



EU AI Act 2024 1689

Artikel 78

IX - 3

Article 78

Confidentiality

1. The Commission, market surveillance authorities and notified bodies and any other natural or legal person involved in the application of this Regulation shall, in accordance with Union or national law, respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:

(a)

the intellectual property rights and confidential business information or trade secrets of a natural or legal person, including source code, except in the cases referred to in Article 5 of Directive (EU) 2016/943 of the European Parliament and of the Council (57);

(b)

the effective implementation of this Regulation, in particular for the purposes of inspections, investigations or audits;

(c)

public and national security interests;

(d)

the conduct of criminal or administrative proceedings;

(e)

information classified pursuant to Union or national law.

2. The authorities involved in the application of this Regulation pursuant to paragraph 1 shall request only data that is strictly necessary for the assessment of the risk posed by AI systems and for the exercise of their powers in accordance with this Regulation and with Regulation (EU) 2019/1020. They shall put in place adequate and effective cybersecurity measures to protect the security and confidentiality of the information and data obtained, and shall delete the data collected as soon as it is no longer needed for the purpose for which it was obtained, in accordance with applicable Union or national law.

3. Without prejudice to paragraphs 1 and 2, information exchanged on a confidential basis between the national competent authorities or between national competent authorities and the Commission shall not be disclosed without prior consultation of the originating national competent authority and the deployer when high-risk AI systems referred to in point 1, 6 or 7 of Annex III are used by law enforcement, border control, immigration or asylum authorities and when such disclosure would jeopardise public and national security interests. This exchange of information shall not cover sensitive operational data in relation to the activities of law enforcement, border control, immigration or asylum authorities.

When the law enforcement, immigration or asylum authorities are providers of high-risk AI systems referred to in point 1, 6 or 7 of Annex III, the technical documentation referred to in Annex IV shall remain within the premises of those authorities. Those authorities shall ensure that the market surveillance authorities referred to in Article 74(8) and (9), as applicable, can, upon request, immediately access the documentation or obtain a copy thereof. Only staff of the market surveillance authority holding the appropriate level of security clearance shall be allowed to access that documentation or any copy thereof.

4. Paragraphs 1, 2 and 3 shall not affect the rights or obligations of the Commission, Member States and their relevant authorities, as well as those of notified bodies, with regard to the exchange of information and the dissemination of warnings, including in the context of cross-border cooperation, nor shall they affect the obligations of the parties concerned to provide information under criminal law of the Member States.

5. The Commission and Member States may exchange, where necessary and in accordance with relevant provisions of international and trade agreements, confidential information with regulatory authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of confidentiality.



[Verify AI Provenance](#)