Automatic recording of events (logs) over the lifetime of the AI system, e.g. each use of the AI system, input data	▪ Accountability, Art. 5 (2) GDPR ▪ Organizational measures for compliance, Art 32 (4) GDPR	●	
Documentation Keeping (Art. 18, 26 AI Act) ▪ Retention requirement of 10 years for documents and records and of 6 months for certain logfile	▪ Accountability, Art. 5 (2) GDPR ▪ Organizational measures for compliance, Art 32 (4) GDPR	●	●
Corrective actions and duty of information (Art. 20, 26 (5) AI Act) ▪ Take necessary corrective actions immediately in case a high-risk AI system is not in conformity with the EU AI Act (including withdrawing, disabling or recalling) and inform other (including potentially the regulator)	▪ Accountability, Art. 5 (2) GDPR ▪ Data protection impact assessment, Art. 35 GDPR ▪ Personal data breach reporting obligation, Art. 33 GDPR	●	●

AI Act Requirements relating to high-risk AI systems	Interplay with GDPR requirements	Responsible actor under the AI Act	
		Provider	Deployer
Post-market monitoring (Art. 72, 26 (5) AI Act) ▪ Establish system to collect and analyze data on the performance of the high-risk AI system to evaluate the continuous compliance with the EU AI Act	▪ Accountability, Art. 5 (2) GDPR ▪ Continuous data protection impact assessment, Art. 35 GDPR	●	●
Reporting of serious incidents (Art. 73, 26 (5) AI Act) ▪ Report serious incidents to regulator immediately (in any event not later than 15 days after becoming aware, in some cases within 2 days)	▪ Personal data breach reporting obligation, Art. 33 and 34 GDPR	●	●
Appointment of representative in the EU (Art. 22 (1) AI Act) ▪ Appoint a representative in the EU if provider is established outside of the EU	▪ GDPR representative, Art. 27 GDPR	●	
Fundamental Rights Impact Assessment (Art 27 AI Act) ▪ Perform fundamental right impact assessment (FRIA) for high-risk AI systems; but only applicable to certain deployers, e.g. bodies governed by public law or private entities providing public services	▪ Data protection impact assessment, Art. 35 GDPR ▪ If any of the obligations under Art. 27 AI Act are already met through a DPIA pursuant to Art. 35 GDPR, the FRIA shall complement the DPIA		●

AI Act Requirements relating to high-risk AI systems	Interplay with GDPR requirements	Responsible actor under the AI Act	
		Provider	Deployer
Technical documentation (Art. 11 AI Act) ▪ Document necessary information to demonstrate compliance with AI Act based on Annex IV of AI Act	▪ Privacy by design, Art. 25 (1) GDPR ▪ Data Protection Impact Assessment, Art. 35 GDPR ▪ Records of Processing, Art. 30 GDPR	●	
TOM to use AI system in accordance with instructions (Art. 26 (1) AI Act) ▪ Implement TOMS to ensure AI system is used in accordance with user instruction of provider	▪ Technical and organizational security measures, Art. 26 and 32 GDPR ▪ Organizational measures for compliance, including privacy policies, Art 24 (2) and 32 (4) GDPR		●
Registration (Art. 49 AI Act) ▪ Registration of Provider in EU database (Art. 71 AI Act) before placing on the market or putting into service an AI system ▪ Registration of Deployers in EU database (Art. 71 AI Act) only relevant for public bodies and other organizations acting on behalf of public bodies	▪ Mandatory registration information of deployer include a summary of the DPIA pursuant to Art. 35 GDPR, where applicable	●	●
Conformity assessments and EU declaration of conformity (Art. 43, 47 AI Act) ▪ Provider to carry out conformity assessment		●	
Cooperation with regulator (Art. 21, 26 (12) AI Act) ▪ Upon request provide information and documentation to regulator to demonstrate compliance	▪ Cooperate with supervisory authority, Art. 31 GDPR	●	●