EU AI Act – obligations on deployers

TaylorWessing

A **deployer** is **"a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity"** (Article 3(4)). Deployers are also included in the definition of "operator" (Article 3(8)). Note that a deployer can also be a provider of a high-risk AI system and subject to the Article 16 obligations where they meet criteria in Article 25(1).

Types of AI systems	Types of duty	Obligations
All AI systems	AI literacy (Article 4)	Deployers must ensure, to their best extent, a suitable level of AI literacy of their staff or anyone dealing with the operation and use of the AI system on their behalf. This will be relative to the technical knowledge, experience, education and training, how the systems are to be used and on whom.
High-risk AI systems	Governance (Article 26)	Deployers must: ■ Take technical and organisational measures to ensure use of systems in line with the provided instructions for use ■ Where the deployer has control over input data, ensure it is relevant and sufficiently representative in view of the intended use of the system ■ Keep automatically generated logs of system use (where under the deployer's control) for a period appropriate to the intended use of the system and for a minimum of six months (or as otherwise specified under applicable law) ■ Co-operate with relevant competent authorities (in addition to the duty set out in Article 79).
	Risk management (Article 26)	Deployers must: ■ Monitor the high-risk AI system and the level of risk it poses. They must inform the provider, distributor and relevant market surveillance authority where use may result in risk to health and safety or fundamental rights without undue delay, in which case they must also suspend use of the system. ■ Report serious incidents to the relevant provider, importer, distributor and market surveillance authority (see Article 73 for details on report) ■ Ensure human oversight by people with necessary training and provide them with support ■ Carry out a Data Protection Impact Assessment when applicable ■ Register in the EU database if required (see Article 49 below).
	Transparency (Article 26)	Deployers must: ■ Inform affected workers and their representatives before using or putting high-risk AI systems into service in the workplace ■ Inform natural persons of the use of high-risk AI in decisions to which they are subject (without prejudice to Article 50).
Annex III high-risk systems (except those used in specified critical infrastructure)	Fundamental Rights Impact Assessments (FRIAs) (Article 27)	Deployers that are bodies governed by public law or private entities providing a public service and deployers of high-risk AI systems used to evaluate financial credit ratings, detect fraud or assess risk and pricing for life and health insurance, must carry out an FRIA. FRIAs must be done prior to first use of the high-risk AI system and kept up to date in the event of changes. The assessment must cover: ■ Descriptions of intended use, intended frequency and time frame of use, affected audience, and any specific risk ■ Human oversight measures implemented in accordance with instructions for use ■ Measures to be taken on materialisation of risk including internal governance and complaint mechanisms. Deployers can rely on DPIAs where and to the extent they cover the required information. The results of the FRIA should be submitted to the market surveillance authority using a standardised template (to be developed by the AI Office), subject to very limited exemptions in Article 46(1).
	Registration (Article 49(3))	If the deployer is or acts on behalf of a public authority or Union institution, it must register itself, the system it is using and its purpose in the relevant EU database and must not use an unregistered AI system (with exceptions provided for high-risk AI systems used in specified types of critical infrastructure).
	Right to an explanation (Article 86)	On request from an individual, deployers must provide a detailed explanation of the role of AI in a decision-making process which has a legal or similarly significant effect on that individual such that it has an adverse impact on their health and safety or fundamental rights. They must also set out the main elements of the decision.
Specified AI systems	Transparency (Article 50)	Deployers of emotion recognition or biometric categorisation systems must inform relevant individuals subject to them and process personal data in accordance with data protection law. Deployers of AI systems creating deepfakes (by manipulating images, sounds or videos) must disclose that the output is the product of an AI system. Deployers must disclose the use of AI to manipulate or generate text developed by an AI system with the purpose of informing the public on matters of public interest. There are limited exemptions for these types of systems when used in law enforcement.
	Restrictions on use of post-biometric identification for law enforcement (Article 26)	Use of post-biometric identification for law enforcement purposes is subject to authorisation requirements and must be targeted. Deployers must submit annual usage reports to the relevant market surveillance and national data protection authorities.
AI systems presenting a risk	Duty to cooperate (Article 79)	All operators (including deployers) have a duty to cooperate with the market surveillance authority and other specified national public authorities or bodies.