ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

GDPR –AI Act – CRA

An Overview of Similarities and Differences

Contact
Fraunhofer-Institute for Secure Information Technology SIT
Rheinstr. 75
64295 Darmstadt
Annika.Selzer@sit.fraunhofer.de
0049 6151 869 100
Compiled by: Ceyda Özdemir, Sarah Stummer

The present results were produced within the framework of the Fraunhofer Heilbronn Research and Innovation Center for Cybersecurity, which is funded by the Dieter Schwarz Foundation.

	GDPR	AI Act	CRA
Applicability	The GDPR applies to the processing of personal data by organizations within the EU, as well as through non-EU organizations if they offer goods or services to, or monitor the behavior of, individuals in the EU.	The AI Act applies to the placing on the market, putting into service, and deployment of AI systems in the EU, provided that the output generated by the AI system is used in the EU, regardless of where the provider or deployer is located. The AI Act also applies to the placing on the market of general-purpose AI models in the EU, again regardless of where the provider is located.	The CRA applies to products with digital elements placed on the EU market when their intended or reasonably expected use involves any kind of data connection—direct or indirect, logical or physical—to another device or network. It is applicable from 11th of December 2027.
Principles	The GDPR contains the following principles relating to the processing of personal data: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.	The AI Act does not contain overarching binding principles. However, in the recitals, the AI Act refers to non-binding ethics guidelines for trustworthy AI presented by the High-Level Expert Group appointed by the Commission, including the following principles: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; and accountability.	The CRA does not contain overarching binding principles. However, Annex I includes essential cybersecurity requirements relating to the properties of products with digital elements, including risk-appropriate level of cybersecurity; vulnerability-free provision; secure default configuration and reset option; security updates; protection against unauthorized access; protection of the confidentiality of processed data; protection of the integrity of processed data and notification of its corruption; data minimization; ensuring the availability of essential and basic functions; minimizing negative effects; limited attack surfaces; reducing incident impact; recording and monitoring security-related information; deletion and secure transfer options for users.
Central Roles	Most of the responsibilities under the GDPR apply to the controller, and in some cases (also) to the processor.	The AI Act addresses multiple players along the AI value chain, including the provider, deployer, importer, and distributor. Most of the responsibilities, however, lie with the provider and deployer.	The CRA addresses manufacturers, importers, distributors, and authorized representatives. Most of the responsibilities under the CRA apply to manufacturers.
Rights of data subjects resp. users	The GDPR regulates the following rights of the data subject: the right to information; the right of access; the right to rectification; the right to erasure and 'to be forgotten'; the right to restriction of processing; the right to be notified of data recipients; the right to data portability; the right to object; the right to withdrawal of consent; and the right to lodging a complaint with a supervisory authority.	The AI Act does not contain any intervention rights to users. It only sets transparency requirements for AI systems that interact with natural persons or are designed to generate content.	The CRA does not regulate intervention rights of users. However, by obliging manufacturers to provide information and instructions to the user, it sets out transparency requirements for the placement of digital elements.
Documentation Obligation	The GDPR requires controllers to be able to demonstrate that processing is carried out in accordance with the GDPR, especially in compliance with the principles relating to the processing of personal data. Furthermore, it obliges controllers and processors to maintain records of processing activities.	The AI Act sets out documentation obligations for both high-risk AI systems and general-purpose AI systems, each requiring comprehensive technical documentation. High-risk AI systems must also retain technical logs. Additionally, they must establish a quality management system that includes, among other things, a concept for compliance with regulatory requirements.	The CRA requires manufacturers to provide detailed technical documentation demonstrating compliance with the essential security requirements set out in Annex I. The technical documentation must be continuously kept up to date.
Risk Assessment	When personal data shall be processed, the risks to the rights and freedoms of individuals must be assessed. The risk assessment determines whether an impact assessment must be carried out and what measures must be taken.	For high-risk AI systems, risks to fundamental rights, health, and safety must be assessed. Also, general-purpose AI systems require systemic risk assessment. The risk assessment determines whether an impact assessment must be carried out and what measures must be taken.	Manufacturers must conduct a cybersecurity risk assessment for the product with digital elements. The risk assessment determines what measures need to be taken to meet the cybersecurity requirements set out in Annex I Part 1 CRA.
Impact Assessment	Where a risk assessment results in the processing of personal data being likely to result in a high risk to the rights and freedoms of natural persons, the controller is obliged to carry out a data protection impact assessment prior to the processing.	Where a high-risk AI system is deployed by certain deployers (e.g., bodies governed by public law or private entities providing public services), a fundamental rights impact assessment must be carried out prior to the deployment of the high-risk AI system.	There is no impact assessment regulation under the CRA.

Conformity Assessment	The GDPR allows data protection certification mechanisms to demonstrate compliance.	The AI Act regulates conformity assessment for high-risk AI systems.	Conformity assessment is regulated depending on the classification of the product with a digital element. Different assessment procedures apply depending on whether the product is classified as a standard product, an important product (Class I or II), or a critical product.
Technical Security Measures	The GDPR requires controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks for the rights and freedoms of natural persons.	The AI Act requires providers of high-risk AI systems to implement appropriate technical and organizational measures to ensure robustness, cybersecurity, and a level of risk management proportionate to the impact on health, safety, and fundamental rights.	The CRA requires manufacturers to ensure that their product with digital elements complies with the cybersecurity requirements set out in Annex I. Likewise, distributors and importers must verify such compliance before making the products available on the market/importing the products
Compliance Mechanism	Certification mechanisms and general validity codes of conduct are the tools that allow demonstration of compliance with the GDPR.	Conformity assessment and CE marking are key mechanisms under the AI Act to demonstrate compliance for high-risk AI systems.	Under the CRA, compliance is ensured through conformity assessment – such as CE marking and the EU Cybersecurity Certificate. The specific procedures vary depending on the products' classification as standard, important, or critical products.
Internal Responsible Person	Under certain conditions –e.g., where the core activities consist of processing sensitive data on a large scale – controllers and processors shall designate a data protection officer. The data protection officer monitors compliance with the GDPR and advises the controller.	The AI Act does not establish the obligation to designate an internal responsible person; rather, such an obligation can be derived from Art. 14 GPSR, which stipulates the responsibility of economic operators to ensure that they have an internal process for product safety.	The CRA does not establish the obligation to designate an internal responsible person; rather, such an obligation can be derived from Art. 14 GPSR, which stipulates the responsibility of economic operators to ensure that they have an internal process for product safety.
Reporting Obligation	A data breach that is likely to result in a risk to the rights and freedoms of natural persons must be reported to the competent supervisory authority no later than 72 hours after becoming aware of the data breach.	A serious incident must be reported by providers of high-risk AI systems to the market surveillance authorities of the Member State where the incident occurred, usually no later than 15 days after becoming aware of the incident - with stricter deadlines: 2 days for widespread violations or serious incidents, and 10 days in cases involving death.	An actively exploited vulnerability in a product with digital elements must be reported by the manufacturer to the competent supervisory authority within 24 hours by means of an early warning, followed by a vulnerability notification within 72 hours, and a final report no later than 14 days after corrective or risk-mitigation measures have been made available. A severe incident affecting such a product must be reported to the competent supervisory authority, with an early warning within 24 hours, an incident notification within 72 hours, and a final report within one month. The distributor and importer must immediately inform the manufacturer of any vulnerability and, where the product poses a significant cybersecurity risk, notify the market surveillance authorities.
Forbidden Actions	Processing data without a legal ground regulated under the GDPR is unlawful, and any infringement of the GDPR is prohibited.	Using AI systems that fall under the prohibited practices regulated in Article 5 of the AI Act is unlawful.	The placing on the market of products with digital elements that are not in conformity with the requirements and obligations laid down in the CRA is unlawful.
Authorities	There is a supervisory authority in each Member State monitoring the application of the GDPR.	Each Member State establishes national competent authorities for the purpose of this Regulation. One of these is the notifying authority, which deals with the conformity assessment procedure, and the other is the market surveillance authority, which serves as the single point of contact under the AI Act.	Each Member State shall designate a market surveillance authority to ensure the effective implementation of the CRA. In addition, a notifying authority must be established to coordinate conformity assessment procedures.
Penalties	Some infringements, especially regarding data subjects' rights or data protection principles, may result in a fine of up to EUR 20 million or 4% of global annual turnover, while others may be penalized with a fine of up to EUR 10 million or 2% of global annual turnover.	Non-compliance with the prohibited AI practices can result in fines of up to EUR 35 million or 7% of global annual turnover. Other infringements may lead to penalties of up to EUR 15 million or 3% of global annual turnover, while administrative violations may be fined up to EUR 7.5 million or 1% of global annual turnover.	In the event of non-compliance with essential requirements, fines may reach up to EUR 15 million or 2.5% of global annual turnover. For other obligations, penalties can go up to EUR 10 million or 2% of global annual turnover, while other infringements may be penalized with a fine of up to EUR 5 million or 1% of global annual turnover.