REPORT
Analysis of the relationship between the Artificial Intelligence Act and selected applicable and draft legal regulations

Report prepared by
Working Group on Artificial Intelligence, Subgroup on Ethics and Law

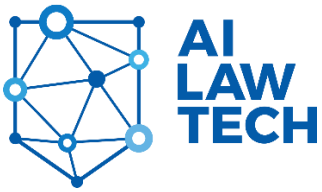
Ministerstwo Cyfryzacji

GRAI
GRUPA ROBOCZA DS. SZTUCZNEJ INTELIGENCJI

THE VIEWS EXPRESSED IN THIS DOCUMENT ARE THOSE OF THE AUTHORS AND DO NOT NECESSARILY REFLECT THE POSITION OF THE POLISH GOVERNMENT

Warsaw, August 2023

Table of contents



Working Group on Artificial Intelligence Ethics and Law

This report was prepared by the Subgroup on Artificial Intelligence Ethics and Law[1] of the Working Group on Artificial Intelligence (GRAI) at the Minister of Digitization.

The primary goal of the subgroup is to support the development of Poland's artificial intelligence ecosystem in the scope of ethics and law.

The sub-working group consists of several dozens of experts specializing in various fields of law, as well as people interested in the ethical dimensions of artificial intelligence. The experts have professional experience from a variety of industries and sectors, including in legal consulting, business sector, government and academia.

The work of the Subgroup on Artificial Intelligence Ethics and Law includes, among others, the following:

- conducting analysis and making recommendations on draft legislation and other documents submitted by the Chancellery of the Prime Minister,
- supporting the evaluation and further development of the Artificial Intelligence Development Policy in Poland,
- conducting analysis and research on legal and ethical aspects of artificial intelligence,
- developing concepts and presenting recommendations on issues related to the development of artificial intelligence, including its legal framework, legislative changes and good practices,
- supporting other working groups.

This report was prepared by the team consisting of:

- Roman Bieda, attorney-at-law
- Michał Chodorek, attorney-at-law
- Witold Chomiczewski, attorney-at-law
- Hanna Jankowska, attorney-at-law
- Alicja Kaszuba, attorney-at-law
- Błażej Koczetkow, attorney-at-law
- dr Dominik Lubasz
- Andrzej Ludwiński, public prosecutor
- dr hab. Monika Namysłowska, prof. UŁ
- Aleksandra Piech, attorney-at-law
- Luiza Piskorek
- Dorota Skrodzka-Kwietniak
- Przemysław Sotowski
- attorney-at-law Monika Susałko
- dr Kamil Szpyt
- dr hab. Marek Świerczyński, prof. UKSW
- dr inż. Paweł Tadejko
- judge Konrad Wasik
- dr n. fiz. Magdalena Wicher
- Michał Włodczak

The team's work was managed by attorney-at-law Roman Bieda - leader of the working subgroup on ethics and artificial intelligence law.

[1] For more on the group, see https://www.gov.pl/web/ai/podgrupa-ds-etyki-i-prawa

I. Scope and Objectives of the Analysis

On 21 April 2021, the European Commission presented a proposal for a regulation of the European Parliament and of the Council establishing harmonized rules for artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts of the EU[2] (hereinafter: Artificial Intelligence Act or AI ACT or AIA).

However, the creation, development and use of artificial intelligence systems will require consideration not only of AI ACT regulations, but also of a number of other existing and currently drafted regulations.

The main purpose of this report is to present the relationship ('mapping") of AI ACT regulations to selected existing and proposed national and European regulations. As part of the analysis, we also referred to the guidelines of the Financial Supervisory Authority, relevant to areas where artificial intelligence can be or is being used by the supervised entities.

The analysis was conducted based on the draft AI ACT presented by the European Commission, as indicated above.

The report does not include an exhaustive presentation of the AI Act's relationship to existing regulations or draft legislation. As part of our analysis, we pointed out the relationship between the AIA and selected legislation, regulations and draft legislation.

This report is the result of the first stage of the analysis. We intend to conduct further analysis of the relationship and connections between the AI Act and the legislation/drafts presented in this report, as well as conduct mapping of further legislation.

We hope that this report will contribute to building awareness of the legal framework for the development and operation of artificial intelligence systems. The report is solely an expression of the personal opinions of its authors, and does not constitute a legal opinion and cannot be the basis for any decisions, particularly business decisions.

[2] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52021PC0206

II. Mapping the Artificial Intelligence Act

1. General Data Protection Regulation (GDPR)

1.1 Introduction

One of the fundamental issues of systemic consistency of artificial intelligence regulation is the issue of consistency with the provisions of the GDPR.

The goal of the EU legislators declared in paragraph 1.2 of the Explanatory Memorandum is that the proposed AI ACT is only intended to supplement the GDPR and Directive 2016/680 with a set of harmonized rules applicable to the design, development and use of certain high-risk AI systems and restrictions on certain applications remote biometric identification systems.

However, doubts about the real intentions arise already from the analysis of the legal basis for issuing the Artificial Intelligence Act. Indeed, it has been pointed out that it is, among others, Article 16 TFEU[3] (protection of personal data) without further clarification, either in the recitals or in the normative section, of the AIA's relationship to existing data protection laws.

It is also questionable whether the prohibitions proposed in the Artificial Intelligence Act can invoke Article 16(2) TFEU. Indeed, the proposed catalogue of prohibited activities does not directly target the protection of personal data, but other fundamental rights and freedoms.

In addition, recital 41 of the AIA expresses the intention that "This Regulation should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data" which, however, is not consistent with the wording of various provisions of the draft regulation, which introduces grounds for processing (see Article 10(5) and Article 54, recital 72 of the AIA).

Consequently, there is a lack of clarification in Article 1 or Article 2 of the AIA that EU legislation on the protection of personal data, in particular the GDPR, applies to the processing of personal data also covered by the scope of the Artificial Intelligence Act, and that the AIA is not in conflict with the changes to the GDPR.

There is no clear indication that the proposed regulation does not exclude the application of existing EU rules governing data processing, including with regard to the competence of competent supervisory authorities.

The above significantly reduces the effectiveness of mapping, which is exacerbated by the current contradiction of some recitals and specific regulations (Recital 41 and Article 10(5) and Article 54), as well as the appearance of delineating relationships in specific regulations, as discussed in more detail in the table.

The regulatory mechanisms used, such as the risk-based approach, which interact to determine the interactions between the GDPR and the AIA, also lack consistency. In the General Data Protection Regulation, risk analysis is directed at verifying the impact on the rights

[3] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A12012E%2FTXT

and freedoms of data subjects, while the AIA introduced a product-centered treatment, specifically included by reference in Article 65 to Article 3(19) of Regulation 2019/1020 stating that artificial intelligence systems posing a risk shall be understood as a product posing a risk within the meaning of Article 3(19) of Regulation (EU) 2019/1020, insofar as said risk involves a threat to the health and safety or fundamental rights of citizens. This affects the accepted regulatory concept of directing the bulk of legal obligations to AI providers and at the same time limiting users' obligations in ways that potentially conflict with the GDPR (Article 29(5) of the AIA).

The lack of a comprehensive regulation of the Artificial Intelligence Act's relationship to not only GDPR, but also, for example, to consumer regulations, was pointed out during the legislative process in the EDPS and EDPB opinions[4], among others.

1.2 Comparison Table

Legislation	**General Data Protection Regulation**	
AIA	GDPR	Description
Article 3(1)	Art. 4(4) and Art. 22	AI systems as defined in Article 3(1) of the AIA in the area using personal data, may perform personal data processing operations, including profiling as defined in Article 4(4) of the GDPR, and consisting in automated decision-making in individual cases within the meaning of Article 22 of the GDPR, making it necessary to apply the relevant GDPR provisions.
Article 3(2)-(4)	Article 4(7)-(8)	An obligated entity, including a supplier, a user, may be simultaneously considered a controller or a processor within the meaning of the GDPR (respectively: Article 4(7)-(8) of the GDPR), depending on the obligations they carry out in determining the purpose of data processing in the respective phases of development and use of AI systems. Consequently, this leads to applicable obligations being imposed on them, resulting from the GDPR.

[4] See. https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en, See also: Analysis of selected aspects of the draft artificial intelligence act, AI LAW TECH Foundation (https://www.gov.pl/web/ai/prawo).

Article 3(29)-32) and Art. 10	Article 4(1)	The respective categories of data, i.e. from training data to validation data to test data, although not containing references to the concept of personal data, may constitute personal data within the meaning of Article 4(1) of the GDPR. This results in the need to apply legalization grounds depending on the categories of personal data used from Article 6 or 9 of Regulation 2016/679, respectively, and to meet the other requirements of the GDPR.
Article 3(33)	Article 4(14)	Recital 7 of the AIA emphasizes the compatibility of the concept of biometric data used in the AIA (Article 3(33)) with the concept of biometric data as defined in Article 4(14) of the GDPR, and does not point out the obligation to interpret the concept in a manner consistent with the definition included in the GDPR.
Recital 24	Article 9(1)	In accordance with recital 24 of the AIA, any processing of biometric and other personal data related to the use of artificial intelligence systems for biometric identification, other than in connection with the use of "real-time" remote biometric identification systems in public spaces for law enforcement purposes under the AIA, including where such systems are used by competent authorities in public spaces for purposes other than law enforcement, should continue to meet all the requirements arising, as the case may be, from Article 9(1) of the GDPR. It should be pointed out that Article 9(1) of the GDPR imposes a fundamental prohibition on the processing of special categories of personal data, including biometric data within the meaning of Article 4(14) of the GDPR. However, the specific requirements for allowing the processing of such data are introduced by Article 9(2) of the GDPR, it is the one that should be referred to.
Article 5(1)(d)	Article 9(1)	Regarding the introduced ban on the use of remote biometric identification systems "in real time" in public spaces for law enforcement purposes, there is a scope overlap in the prohibitions on processing biometric identification data under Article 9(1) of the GDPR.

Art. 10.	Article 5(1)(a), c) I d)	Article 10 of the AIA introduces data quality criteria, which, in the case of personal data, are subject at the same time to the principles arising from Article 5(1) of the GDPR, in particular the principle of integrity underlying the anti-discrimination approach, the principle of data minimization that sets the framework of adequacy and the principle of regularity indicatingthe need to ensure that data is error-free.
Article 10(5)	Article 9(2)	Contrary to the assumption of not creating new legal grounds for the processing of personal data (recital 41 of the AIA), the legislator decided to propose the regulation of the legalization premise for the processing of special categories of data indicated in Article 9(1) of the GDPR for suppliers of AI systems as controllers to the extent that it is strictly necessary for their purposes of ensuring monitoring, detection and correction of bias in AI and high-level risk systems.
Article 29(6)	Article 35(1), section 3 and section 4	It noted the need to carry out, where appropriate, impact assessments for data protection (Article 35 GDPR) by users of AI systems, however, a restriction has been introduced that such assessment is made on the basis of the data provided by the provider required under Article 13 of the AIA without verification, which may significantly limit the scope of the data protection impact assessment (DPIA), and thus may negatively affect the scope of application of the GDPR.
Article 52(2)	Article 5(1)(a), Art. 13, 14, Art. 22	Transparency of Personal Data Processing. Transparency obligations for users of emotion recognition or biometric categorization systems, extend the transparency obligations required by the provisions of the GDPR in the case of biometric data processing.
Art. 54	Art. 6(1) and Art. 9(2)	Article 54 of the AIA introduces the legal basis for processing, in a regulatory sandbox, of personal data collected for other purposes to develop certain AI systems in the public interest. Thus, the regulatory intent expressed in recital 72 AIA is realized.
Art. 59	Articles 51 et seq.	There may be a dependency in the event of the final selection of a national supervisory authority in the form of a supervisory authority from the area of personal data.

Article 71(6)	Article 83(2)	The concurrence of sanctions under Article 71 of the AIA and Article 83 of the GDPR is possible. In doing so, it should be noted that there are significant scope discrepancies as to the circumstances taken into account in determining the amount of the fine in the two regulations.
Recital 72 and Art. 53	Article 83(2)(k)	Recital 72 of the AIA expresses an intention that is not reflected in the normative part of the draft, but can be read in the context of Article 83(2)(k) of the GDPR, which stipulates the authority's obligation to take into account any circumstances affecting the level of the penalty in such a way that when the competent authorities take decisions on the possible imposition of an administrative fine, what should be taken into account is the conduct of the participants using the regulatory sandbox.

2. EP and Council Regulation (EU) 2017/745 of 5 April 2017 on medical devices (MDR).

2.1 Introduction

An artificial intelligence system may constitute a medical device, or it may not meet the definition of a medical device, but be used in a medical context.

When an artificial intelligence system constitutes a medical device, it must comply with regulatory requirements under both the MDR and AIA. Importantly, the interaction of regulatory requirements under the MDR and the AIA is particularly deep and extensive.

First of all, as a general rule, the evaluation of the compliance of an artificial intelligence system that is a medical device with the requirements of the MDR will be carried out with the participation of an external notified body. This causes an artificial intelligence system that is a medical device to automatically meet the definition of a high-risk artificial intelligence system - and therefore such systems are subject to all the regulatory requirements for high-risk AI systems.

In doing so, the MDR and AIA methodologies for the obligations that a medical device manufacturer or high-risk AI system provider must fulfil are similar - both regulations focus on similar stages of the product life cycle and regulate these obligations in similar ways.

In particular, MDR and AIA regulations will overlap in such key areas as:

- requirements for the quality of data used for training, validation and testing of the AI system;
- methodology for conducting performance evaluation / clinical evaluation of the AI system;
- quality management system;
- technical documentation;

- security and transparency of operation, user control over the operation of the AI system which is a medical device;
- cyber security and data security;
- change management.

2.2 Comparison Table

Legislation	**EP and Council Regulation (EU) 2017/745 of 5 April 2017 on medical devices (MDR)**	
AIA	MDR	Description
Article 3(1) in conjunction with Article 6(1)(a) AIA	Art. 2 MDR	A medical device can be an AI system
Article 6, Annex II to AIA		Classification of medical devices as high-risk AI systems. "Regardless of whether the artificial intelligence system is marketed or put into service independently of the products referred to in point (a) and (b), such an artificial intelligence system shall be considered a high-risk system if both of the following conditions are met: a) the artificial intelligence system is designed to be used as a security-related element of a product covered by EU harmonization legislation listed in Annex II or is itself such a product; b) a product whose security-related component is an artificial intelligence system, or the artificial intelligence system itself as a product is subject to - under EU harmonization legislation listed in Annex II - to conformity assessment carried out by a third party for the purpose of placing this product on the market or putting it into service."
Art. 8 - 20 AIA	Articles 5, 10, 20 MDR	AIA provisions set out mandatory requirements for high-risk AI systems. These include: 1. the requirement to establish, implement, maintain a risk management system; 2. defining requirements for training, validation and test data; 3. the requirement to maintain technical records;

		4. the requirement to keep a record of events; 5. the obligation to design and create transparent systems; 6. the information obligation; 7. the requirement of human supervision; 8. the requirement for accuracy, reliability and cyber security of systems. 9. the requirement to establish, implement, maintain a quality management system. 10. the requirement to meet general security and performance requirements in correlation with Annex I to MDR. Analogous requirements are imposed by MDR on AI systems that are medical devices.
Article 9 AIA	Art.10, Annex I MDR	Risk Management System. Both MDR and AI regulate the responsibilities for implementing a risk management system as a continuous, iterative process carried out throughout the life cycle of a high-risk AI system, requiring regular, systematic updates.
Article 10 AIA	Article 10, Annex I to MDR	Training Data Requirements. Both MDR and AI regulate obligations for adequate quality of training data and appropriate data management practices.
Art. 16-29 AIA	Article 10, Annex I to MDR, Annex II to MDR	Responsibilities of high-risk AI system providers: Art. 16 AIA. Providers of high-risk artificial intelligence systems: a) ensure that their high-risk AI systems comply with AIA requirements; b) have a quality management system in accordance with Article 17 of the AIA; c) compile technical documentation of the high-risk AI system; d) keep records of events automatically generated by their high-risk AI systems if they are under their control; e) ensure that a high-risk AI system undergoes an appropriate conformity assessment procedure before it is placed on the market or put into service;comply with the registration obligations referred to in Article 51 of the AIA;

		g) undertake the necessary corrective measures, if the high-risk AI system does not meet the requirements established in Chapter 2 of this title; h) they will inform the competent national authorities of the Member States in which they have made available or put into service the AI system and, if applicable, the notified body, of the non-compliance with requirements and of any and all the corrective measures taken; i) place CE markings on their high-risk AI systems to confirm compliance with this regulation in accordance with Article 49 of the AIA; j) demonstrate, at the request of the competent national authority, the compliance of the high-risk AI system with the requirements established in AIA Title III, chapter 2. General responsibilities of medical device manufacturers: Article 10(1) MDR Manufacturers placing products on the market or into service shall ensure that products are designed and manufactured in accordance with MDR requirements. Art. 10(2) MDR. Manufacturers shall establish, document, implement and maintain a system for risk management as described in Section 3 of Annex I of the MDR. Article 10(3) MDR Manufacturers shall conduct a clinical evaluation in accordance with the requirements set out in Article 61 and Annex XIV to MDR, including a post market clinical follow up (PMCF). Article 10(9) MDR. (...) Manufacturers of devices, other than investigational devices, shall establish, document, implement, maintain, keep up to date and continually improve a quality management system that shall ensure compliance with this Regulation in the most effective manner and in a manner that is proportionate to the risk class and the type of device (...) Art. 10(10) MDR. Manufacturers of devices shall implement and keep up to date the post-market surveillance system in accordance with Article 83 of MDR.

		Article 10(11). Manufacturers shall ensure that the device is accompanied by the information set out in Section 23 of Annex I in an official Union language(s) determined by the Member State in which the device is made available to the user or patient. The particulars on the label shall be indelible, easily legible and clearly comprehensible to the intended user or patient. MDR Annex I (General Safety and Performance Requirements): 15. Devices with a diagnostic or measuring function 15.1. Diagnostic devices and devices with a measuring function, shall be designed and manufactured in such a way as to provide sufficient accuracy, precision and stability for their intended purpose, based on appropriate scientific and technical methods. The limits of accuracy shall be indicated by the manufacturer. 15.2. 12.2. The measurements made by devices with a measuring function and expressed in legal units shall conform to the provisions of Council Directive 80/181/EEC. 17. Electronic programmable systems - devices containing electronic programmable systems and software itself being a device 17.1. Devices that contain electronic programmable systems, including software, or software that is itself a device, shall be designed to ensure repeatability of results, reliability and operation in accordance with their intended use. In the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible and appropriate consequent risks. 17.2. For the devices that incorporate software or for standalone software that are devices in themselves, the software shall be developed and manufactured according to the state of the art taking into account the principles of development life cycle, risk management, verification and validation.

		17.3. 13.3. Software referred to in this Section that are intended to be used in combination with mobile computing platforms shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards to level of light or noise). 17.4. Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.
Art. 17 AIA	Article 10(2), Annex I, section 3 of the MDR	Obligation to implement a quality management system. Both the MDR and AI regulate responsibilities for implementing a quality management system. This system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions.
Article 18, Annex IV to AIA	Article 10(4), Annex II to MDR	Technical documentation. Both the MDR and AI regulate the obligations to prepare technical documentation for a high-risk AI system / an AI system that is a medical device.
Art. 30 AIA	Article 35 MDR	Notifying Authorities. 1. Each Member State shall designate or establish a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring.
Art. 31 AIA	Art. 38 MDR	Application from the conformity assessment body. Formal requirements for a request for notification to the supervisory authority.
Art. 32 AIA .	Art. 42 MDR .	Notification procedure. Member States shall notify the Commission and the other Member States of the conformity assessment bodies they have designated, using the electronic notification tool developed and managed by the Commission

Art. 33 AIA	Art. 36 MDR	Notification units. Notified bodies verify the conformity of a high-risk / medical device AI system in accordance with conformity assessment procedures.
Art. 34 AIA	Art. 37 MDR	Subsidiaries and subcontractors. Notified bodies bear the full responsibility for tasks performed by subcontractors or subsidiaries regardless of their location.
Art. 35 AIA	Art. 43 MDR	Identification numbers and list of notified bodies. The EU Commission assigns notified bodies an identification number. Each unit is assigned one such number, even if it has been notified based on several acts of the Union.
Art. 36 AIA	Article 46 MDR	Changes in notifications. Where the notifying authority suspects or receives information that the notified body no longer meets the requirements set forth in the AIA or does not performs its duties, the authority shall immediately initiate an investigation into the matter with the utmost care. If the notifying authority comes to the conclusion that the notified body no longer meets the requirements laid down in Article 33 or that it is failing to fulfil its obligations, it shall restrict, suspend or withdraw the notification as appropriate, depending on the seriousness of the failure. It shall also immediately inform the Commission and the other Member States accordingly.
Art. 37-38 AIA	Articles 47, 49 MDR	Other regulations concerning notified bodies. Challenging the competences of bodies and coordination of notified bodies.
Art. 43 AIA	Article 52 MDR	Conformity Assessment. The supplier of a high-risk AI system conducts a system conformity assessment. For high-risk AI systems that are medical devices or that are part of a product that is a medical device, the conformity assessment must take into account not only AIA requirements, but also MDR requirements.

		For the purposes of this assessment, notified bodies that have been notified in accordance with the MDR are authorized to conduct inspections of the compliance of high-risk AI systems with the requirements established in the AIA, provided that the compliance of these notified bodies with the requirements established in Article 33 (4), (9) and (10) of the AIA was assessed in the context of the notification procedure provided for in the MDR. If the acts listed in Annex II, section A of the AIA provide the product manufacturer with the option to opt out of third-party conformity assessment, as long as they have ensured compliance with all harmonized standards covering all applicable requirements, such manufacturer may exercise this option only if they have also ensured compliance with harmonized standards or, where applicable, common specifications referred to in Article 41 of the AIA, covering the requirements established in Chapter 2 of the AIA.
Article 44 AIA	Article 56 MDR	Certificates - Description. According to Article 56 (1) of the MDR, certificates issued by the notified bodies in accordance with Annexes VIII, IX and X of the MDR shall be in an official Union language determined by the Member State in which the notified body is established or otherwise in an official Union language acceptable to the notified body. The minimum content of the certificates is set out in Annex XI of the MDR.
Article 47 AIA	Article 59 MDR	Derogation from the conformity assessment procedure. Art. 47(1) of the AIA By way of derogation from Article 43, any national supervisory authority may request a judicial authority to authorise the placing on the market or putting into service of specific high-risk AI systems within the territory of the Member State concerned, for exceptional reasons of the protection of life and health of persons, environmental protection and the protection of critical infrastructure.

		That authorisation shall be for a limited period of time, while the necessary conformity assessment procedures are being carried out, and shall terminate once those procedures have been completed. The completion of those procedures shall be undertaken without undue delay. Article 59 (1) of the MDR 1. By way of derogation from Article 52, any competent authority may authorise, on a duly justified request, the placing on the market or putting into service within the territory of the Member State concerned, of a specific device for which the procedures referred to in that Article have not been carried out but use of which is in the interest of public health or patient safety or health.
Article 48 AIA	Article 19, Annex IV to MDR	EU Declaration of Conformity. 1. The provider shall draw up a written machine readable, physical or electronic EU declaration of conformity for each high-risk AI system and keep it at the disposal of the national supervisory authority and the national competent authorities for 10 years after the AI high-risk system has been placed on the market or put into service.
Article 49 of the AIA	Art. 20 MDR	CE Conformity Marking. The physical CE marking shall be affixed visibly, legibly and indelibly for high-risk AI systems.
Article 61 AIA	Articles 83, 84 MDR	Obligation of post-marketing monitoring of high-risk AI system. 1.Providers shall establish and document a post-market monitoring system in a manner that is proportionate to the nature of the artificial intelligence technologies and the risks of the high-risk AI system. The post-market monitoring system shall actively and systematically collect, document and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2.

Article 62 AIA	Article 87 MDR	Report serious incidents and malfunctions. Suppliers of high-risk AI systems marketed in the Union shall report any serious incidents related to these systems or any malfunction of these systems that constitute a violation of obligations under Union law designed to protect fundamental rights, to the market surveillance authorities of the member states where the incident or violation occurred. Such notification shall be made immediately after the provider has established a causal link between the AI system and the incident or malfunctioning or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the providers becomes aware of the serious incident or of the malfunctioning.
Article 63 AIA	Articles 92-94 MDR	Market surveillance and control of artificial intelligence systems in the EU market - enforcement.
Article 65 AIA	Article 95 MDR	Procedure for dealing with AI systems that pose a risk. 'Product presenting a risk' means a product having the potential to affect adversely health and safety of persons in general, health and safety in the workplace, protection of consumers, the environment, public security and other public interests, protected by the applicable Union harmonisation legislation, to a degree which goes beyond that considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use of the product concerned, including the duration of use and, where applicable, its putting into service, installation and maintenance requirements (Regulation (EU) 2019/1020).
Article 70 AIA	Article 109 MDR	Confidentiality. National competent authorities and notified bodies involved in the application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks.

Art. 71 AIA	Act on Medical Devices dated 7 April 2022 (Journal of Laws of 2022 item 974).	Criminal provisions. Member States shall adopt, in accordance with the AIA, penalty provisions, including administrative fines, applicable to violations of the AIA, and take all necessary measures to ensure their proper and effective implementation. The penalties provided must be effective, proportionate and dissuasive. They shall take into account the interests of SMEs and start-ups and their economic viability.

3. Data Act

3.1 Introduction

On 23 February 2022, the European Commission presented a proposal for a regulation on harmonized rules on fair access to and use of data (hereinafter: DA).

In general terms, DA's goal is to "ensure fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data[5]." The legal solutions envisioned in the draft DA can be used to acquire data to train AI systems.

3.2 Comparison Table

Legislation	**Proposal Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)**	
AIA	Data Act (DA)	Description
Article 3(29)-(33)	Article 2(1)	The DA contains a very broad definition of "data". In turn, the AIA defines the terms: "training data", "validation data", "test data", "input data", "biometric data". Each of the data categories defined in the AIA may include data within the meaning of the DA.
Article 3(1)	Article 2(3)	According to Article 2(3) of the DA, a "related service" is defined as "a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions". This term may also include the AI system as defined by the AIA.
Article 3(1)	Article 2(4)	According to Article 2(4) of the DA, the term "virtual assistants" means "software that can process demands, tasks or questions including based on audio, written input, gestures or motions, and based on those demands, tasks or questions provides access their own- and third-party services

[5] Application for Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final.

		or control their own- and third-party devices." A virtual assistant may constitute or comprise an AI system as defined by the AIA.
Entire Act	The entire DA, in particular Art. 5, Art. 6, Art. 8, Art. 9, Art. 13	of the DA create opportunities to acquire data for training AI systems. The recipient of the data must take into account the DA rules on data sharing (including restrictions on the use of the data, the terms of the data sharing agreement, the issue of remuneration).
Article 3(29)-(32)	Art. 35	Article 35 of the DA provides that the sui generis right provided for in Article 7 of Directive 96/9/EC does not apply to databases containing data acquired or generated during the use of a product or related service. Exclusively, this may also apply to databases used as so-called training, testing or validation sets.

4. Draft Artificial Intelligence Liability Directive

4.1 Introduction

The draft Directive on adapting non-contractual civil liability rules to artificial intelligence aims to eliminate one of the main obstacles to the use of artificial intelligence, which is the problem of defining liability rules for the operation of AI systems. According to the European Commission, the liability laws in effect in member countries are not adapted to handle claims for liability for damage caused by artificial intelligence-based products and services due to the need to prove the wrongful conduct or omission of the person who has caused the damage, which, due to the characteristics of artificial intelligence (complexity, autonomy, lack of transparency), may be too difficult or prohibitively expensive for the injured party.

To offset these problems, the Directive regulates the following:

a) disclosure of evidence of high-risk AI systems to enable the plaintiff to substantiate a claim for damages based on fault;
b) distribution of the burden of proof in cases of non-contractual fault-based claims for damages caused by the AI system.

4.2 Comparison Table

Legislation	Application: Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI liability directive)	
AIA	Draft Directive	Description
Art. 3, Art. 6	Article 2(1)-4)	The definitions of AI system, high-risk AI system, provider and user found in Article 2 of the Draft Directive refer to the definitions included in the AIA for consistency purposes.
Art. 16, Art. 24, Art. 28, Art. 29	Art. 3.	The directive introduces the power for courts to order the disclosure of evidence relating to a specific AI system to the potential plaintiff, provided that the potential plaintiff has previously requested the supplier, a person subject to the supplier's obligations, or the user, to disclose relevant evidence in their possession regarding a specific high-risk AI system that is suspected of having caused the damage, and the potential plaintiff has faced refusal to disclose the evidence. The request must be supported by facts and evidence substantiating the claim. The courts, at the request of the plaintiff, will be authorized to apply special measures to secure evidence. The scope of the information disclosed should be limited to that which is proportionate and necessary to substantiate the claim for damages, taking into account business secrets. There are available legal remedies to challenge the disclosure order. Failure to comply with the order will result in a (rebuttable) presumption of lack of due diligence.
Chapters 2 and 3 of Title III	Art. 4.	Article 4 introduces a rebuttable presumption of a causal link between the defendant's fault and the result obtained by the AI system (or lack thereof) if: i. the defendant's guilt has been demonstrated (or the presumption was applied), ii. based on the circumstances, it can be concluded that there is a reasonable probability that the fault affected the result obtained by the AI system (or the fact that the result was not obtained), iii. the plaintiff has shown that the damage was caused by the result obtained by the AI system.

		In the case of a claim for damages against a high-risk AI system provider subject to the requirements of Chapters 2 and 3 of Title III of the AI ACT (or a person subject to the obligations of a provider), fault will be proven only by showing that any of the following requirements have not been met: a) the artificial intelligence system uses techniques that include training models using data that was not developed from training, validation or test datasets that meet the quality criteria referred to in (Article 10(2)-(4) of the AI Act); b) the artificial intelligence system was not designed and developed to meet the transparency requirements of (Article 13 of the AI Act); c) the artificial intelligence system was not designed and developed in a way that allows individuals to effectively supervise it during the period of use of the artificial intelligence system in accordance with (Article 14 of the AI Act); d) the artificial intelligence system was not designed and developed to achieve, given its purpose, an appropriate level of accuracy, reliability and cyber security in accordance with [Articles 15 and 16(a) of the AI Act] or e) there was failure to promptly take the necessary corrective measures to ensure that the artificial intelligence system complies with the obligations specified in (Title III, Chapter 2 of the AI Act), or to withdraw it from the market or recall it from users in accordance with [Article 16(g) and Article 21 of the AI Act]. In the case of a claim against a high-risk AI system user, guilt will be proven by demonstrating that the user: a) has failed to comply with the obligation to use or monitor the artificial intelligence system in accordance with the attached operation manual or, where applicable, to stop or discontinue its use in accordance with (Article 29 of the AI Act), or b) they have fed the input data into the artificial intelligence system over which they have control and which is not adequate with respect to the purpose of this system as defined in (Article 29(3) of the act).

		The presumption of causality in a high-risk AI system claim will not be applied by the court if the defendant demonstrates that the plaintiff can obtain relatively easy access to evidence and expertise sufficient to prove a causal link between the fault and the result of the AI system. For claims for damages involving non-high-risk AI systems, the presumption of causality applies only if the court finds it unduly difficult to prove. When the defendant is the person who has used the AI system as part of their personal, non-professional activities, the presumption applies only if they have materially influenced the conditions of operation of the AI system or if they had the duty to do so and failed to do so.

5. The Act on Principles of Implementation of Tasks Financed from European Funds in the Financial Perspective 2021-2027 (Journal of Laws 2022, item 1079, hereinafter: "the New Implementation Act").

5.1 Introduction

Recital 163 of the European Parliament resolution of 3 May 2022 on artificial intelligence in a digital age (2020/2266(INI)[6] emphasizes the need to improve access to finance, especially for SMEs, start-ups and scale-ups.

The notifying authority, conformity assessment body, notified body and operators of artificial intelligence systems (in particular - suppliers) may require support from public funds.

The available sources of financial support include EU funds, national funds and other sources of funding (e.g. the Norwegian Financial Mechanism).

In order to use the appropriate source of funding, it is necessary to meet the requirements arising from specific legislation and concretized in the rules of a given support, such as competition documentation.

5.2 Comparison Table

Legislation	Act on Principles of Implementation of Tasks Financed from European Funds in the financial perspective 2021-2027 ("New Implementation Act")	
AIA	New implementation act	Description

[6] https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_PL.html

Article 3(8), point 19, point 21, 22	Article 1(1)	AIA regulations define: • the operator (including the supplier and the user), • the notifying authority, • the assessing unit, • the notified body. These entities may be subject to the New implementation act if they seek EU funding for the project.
Article 3(8), point 19, point 21, 22	Article 2(1) and point 34	The aforementioned categories of entities in the New Implementation Act are referred to as: • the applicant (who submitted the project financing application), • the beneficiary (who entered into the project financing agreement).
none	Article 2(30) Art. 5.	The provision defines "guidelines" - guidelines are aimed at institutions involved in the implementation of operational programs, e.g. ministries or executive agencies, but also to beneficiaries. The guidelines are intended to ensure standardized conditions and procedures. Execution of the project by the beneficiary must take place in accordance with the guidelines in order for agreement for co-financing to be considered properly performed. All the entities seeking European funding should read the relevant guidelines. The guidelines are published at https://www.gov.pl/web/fundusze-regiony/wytyczne
Art. 5. Art. 6. Art. 8 et seq. of chapter 2 and 3	Article 22(1)	The provision indicates what the control and audit of the operational program consists of. They serve to ensure that the operational program management and control system is working properly, and expenditures under the operational program are incurred in accordance with the law and EU and domestic principles. This translates into rules for concluding and supervising the performance of the project financing agreements. Thus, the control of performance of the project agreement may concern the use of prohibited artificial intelligence practices and the correct classification of AI systems according to the principles adopted in the AIA. Consequently, the control of high-risk AI systems may address compliance with the requirements established in the AIA.
Art. 33	Article 2(1) and point 30	Notified bodies may become the applicant/beneficiary depending on the rules of the specific financing.
Article 53(1) and section 6 Art. 55	Article 2(38) Art. 5.	Creating and funding regulatory sandboxes requires compliance with AIA regulations and may require the issuance of new guidance under the New Implementation Act or changes to the adopted guidelines.

6. Criminal Law

6.1 Introduction

The Artificial Intelligence Act regulates the use of AI systems for criminal investigation, evidence collection and crime prevention. It also raises the issue of illegal use of such systems and the need for appropriate tools to control their use. This affects the applicable regulations indicated in the table below.

The Artificial Intelligence Act, due to the broad subject matter it covers and the multifaceted nature of the regulated issue, taking into account the currently already quite extensive use of information technology (for the purpose of primarily identifying and detecting perpetrators of offences), hitherto regulated by the provisions of the Code of Criminal Procedure (but also other laws, including the Police Act of 6 April 1990), is directly related to the provisions of the criminal procedural law, and indirectly with the substantive criminal law.

The particular influence of the AIA can be seen especially in the field of legislation on the use of personal data (especially a person's image and biometric data) for the purpose of combating and preventing offences and determining their perpetrators, and the principles of the use of such data by the competent authorities.

Therefore, the introduction of the AIA will result in the need to further adapt Polish law. Within the criminal trial provisions, the need is due to the fact that the provisions of the Code of Criminal Procedure currently do not regulate the sharing of biometric data and the use of data collected during the proceedings by artificial intelligence systems. It also seems reasonable to regulate issues related to the storage of records of events automatically generated by the high-risk artificial intelligence system in question for the purposes of criminal proceedings and operational activities of the competent authorities, including issues such as: the data retention period, the authority authorized to request the data, the form of the decisions on the subject, while not necessarily within the framework of the Code of Criminal Procedure itself. Under substantive criminal law, on the other hand, the need arises to consider the criminalization of violations of the principles under the AI Act, taking into account the principles of effectiveness, proportionality and deterrence.

6.2 Comparison Table

Legislation	**The Police Act of 6 April 1990 (consolidated text: Journal of Laws 2023.171) (hereinafter: the Police Act)**	
AIA	Police Act	Description
Art. 5 (d), Art. 5 point. 3, Art. 52	Art. 20	Article 20 of the Police Act specifies the type and manner of use of personal data for the purposes referred to in Article 5d of the AIA. Article 5(3) of the AIA - any single use of a remote biometric identification system “in real time” in public space for law enforcement purposes requires prior authorization from

		a judicial or independent administrative authority of the Member State where the use is to take place, issued upon reasonable request and in accordance with the specific provisions of national law referred to in section 4. However, in duly justified emergencies, the use of the system may be started without a permit, and a permit may be requested during or after the use has been completed. In addition, Article 52 of the AIA indicates the removal of the strictures set forth in Article 5(3) of the AIA regarding the application of the so-called deepfakes where the use of such solutions has been approved by law for detection of offences, prevent offences, investigate offences and prosecute perpetrators, or when necessary to exercise the right to freedom of expression and the right to freedom of arts and sciences guaranteed by the Charter of Fundamental Rights of the European Union, subject to appropriate safeguards to secure the rights and freedoms of third parties.
Legislation	**The Internal Security Agency (ABW) and Intelligence Agency Act of 24 May 2002 and (consolidated text: Journal of Laws of 2022, item 557) (hereinafter: the ABW Act)**	
AIA	ABW Act	Description
Art. 5 (d), Art. 5 point 3,	Art. 23, 27-28b of the ABW Act	The provisions of Articles 23, 27-28b of the ABW Act refer to operational and reconnaissance activities carried out with the use of technical means, operating surveillance with the use of such measures, as well as the principles of obtaining permissions from the authorities to carry them out and the manner of handling the material so obtained - the use of remote biometric identification systems
Legislation	**Code of Criminal Procedure Act of 6 June 1997 (consolidated text: Journal of Laws 2022.1375) (hereinafter: Code of Criminal Procedure Act)**	
Article 5 (d)	Art. 15 § 2 and 3.	The provision provides the basis for requesting information, for the purposes of criminal proceedings , held by local governments and state institutions - i.e. among others, the information referred to in the provision of Article 15 § 2 of the Code of Criminal Procedure and 21 of the Personal Data Protection Act of 14 December 2018 in connection with preventing and combating offences, and which, under the exception indicated in Article 5 d of the AIA, could be used by criminal investigation authorities using remote biometric identification systems in “real-time” in public spaces for law enforcement purposes.

Article 63(5)	Art. 19 § 1 and 2.	Article 19 of the Code of Criminal Procedure stipulates that the public prosecutor and the court must inform of any violations discovered in their activities. Article 63(5) of the AIA provides that law enforcement supervisors may constitute the market surveillance authority for the purposes of the AIA.
Art. 5 (d) (iii), Art. 52	Art. 74	The provision of Article 74 specifies the obligations of the suspect to make the data available and the means to enforce these obligations. Among these are the obligations regarding biometric data and submitting to the process of acquiring it for law enforcement purposes, as stated in Article 5 (d) of the AIA.
Article 5 (d)	Art. 168b	What is not regulated is the issue of use of information obtained through the use of AI systems referred to in Article 5 of the AIA as evidence in criminal proceedings, and without which the question of admissibility of their use in the proceedings will be doubtful.
Article 5 (d) (iii)	Art. 192a § 1	Article 192a of the Code of Criminal Procedure regulates elimination testing, for which AI systems may be used and how to handle the material no longer relevant to the proceedings - the point also emphasized by the AIA.
Article 5 (d)	Art. 205 § 1	The provision of Article 205 of the Code of Civil Procedure regulates the position of specialists in criminal proceedings. It seems that a person who operates AI systems used for criminal proceedings should also be included in this provision.
Article 5 (d),	Art. 218, 218a, 236a	The sharing of biometric and other data used for the purposes of AI systems, has not been regulated in Polish criminal law. There is missing a regulation on the form of data request, the authorized authority (court, public prosecutor?) in the scope of the requested data, etc.
Art. 5 (d) (ii), Art. 5 (3) and (4)	Art. 241	The provision regulates operating surveillance and the use of evidence obtained in this way for criminal proceedings. Instead, the AIA refers to the use of AI systems for preventive purposes, so this will be done as part of operating surveillance and, in accordance with Article 5(3) of the AIA, will require consent of the competent authority (court/public prosecutor).

Art. 5.	Art. 308	There are no relevant provisions in the Code of Criminal Procedure stipulating rules for the use of the systems referred to in Article 5 (d) of the AIA in so-called necessary activities.

7. Civil Law (procedural)

7.1 Introduction.

The AI Act is a multifaceted act with a virtually unlimited scope in terms of its connection to the various branches of the law, including civil procedural law. Algorithms and modern technological tools can help the Polish justice system work more efficiently and quickly. Trials in Poland take years, and artificial intelligence provides an opportunity to improve this situation. In this context, it is important to highlight several interfaces between justice and artificial intelligence and, consequently, the relationship between AIA and civil procedural law.

We should point to the institutions of the civil court's authority to access data generated by AI systems (Article 248 of the Code of Civil Procedure), the user of which is not the court (including, for example, the register of events), to provide experts with access to the AI system when necessary (Article 284 of the Code of Civil Procedure, Article 293 of the Code of Civil Procedure), to introduce into evidence information obtained from the AI system (Article 309 of the Code of Civil Procedure) and the basis for judgment (Article 316 of the Code of Civil Procedure). Indeed, alignment with the AIA is required by regulations of procedural institutions that would allow the court to access AI systems belonging to third parties, as well as information and documents relating to the high-risk AI system and the issue of cooperation with civil courts in any activities taken with regard to the high-risk artificial intelligence system and suppliers of high-risk artificial intelligence systems, making it necessary to consider supplementing the code with these regulations.

Second, there is a relationship with the AIA on the level of using AI systems to identify specific cases in computerized litigation, i.e. the land and mortgage register proceedings, registration proceedings, the European payment-order proceedings under Regulation No. 1896/2006 of the European Parliament and of the Council of 12 December 2006 (Official Journal of the EU L 399 of 30.12.2006, p. 1, as amended), electronic payment-order proceedings and arbitration proceedings.

Third, artificial intelligence can be used effectively by the justice system. AI systems can help analyse case law, detect trends and lines of case law in cases, predict the direction of judgment, analyse extensive data sets, or even search for legal norms that may apply to a particular case. It is impossible at this point to determine even the framework of the law applied in the adjudication of civil, business, labour, social security, family, land and mortgage register cases, etc., to list the numerous lines of case law of the Supreme Court and the various appellate courts, let alone the decisions of district and regional courts that often assess identical facts differently. Each adjudicator has repeatedly drawn a case with identical facts to one that had already been resolved by another court with a final and valid decision. There are even cases of judges ruling differently in identical cases within the same division of the court. This does not constitute a problem when the reason for this is different legal mentality of the judges.

The problem, however, is when judges remain unaware of this fact. AI systems can prove useful not only in gathering evidence but, more importantly, they can help the judge become familiar with other similar decisions, the arguments relied on, and thus allow to make a quick decision. For this purpose, one can use the Common Courts Judgments Portal database available on the Internet, which, as of 4 March 2023, contained 404,775 court decisions. However, the contemporary Code of Civil Procedure is mainly oriented towards traditional court proceedings without the involvement of machines in shaping the final judgment.

In turn, the EU legislator has specifically provided for the hypothetical use of the AI system when courts make procedural decisions. The legal framework proposed by the European legislator is comprehensive and introduces a proportionate regulatory regime centered around a defined and risk-based regulatory approach. Indeed, in the AIA the European lawmakers have proposed separating high-risk artificial intelligence systems from other artificial intelligence systems. High risk is considered in accordance with Article 6(2) in conjunction with Annex III point 8 of the system from the area of administration of justice and democratic processes, i.e. artificial intelligence systems to assist the judicial authority in investigating and interpreting the facts and laws, and in applying the law to a specific factual situation.

It is necessary to make a general differentiation of legal artificial intelligence into two categories: legal retrieval systems and legal analysis systems. The former, in simple terms, comprise the commercial legal software currently on the market, which Polish judges use for work. In turn, the purpose of legal analysis systems is to determine the legal consequences of specific factual circumstances. Among them are the aforementioned sentencing machines and legal expert systems. The latter can be divided into rule-based systems, case-based systems and hybrid systems. Such systems are missing from the daily work of a judge.

In turn, according to Article 6(2) of the AIA and section 8(a) of Annex III, high-risk artificial intelligence systems are considered to be artificial intelligence systems that are intended to assist the judicial authority in investigating and interpreting the facts and laws, and in applying the law to a specific factual situation. In the event of introduction of this type of AI system into the Polish legal order, it will be necessary to regulate the basis for its application in the context of Article 316 of the Code of Civil Procedure. Artificial intelligence algorithms can be applied to the preparation of fairly standard parts of court judgments, such as the description regarding the parties to the proceedings, the conduct of the proceedings, together with a concise description of the parties' positions on the key disputed issues, a summary of the pleadings filed by the parties, the law applicable to the resolution of the case and the costs of the proceedings. The judge's role could come down to making a subsumption. The judge's time thus freed up could be devoted to dealing with the more complex elements of dispute recognition, both more quickly and arguably with a more careful analysis of the arguments presented.

7.2 Comparison Table

Legislation	Code of Civil Procedure	
AIA	Code of Civil Procedure	Description
Article 3(1) Art. 5. Art. 12 Art. 64	Art. 248	The EU legislator did not regulate the issue of special mode of access for the court to the data developed by AI systems. In turn, the provision of Article 248 of the Code of Civil Procedure introduces the obligation to present a document upon order of the court within the meaning of Article 77(3) of the Civil Code (the concept of document is broad and it is any information carrier that makes it possible to get acquainted with its content). The use of AI systems with their special features (e.g. black box effect, complexity, data dependency, autonomous behaviour) can have a negative impact on a number of fundamental rights. Regardless of the fact that the AIA is aiming to provide a high level of protection of fundamental rights and minimize the risk of erroneous or biased decisions undertaken with the support of AI systems, it is important to provide civil courts with access to data developed by artificial intelligence systems, including by remote biometric identification systems “in real time”. There is absence of regulation of issues related to the provision of such data for civil court purposes, as well as information and documents necessary to demonstrate compliance of the high-risk artificial intelligence system, and issues of cooperation with civil courts with regard to the high-risk artificial intelligence system, system providers, authorized representatives and users, making it necessary to supplement the Code with these regulations. This is in conjunction with Articles 3(1) and 5 of the AIA. There also arises the relationship of the application of Article 248 of the Code of Civil Procedure in conjunction with Article 12 of the AIA regarding civil court access to event records.What is also unregulated is the issue of access by courts to documentation prepared or maintained under the AIA regulation, as provided for in Article 64 (3) of the AIA.

Article 3(1) Art. 5.	Art. 254	The provision of Article 254 of the Code of Civil Procedure sets out the rules for the court to examine the veracity of a document, including the provision of the computer data storage medium. The court may, if necessary, summon the issuer of a document drawn up in the electronic form to provide the computer data storage medium on which this document was recorded. It should be considered whether the entire artificial intelligence system, and not just the data it produces, can be considered a carrier. There is no regulation providing for how to access the data carrier that is an AI system. Thus, a connection arises between Article 248 and Article 254 of the Code of Civil Procedure and the provisions of Article 3(1) and Article 5 of the AIA.
Art. 12 Article 64(3)	Art. 284 Art. 293 Art. 294	The provision of Article 284 of the Code of Civil Procedure sets forth the court's orders aimed at ensuring that an expert witness properly prepares a court opinion. Consideration should be given to supplementing the regulation with the manner and procedure (if only in the form of a regulation issued pursuant to a reference in the Code of Civil Procedure) of access by a court expert to documentation prepared or maintained on the basis of the AIA, as well as to the source code of the artificial intelligence system for the purposes related to civil proceedings.
Article 3(1) and Art. 5	Art. 309	Article 309 of the Code of Civil Procedure provides for the possibility of admitting and examining other evidence, unnamed in the act, with appropriate application of the rules of evidence. There is currently no regulation providing for the mode or procedure of using AI systems as a source of evidence (e.g. witnesses) in evidence proceedings. As absurd as it may seem, it should be noted that digital machines accompanying humans, i.e. machines with their own memory and computing power, equipped with the right devices, do not need people to watch the world (with the right configuration) (Alexa, Siri). Not all digital data exists as a result of human input into the memory of digital machines. Hence arises the problem of admitting evidence in the form of data obtained by an AI7 system, or access to data developed through the Internet of Things, such as city surveillance cameras, data diagnostics from self-driving cars.

[7] https://assets.documentcloud.org/documents/5113287/Timothy-Verrill-order-for-Amazon-Echo-data.pdf; see I.A. Hamilton, *A judge has ordered Amazon to hand over recordings from an Echo to help solve a double murder case* https://www.businessinsider.com/amazon-ordered-to-disclose-echo-alexa-recordings-murder-case-2018-11

Article 6(2) in conjunction with point 8(a) of Annex III	Art. 316	The provision of Article 316 of the Code of Civil Procedure specifies what state of things the court takes into account in sentencing.In turn, according to Article 6(2) of the AIA and section 8(a) of Annex III, high-risk artificial intelligence systems are considered to be artificial intelligence systems that are intended to assist the judicial authority in investigating and interpreting the facts and laws, and in applying the law to a specific factual situation. In the event of introduction of this type of AI system into the Polish legal order, it will be necessary to regulate the basis for its application in the context of Article 316 of the Code of Civil Procedure.Artificial intelligence algorithms can be applied to the preparation of fairly standard parts of court judgments, such as the description regarding the parties to the proceedings, the conduct of the proceedings, together with a concise description of the parties' positions on the key disputed issues, a summary of the pleadings filed by the parties, the law applicable to the resolution of the case and the costs of the proceedings. The judge's role could come down to making a subsumption. The judge's time thus freed up could be devoted to dealing with the more complex elements of dispute recognition, both more quickly and arguably with a more careful analysis of the arguments presented.
Article 3(1) in conjunction with Annex I Article 5	Art. 505(15)	Article 505(15) of the Code of Civil Procedure governs the proceedings in cross-border cases, so-called European payment request proceedings, regulated by Regulation (EC) No. 1896/2006 of the European Parliament and of the Council of 12 December 2006 establishing a European order for payment procedure (Official Journal of the EU L 399 of 30.12.2006, p. 1, as amended) In Article 8 sentence 2 of Regulation 1896/2006, the EU legislator allowed for automatic examination of the lawsuit. Hypothetically, it was allowed to make decisions in civil proceedings without human involvement. This standard is optional for member states, and the Polish legislator has not decided to automate European payment order proceedings. However, it is possible to shape the proceedings under Article 505(15) of the Code of Civil Procedure, to allow the participation of an AI system in Polish civil proceedings. It should be noted that the EU legislator (recital 11) explicitly stressed that the proceedings on the European payment order should allow the use of automatic data processing.

Article 3(1) Art. 5.	Art. 505(28) Art. 505 (29) Art. 505(30) Art. 505(31)	The electronic writ-of-payment proceedings aim, in conjunction with Art. 505(29), to streamline the recognition of small civil cases with Annex I by linking the traditional model of writ-of-payment proceedings with the possibilities arising from the use of modern technological solutions. The electronic writ-of-payment proceedings are a computerized civil procedure, in which the vast majority of activities are performed electronically, and this includes the acts of the court of the court clerk. The Polish legislator did not decide to exclude human participation (analogous to the Money Claim Online functioning in Great Britain) and introduce automation in some decisions (as in Germany: automatisertes Mahnverfahren). At the moment, the information system supporting the electronic writ-of-payment proceedings are not an artificial intelligence system within the meaning of Article 3(1) of the AIA, since it is not developed using one of the techniques and approaches listed in Annex I. It is characterized only by automatic data processing, expressed basically in the self-copying of information between pleadings and court documents, it seems possible and expedient to redefine the system in the direction of an expert system examining, at least automatically, the formal conditions of a lawsuit (Article 505(32) of the Code of Civil Procedure) and the maturity of a claim (Article 505(29) of the Code of Civil Procedure) without the involvement of the human factor. The model for this could be Article 14 § 1b of the Code of Administrative Procedure, added by the Act of 18 November 2020 (Journal of Laws of 2020, item 2320, as amended by Journal of Laws of 2021, item 1135), which came into force on 5 October 2021, providing for autonomous operation of the system and generation of pleadings in administrative proceedings. The above could take place in compliance with Article 22 of the GDPR. What should be advocated is improvement in electronic writ of payment proceedings toward an AI system based on a human-supervised machine learning mechanism, given that the issuance of a ruling in electronic writ of payment proceedings occurs without examination of evidence.

Article 3(1) in conjunction with Annex I Article 5	Article 626(1) of the Code of Civil Procedure in conjunction with Articles 1 and 36(3)(1) of the Act on Land and Mortgage Registers and Mortgages of 22 July 2022 (Journal of Laws of 2022, item 1728)	Cases in land and mortgage register proceedings are decided by the courts by making entries in the central database. Recently, Poland has made progress in the field of information technology application in the land and mortgage register proceedings.It follows from Article 36(3) of the Act on Land Mortgage Registers and Mortgages that the Minister of Justice maintains a central database of land and mortgage registers constituting a nationwide set of land and mortgage registers maintained in an ICT system. At the same time, due to the rapid development of initiatives to use blockchain technology (ensuring the reliability of transactions) and the increasing computerization of real estate trading, there is a need to analyse the impact of blockchain technology on streamlining real estate transactions and registration procedures. In this context, land and mortgage proceedings may be indirectly connected with Article 3(1) in conjunction with Annex I and Article 5 of the AIA.
Article 3(1) in conjunction with Annex I Article 5	Article 694 (1) et seq. of the Code of Civil Procedure in conjunction with Article 1(1) and (2), Article 3a(1) of the Act on the National Court Register of 23 March 2022 (Journal of Laws of 2022, item 1683)	Cases in the registry proceedings are conducted through the ICT system. To the extent regulated by Article 694(2a) of the Code of Civil Procedure, all acts of the court are recorded exclusively in this system. With regard to the registration procedure, the same remarks should be made as for the land and mortgage register proceedings.
Article 3(1) in conjunction with Annex I Article 5	Art. 1165 Art. 1170 § 1 Art. 117, Art. 1174 Art. 1197 § 2 Art. 1206 § 1 point 1 Art. 1214 § 3 point 2 Art. 1215 § 2	Currently, the arbitration proceedings have a traditional character, while the arbitrator can only be a natural person (Article 1170 § 1 of the Code of Civil Procedure). However, there appear ideas about the potential for arbitration courts to use AI systems[8]. First, artificial intelligence algorithms can be a significant convenience for both the parties to the proceedings and their attorneys. The ability to analyse a large amount of data and contrast it with past awards, for example, within a given arbitration institution or by a given arbitrator, can help not only

[8]See also L. Lai, M. Świerczyński (eds.), *Prawo sztucznej inteligencji [Artificial Intelligence Law]*, Warsaw 2020, Chapter XIX.

		in a party's choice of a suitable arbitrator, but also in predicting the cost, duration and outcome of arbitration proceedings. Access to this type of analyses can also help parties and attorneys decide on the best way to resolve a dispute in a given situation, as it may occur that it would be more beneficial in a particular factual situation, for example, to use proceedings before a common court or mediation. In international arbitration, on the other hand, it is necessary to browse large datasets of interpretations of individual rules, including often extensive case law not only as to arbitration-related procedural issues, but also in relation to substantive, often foreign, law. These tasks have traditionally been performed by junior lawyers. Artificial intelligence algorithms can be used to perform such tasks faster and more accurately, relieving the burden on lawyers.

8. Capital, Financial, Insurance Market Law

8.1 Introduction

Confidence in the capital market is largely dependent on certainty regarding the regulatory and supervisory environment. In order for Poland to compete with the best developed economies in the world, it must become a leader in technology development. This should contribute to raising productivity and lowering unit costs. To achieve this, technology must be supported by a properly linked legal, tax and educational framework that facilitates the development of the FinTech and InsurTech sectors. It is necessary to eliminate the barriers that limit the ability of capital market institutions to undertake such measures and to encourage their innovative activities. This can be achieved, among others, through significant use of legal and regulatory processes, e-government, and the creation of forward-looking FinTech, PayTech and InsurTech solutions.

The Polish capital market needs a predictable, pro-business legal environment that facilitates investment and capital raising, provides the highest protection for investors, and removes obstacles to accessing the highest quality services. Transparent communication with stakeholders is essential, including the active use of official recommendations and guidelines available to the entire market to standardize the interpretation of regulations and supervisory practices.

The entry into force of the Artificial Intelligence Act, which will regulate the provision of services by capital market institutions, may affect the timeliness of certain fragments of the publications of the Polish Financial Supervision Authority, especially when there are regulations explicitly addressing a particular form of market participant activity. As a result, there may be a need to publish the following subsequent positions of the supervisory authority, which will regulate issues related to the use of AI tools by the capital market.

Taking into account the issue, raised by market players, of the complexity of regulatory requirements for investment services, which at the same time may constitute barriers to market entry or limit competition, it is necessary to take measures to build a friendly regulatory environment for entities seeking to introduce innovative solutions and new technologies into the market, which can lead to an increase in the level of investment activity in Poland and guarantee the competitive advantage of Polish entities against counterparts from EU countries. It seems necessary for the Financial Supervision Authority to introduce a so-called regulatory sandbox for FinTech and InsureTech-type entities. Activities undertaken in the "regulatory sandbox" should result in smooth cooperation between the Financial Supervision Authority and the users.

8.2 Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to organizational requirements and conditions for the performance of the activities of investment firms and terms defined for the purposes of that directive

Comparison Table

Legislation	**Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing directive of the European Parliament and of the Council 2014/65/EU with regard to organizational requirements and conditions for the performance of the activities of investment firms and terms defined for the purposes of that directive**	
AIA	Commission Delegated Regulation (EU) 2017/565	Description
Article 3(1)	Article 54(1)(2)	Where investment advisory or portfolio management services are provided in whole or in part through an automated or semi-automated system, the responsibility for assessing suitability rests with the investment firm providing the service and may not be diminished by the use of an electronic system in making a personal recommendation or decision to enter into a transaction. The system, referred to in Article 54, may be an artificial intelligence system.

8.3 Act on Trading in Financial Instruments of 29 July 2005 (Journal of Laws 2022, item 1500 as amended; hereinafter referred to as the Trading Act)

Comparison Table

Legislation	**Act on Trading in Financial Instruments of 29 July 2005 (Journal of Laws 2022, item 1500 as amended; hereinafter referred to as the Trading Act)**	
AIA	Trading Act	Description
Article 3(1)	Article 3(2b)	Algorithmic trading can use an artificial intelligence system.
Article 3(1)	Article 3(2c)	A high-frequency algorithmic trading technique can use an artificial intelligence system.
Art. 15	Article 18(1) point 2	The obligation of regulated market operators to ensure the secure and efficient conduct of transactions.
Art. 15	Art. 29d	The company operating the regulated market will provide protection against unauthorized access to the information system in which personal data is stored.
Art. 15	Art. 74e	An investment firm acquiring or disposing of financial instruments using algorithmic trading will develop, implement and apply adequate and effective solutions aimed at: 1) ensuring the resilience and performance of ICT devices and systems to an extent that is commensurate with the scale of the business, particularly the limits and transaction thresholds; 2) preventing abnormal influence impact of ICT devices and systems on the smooth and safe trading in financial instruments, in particular by placing erroneous orders; 3) preventing the use of ICT devices and systems in violation of the Regulation of the European Parliament and of the Council (EU) No. 596/2014 of 16 April 2014 on market abuse (Market Abuse Regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC or regulation of financial instruments trading systems; 4) ensuring continuity of service and operation of ICT devices and systems used in its operations.

		In addition, the investment company monitors the operation of its ICT devices and systems and conducts tests in assessing the correctness of their operation in order to identify and eliminate potential or actual violations of the requirements mentioned above.
Art. 15	Article 78(1) point 2	Obligation of alternative trading system operators to ensure secure and efficient trading.
Art. 15	Article 78 section 15	An investment firm operating an alternative trading system or an organized trading platform must inform the Polish Financial Supervision Authority in the event of a material breach of the regulations concerning trading performed at that investment firm or the principles of fair trading, as well as significant disruptions to the functioning of its IT system.
Art. 15	Art. 81 a	It provides for the possibility of commissioning a trader or a foreign trader with performing a process, service or activity that would otherwise be performed by the investment firm itself, including the possibility of performing all or part of the operational functions relating to trading systems that allow or support the use of algorithmic trading.
Art. 15	Art. 83a	The obligation of investment firms to use, in their operations, the technical and organizational solutions to ensure the security and continuity of the brokerage services provided, as well as the protection of clients' interests as well as of confidential information and business secrets.

8.4 Commodity Exchange Act of 26 October 2000 (Journal of Laws of 2022, item 170, as amended)

Comparison Table

Legislation	Commodity Exchange Act of 26 October 2000 (Journal of Laws of 2022, item 170, as amended)	
Art. 15	Article 4(2)	The purpose of the company operating the exchange is to ensure the secure and efficient conduct of exchange transactions and settlements.

8.5 Regulation of the Minister of Finance of 8 December 2021 on the estimation of internal capital and liquid assets, risk management system, supervisory examination and assessment, as well as remuneration policy at brokerage houses and small brokerage houses.

Comparison Table

Legislation	Regulation of the Minister of Finance of 8 December 2021 on the estimation of internal capital and liquid assets, risk management system, supervisory examination and assessment, as well as remuneration policy at brokerage houses and small brokerage houses	
AIA	Regulation	Description
Art. 15	§ 6(3)	The obligation of the management board and supervisory board of a brokerage house or small brokerage house to provide adequate resources, including IT resources, necessary for sound risk management.

8.6 Regulation of the Minister of Finance of 30 May 2018 on the procedure and conditions for the conduct of investment companies, banks referred to in Article 70 (2) of the Act on Trading in Financial Instruments, and Custodian Banks (Journal of Laws of 2018, item 1112, as amended).

Comparison Table

Legislation	Regulation of the Minister of Finance of 30 May 2018 on the procedure and conditions for the conduct of investment companies, banks referred to in Article 70 (2) of the Act on Trading in Financial Instruments, and Custodian Banks (Journal of Laws of 2018, item 1112, as amended).	
AIA	Regulation	Description
Article 3(1)	§ 1	The regulation defines the procedure and conditions of conduct of investment firms, banks referred to in Article 70(2) of the Act on Trading in Financial Instruments of 29 July 2005 and custodian banks in the scope of activities for the performance of which artificial intelligence systems may be used.

8.7 Regulation of the Minister of Finance of 30 May 2018 on the procedure and conditions for the conduct of investment companies, banks referred to in Article 70 (2) of the Act on Trading in Financial Instruments, and Custodian Banks (Journal of Laws of 2018, item 1112, as amended).

Comparison Table

Legislation	Regulation of the Minister of Finance of 29 May 2018 on the specific technical and organizational requirements for investment companies, banks referred to in Article 70 (2) of the Act on Trading in Financial Instruments, and Custodian Banks (Journal of Laws of 2018, item 1111, as amended).	
AIA	Regulation	Description
Article 3(1)	§ 1	The Regulation specifies the detailed technical and organizational conditions required to carry out the activities of the investment firm and the bank referred to in Article 70(2) of the Act on Trading in Financial Instruments of 29 July 2005, and for the operation of a securities account, derivatives accounts and omnibus accounts by a custodian bank, which may use artificial intelligence systems in their operations.
Art. 15	§ 21	The regulation specifies detailed technical and organizational conditions to which the information systems of investment companies and banks referred to in Article 70(2) of the Act on Trading in Financial Instruments of 29 July 2005 are subject.

8.8 Recommendation D of the Financial Supervision Authority on the management of information technology and security areas of the ICT environment in banks

Comparison Table

Legislation	Recommendation D of the Financial Supervision Authority on the management of information technology and security areas of the ICT environment in banks	
AIA	Recommendation D	Description
Art. 15	Entire Recommendation	Technical solutions to ensure the cyber security of high-risk artificial intelligence systems must be tailored to the relevant circumstances and risks. Given the specificity of issues related to technology and security of the ICT environment of banks, these issues should be considered in conjunction with the set of good practices indicated in the recommendation of the bank supervision authority. Recommendation D is intended to indicate to banks the supervisory expectations for prudent and stable management of information technology and security areas of the ICT environment, in particular the risks associated with these.

8.9 Banking Law Act of 29 August 1997

Comparison Table

Legislation	Banking Law Act of 29 August 1997 (consolidated text: Journal of Laws of 2022, item 2324 as amended)	
AIA	Banking Law Act	Description
Article 3(1)	Article 1(1)	Banks, branches and representative offices of foreign banks, as well as branches of lending institutions can use artificial intelligence systems in their operations.
recital 37 of the explanatory memorandum; Article 6(2)	Article 105a(1a)	Banks, other institutions authorized by law to grant loans, lending institutions and entities referred to in Article 59d of the Consumer Credit Act of 12 May 2011, as well as institutions established under Article 105 (4), may, for the purposes of assessing creditworthiness and analysing credit risk, make decisions based solely on automated processing, including profiling, of personal data - including those constituting bank secrecy - provided that the person affected by the automated decision has the right to receive an adequate explanation of the grounds for the decision made, to obtain human intervention for the purpose of making a new decision, and to express his or her own position.

Art. 9.	Art. 9(3) in conjunction with Art. 9b	The bank has a management system, which is a set of rules and mechanisms relating to the decision-making processes that take place in the bank and to the evaluation of the banking activities carried out. The bank has a risk management system as part of the management system. Credit institutions subject to Directive 2013/36/EU must have sound governance arrangements that include a clear organizational structure with well-defined, transparent and consistent lines of responsibility, effective procedures to identify, manage, monitor and report the risks to which they are or may be exposed, adequate internal controls including sound administrative and accounting procedures, information networks and systems established and managed in accordance with Regulation (EU) 2022/2554, and remuneration policies and practices consistent with and conducive to sound and effective risk management. According to Article 9 of the AIA, a risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems which, for credit institutions regulated by Directive 2013/36/EU, shall be part of the risk management procedures established by those institutions pursuant to Article 74 of that Directive.
Art. 17	Art. 9(3) in conjunction with Art. 9b	Providers of high-risk AI systems shall have a quality management system in place which complies with that regulation. 3.For providers that are credit institutions regulated by Directive 2013/36/ EU, the obligation to put a quality management system in place shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

Art. 18	Article 9(3) in conjunction with Article 9b	1.Providers of high-risk AI systems shall draw up the technical documentation referred to in Article 11 in accordance with Annex IV, while providers that are credit institutions regulated by Directive 2013/36/EU shall maintain the technical documentation as part of the documentation concerning internal governance, arrangements, processes and mechanisms pursuant to Article 74 of that Directive.
Art. 20	Article 9(3) in conjunction with Article 9b	Providers of high-risk AI systems shall keep the logs automatically generated by their high-risk AI systems, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law. Providers that are credit institutions regulated by Directive 2013/36/EU shall maintain the logs automatically generated by their high-risk AI systems as part of the documentation under Articles 74 of that Directive.
Article 29(4)	Article 9(3) in conjunction with Article 9b	Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. For users that are credit institutions regulated by Directive 2013/36/EU, the monitoring obligation set out in the first subparagraph shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.
Article 29(5)	Article 9(3) in conjunction with Article 9b	Users of high-risk AI systems shall keep the logs automatically generated by that high-risk AI system, to the extent such logs are under their control. The logs shall be kept for a period that is appropriate in the light of the intended purpose of the high-risk AI system and applicable legal obligations under Union or national law. Users that are credit institutions regulated by Directive 2013/36/EU shall maintain the logs as part of the documentation concerning internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

Art. 19	Art. 133a	For high-risk AI systems referred to in point 5(b) of Annex III that are placed on the market or put into service by providers that are credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to 101 of that Directive. At least once a year, the Polish Financial Supervision Authority conducts either a supervisory examination and evaluation of the bank or a review and verification of the results of the previous supervisory examination and evaluation.
Article 43(2)	Art. 133a	In the case of high-risk artificial intelligence systems, as referred to in Annex III, points 2-8 of the AIA, providers shall follow a conformity assessment procedure based on internal control, as referred to in Annex VI, and which does not involve a notified body. For high-risk AI systems referred to in point 5(b) of Annex III, placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to 101 of that Directive. At least once a year, the Polish Financial Supervision Authority conducts either a supervisory examination and evaluation of the bank or a review and verification of the results of the previous supervisory examination and evaluation.

8.10 Guidelines for management of information technology areas and security of the ICT environment in universal pension funds

Comparison Table

Legislation	Guidelines for management of information technology areas and security of the ICT environment in universal pension funds	
AIA	Guidelines	Description
Art. 15	Entire Guidelines	Technical solutions to ensure the cyber security of high-risk artificial intelligence systems must be tailored to the relevant circumstances and risks.

		Given the specificity of issues related to technology and security of the ICT environment of universal pension funds, these issues should be considered in conjunction with the set of good practices indicated in the guidelines of the supervisory authority of universal pension funds. Guidelines for management of areas of information technology and security of the information and communications environment at universal pension funds are intended to indicate to supervised entities supervisory expectations for prudent and stable management of areas of information technology and security of the information and communications environment, in particular the risks associated with these areas.

8.11 Guidelines for management of information technology and security areas of the ICT environment in insurance and reinsurance companies

Comparison Table

Legislation	Guidelines for management of information technology and security areas of the ICT environment in insurance and reinsurance companies	
AIA	Guidelines	Description
Art. 15	Entire Guidelines	Technical solutions to ensure the cyber security of high-risk artificial intelligence systems must be tailored to the relevant circumstances and risks. Given the specificity of issues related to technology and security of the ICT environment in insurance and reinsurance companies, these issues should be considered in conjunction with the set of good practices indicated in the guidelines of the supervisory authority of insurance and reinsurance companies. Guidelines for management of areas of information technology and security of the information and communications environment at insurance and reinsurance companies are intended to indicate to supervised entities supervisory expectations for prudent and stable management of areas of information technology and security of the information and communications environment, in particular the risks associated with these areas.

8.12 Guidelines for management of information technology and security areas of the ICT environment at investment fund companies

Comparison Table

Legislation	Guidelines for management of information technology and security areas of the ICT environment in investment fund companies	
AIA	Guidelines	Description
Art. 15	Entire Guidelines	Technical solutions to ensure the cyber security of high-risk artificial intelligence systems must be tailored to the relevant circumstances and risks. Given the specificity of issues related to technology and security of the ICT environment in investment fund companies, these issues should be considered in conjunction with the set of good practices indicated in the guidelines of the supervisory authority of investment fund companies. Guidelines for management of areas of information technology and security of the information and communications environment at investment fund companies are intended to indicate to supervised entities supervisory expectations for prudent and stable management of areas of information technology and security of the information and communications environment, in particular the risks associated with these areas.

8.13 Guidelines for management of information technology and security areas of the ICT environment at investment firms

Comparison Table

Legislation	Guidelines for management of information technology and security areas of the ICT environment in investment fund companies	
AIA	Guidelines	Description
Art. 15	Entire Guidelines	Technical solutions to ensure the cyber security of high-risk artificial intelligence systems must be tailored to the relevant circumstances and risks. Given the specificity of issues related to technology and security of the ICT environment in investment firms, these issues should be considered in conjunction with the set of good practices indicated in the guidelines of the investment company regulator. Guidelines for management of areas of information technology and security of the information and communications environment at investment firms are intended to indicate to supervised entities supervisory expectations for prudent and stable management of areas of information technology and security of the information and communications environment, in particular the risks associated with these areas.

8.14 Recommendation D-SKOK on management of information technology and security areas of the ICT environment in cooperative savings and credit unions

Comparison Table

Legislation	Recommendation D-SKOK on management of information technology and security areas of the ICT environment in cooperative savings and credit unions	
AIA	Recommendation D-SKOK	Description
Art. 15	Entire recommendation	Technical s olutions to ensure the cyber security of high-risk artificial intelligence systems must be tailored to the relevant circumstances and risks. Given the specificity of issues related to technology and security of the ICT environment in cooperative savings and credit unions, these issues should be considered in conjunction with the set of good practices indicated in the guidelines of the investment company regulator. Recommendation D-SKOK on management of information technology and security areas of the ICT environment at cooperative savings and credit unions is intended to indicate to supervised entities the supervisory expectations for prudent and stable management of information technology and security areas of the ICT environment, in particular the risks associated with these.

8.15 Recommendation W on model risk management in banks

Comparison Table

Legislation	Recommendation W on model risk management in banks	
AIA	Recommendation W	Description
Art. 15	Entire recommendation	Technical solutions to ensure the cyber security of high-risk artificial intelligence systems must be tailored to the relevant circumstances and risks. Given the increase in the use of models understood as tools for making limited (to the most relevant dimensions) descriptions of a selected aspect of reality, the issues related to them should be considered in conjunction with the set of good practices indicated in the guidelines of the investment firm regulator. Among others, Recommendation W sets out standards for the model risk management process, taking into account the need to define a framework for the process, including principles for building models and assessing the quality of their performance, while ensuring appropriate corporate governance arrangements

8.16 Announcement from the Financial Supervision Authority regarding the processing of information by supervised entities in public or hybrid cloud computing

Comparison Table

Legislation	Announcement from the Financial Supervision Authority regarding the processing of information by supervised entities in public or hybrid cloud computing	
AIA	Cloud Message	Description
Art. 15	Entire message	Technical solutions to ensure the cyber security of high-risk artificial intelligence systems must be tailored to the relevant circumstances and risks. The processing of legally protected information in cloud computing generates risks related to the protection of the processed information. Protecting the processing of information relevant to the processes or operations of the entity supervised by the Polish Financial Supervision Authority requires consideration of the issues identified in the Cloud Communication

9. Consumer Law

9.1 Introduction

The impact of the projected AIA on consumers is obvious, as they are the end users of artificial intelligence system applications. Despite this, references to consumer law and consumers do appear in the draft's explanatory memorandum and in the AIA, but only in several places.

The explanatory memorandum to the AIA indicated that:

- the choice of the form of the regulation and the solutions adopted, especially those relating to high-risk systems, will ensure legal certainty for both operators and consumers (Section 2.4);
- the future regulation will strengthen and promote the protection of rights protected by the Charter of Fundamental Rights of the European Union, which include the high level of consumer protection regulated by its Article 38 (point 3.5 and recital 28);
- the introduced restrictions on the freedom to conduct business are intended to ensure compliance with the overriding public interest, manifested, among others, in the protection of consumers (Section 3.5);
- the draft is consistent with the Union's secondary law on consumer protection (Section 1.2).

In the AIA itself, the consumer does not appear in its normative section, but only once in the aforementioned recital 28. Recital 28 presents consumer rights in the context of fundamental rights, because "(...) The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high-risk. Those rights include the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, and non-discrimination, consumer protection, workers' rights, rights of persons with disabilities, right to an effective remedy and to a fair trial, right of defence and the presumption of innocence, right to good administration (...)".

The lack of references to consumers in the AIA is due to the fact that few regulations apply directly to consumers. However, this neither diminishes the importance of the AIA for consumers, nor does it mean there is no need to determine the relationship of many regulations to consumer law.

Due to the extensive nature of this area of law, the most important consumer legislation will be presented below: 1) Directive 2005/29/EC on unfair commercial practices and its implementation into Polish law in the form of the Act on Combating Unfair Market Practices of 23 August 2007, and 2) Directive 2011/83/EU on consumer rights together with the Consumer Rights Act of 30 May 2014.

9.2 Directive 2005/29/EC on unfair commercial practices/ Act on Combating Unfair Market Practices of 23 August 2007

The provisions of the AIA bear a strong resemblance to some of the provisions of Directive 2005/29/EC and, respectively, the provisions of the Polish Act on Combating Unfair Market Practices.

Although they sometimes have a broader scope of subject matter, covering not only business-to-consumer relations, they can be compared, in terms of B2C relations, to the typical provisions of the legal acts indicated above. Their interpretation, therefore, can be facilitated, but should not be a copy due to distinctiveness of certain premises.

Comparison Table

Legislation	**Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 on Unfair Commercial Practices/ Act on Combating Unfair Market Practices of 23 August 2007**	
AIA	**UCPD/Act on Combating Unfair Market Practices**	**Description**
Title II (Art. 5)	Art. 2(d) UCPD / Art. 2(4) of the Act on Combating Unfair Market Practices annex I to the UCPD/ Articles 7 and 9 of the Act on Combating Unfair Market Practices	Title II of the AIA consists solely of Article 5 and prohibits certain artificial intelligence practices. Thus, the AIA uses the term “practice”, while Directive 2005/29/EC uses the term “commercial practice" and the Polish act implementing the directive uses the term “market practice”. In many cases, the term “practice” will be the same as the term “commercial/market practice”, as some of the practices listed in Article 5 may involve the trader-consumer relationship and be of a commercial nature, meeting the definition in Article 2(d) of Directive 2005/29/EC/ Article 2(4) of the Act on Combating Unfair Market Practices. The prohibitions on artificial intelligence practices in Article 5 of the AIA resemble the prohibitions on commercial practices in all circumstances in Annex I to Directive 2005/29/EC / Articles 7 and 9 of the Act on Combating Unfair Market Practices. However, they are not limited to violations of the economic interests of consumers, but take into account the infliction of physical harm or psychological harm on the individuals concerned. Thus, it can be concluded that the prohibitions of Article 5, at least to some extent, such as the use of subliminal techniques (Article 5(1)(a), exploiting the vulnerability of a certain group of people (Article 5(1)(b)), can be considered as per se prohibitions of unfair commercial practices.

Article 52 (2) and (3)	Art. 2(d) UCPD / Art. 2(4) of the Act on Combating Unfair Market Practices Art. 7 UCPD/ Art. 6 of the Act on Combating Unfair Market Practices Art. 8 UCPD/ Art. 8 of the Act on Combating Unfair Market Practices annex II to the UCPD	Article 52 (2) and (3) of the AIA deals with the relationship between users of artificial intelligence systems and individuals who are recipients of specific artificial intelligence systems or entities to which they are applied. In many situations, these individuals will be consumers. Then, the regulations under review are similar to directive 2005/29/EC/ Act on Combating Unfair Market Practices Also, the scope of subject matter is similar, as many times the use of emotion recognition systems or biometric categorization systems (Article 52(2)) and the use of deepfakes (Article 52(3)) may be part of the commercial/market practice within the meaning of Article 2(d) of Directive 2005/29/EC / Article 2(4) of the APA, respectively. Both Article 52(2) and Article 52(3) of the AIA introduce a typical information obligation which involves informing individuals who may be consumers that certain artificial intelligence systems are being used on them. Failure to provide this information to consumers can be assessed as a misleading omission under Article 7 of Directive 2005/29/EC / article 6 of the Act on Combating Unfair Market Practices In connection with these proposed provisions, Annex II to Directive 2005/29/EC, which contains the information requirements established in EU law, concerning commercial communications, including advertising and marketing, which is an important information within the meaning of Article 7 (4) of Directive 2005/29/EC. While this annex is non-exhaustive, it has not been updated since the Directive on unfair commercial practices was enacted in 2005. This significantly weakens its information nature. Failure to provide the consumer with the information required by Article 52 (2) and (3) of the AIA, or its provision in a vague or inadequate manner, may be assessed as an aggressive business practice (Article 8 of Directive 2005/29/EC / Article 8 of the Act on Combating Unfair Market Practices). Although the AIA does not regulate the relationship between it and Directive 2005/29/EC, there is no obstacle to applying these acts in parallel if the commercial practice concerns the relationship between a trader and a consumer. Accordingly, the Act on Combating Unfair Market Practices can be applied together with the AIA.

9.3 Directive 2011/83/EU on consumer rights/ Consumer Rights Act of 30 May 2014

Mapping Directive 2011/83/EU and the Consumer Rights Act in light of the AIA requires emphasising that their subject scope is different from the indicated provisions of the AIA.

In particular, Articles 13 and 14 of the AIA will not apply to the trader-consumer relationship. Nevertheless, it is worth pointing in particular to the provisions on information obligations in Directive 2011/83/EU and, accordingly, in the Consumer Rights Act, as this may provide a starting point for thinking about the need for appropriate rules for B2C relationships.

Comparison Table

Legislation	**Directive 2011/83/EU of the European Parliament and of the Council of 25.10.2011 on consumer rights (CRD)/ Consumer Rights Act 30 May 2014**	
AIA	CRD/Consumers Rights Act	Description
Art. 13	in particular Article 6 CRD / Article 12 of the Consumers Rights Act	Note Chapter II of the AIA, particularly Article 13, which introduces transparency requirements relating to high-risk artificial intelligence systems, and the similarity of Article 12 of the Consumer Rights Act in terms of information provided to consumers. However, according to Article 13 of the AIA, the supplier must ensure transparency only to the system user, not to the consumer. Therefore, one may wonder to what extent there should be transparency in the application of AI to the consumer, and whether this should not be imposed by the AIA. It would be important that in the process of concluding a contract with a consumer, or in the course of activities aimed at concluding such a contract, it would be necessary to inform the consumer about the use of a high-risk AI system, together with an indication of the possible ways in which such a system affects the consumer and the risks posed by the system to the consumer. With the current wording of AIA Annex III, this would not be applied broadly to consumers, but would apply in the area of biometric identification and categorization. This would provide comprehensive transparency of the system. Not only for the user, as per the AIA, but also for consumers. Article 13 of the AIA does not specify an obligation to provide transparency to the person affected by a forecast or decision based on artificial intelligence, which is done, for example, by Article 6(1)(ea) of the CRD, according to which, before a

		consumer is bound by a distance or off-premises contract, or any offer for that matter, the trader is required to provide the consumer with information in a clear and comprehensible manner about the fact that the price has been individually adjusted based on automated decision-making (where applicable), so that the consumer can take into account potential risks when making a purchase decision. This obligation has been limited to situations where personalization is carried out through automated decision-making, and does not include so-called dynamic pricing. To be considered is the introduction of an obligation to inform consumers about the use of AI mechanisms to tailor marketing messages to their needs, along with the reasons which have allowed to decide to display such a message to them, next to the message. A similar obligation appears in the Digital Services Act9 for online platforms. However, in order to ensure transparency in consumers' decision-making process, it would be prudent to give them the opportunity to understand why the AI matched a particular marketing message to a particular person.
Article 52 (2) and (3), especially Article 6 CRD/ Article 12 of the Consumers Rights Act, Article 52 (2) and (3) introduce information and transparency obligations for	virtual agents, deepfake and emotion recognition systems, or biometric categorization systems.	Thus, these regulations establish a typical information obligation to inform individuals who may be consumers about the application of certain artificial intelligence systems to them. What should be considered is introduction of analogous provisions in Directive 2011/83/EU and the Consumer Rights Act.

[9] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_pl

Ministerstwo
Cyfryzacji

GRAI
GRUPA ROBOCZA
DS. SZTUCZNEJ INTELIGENCJI