
CHAMBERS GLOBAL PRACTICE GUIDES

Artificial Intelligence 2025

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Poland: Law & Practice

Agata Szeliga, Michał Kalinowski,
Maciej Gil, Sylwia Macura-Targosz
and Anna Tujakowska
Sołtysiński Kawecki & Szlęzak

Poland: Trends & Developments

Agata Szeliga
Sołtysiński Kawecki & Szlęzak



POLAND

Law and Practice

Contributed by:

Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska

Softysiński Kawecki & Szlęzak



Contents

1. General Legal Framework p.6

1.1 General Legal Background p.6

2. Commercial Use of AI p.6

2.1 Industry Use p.6

2.2 Involvement of Governments in AI Innovation p.6

3. AI-Specific Legislation and Directives p.7

3.1 General Approach to AI-Specific Legislation p.7

3.2 Jurisdictional Law p.7

3.3 Jurisdictional Directives p.7

3.4 EU Law p.8

3.5 US State Law p.8

3.6 Data, Information or Content Laws p.8

3.7 Proposed AI-Specific Legislation and Regulations p.9

4. Judicial Decisions p.9

4.1 Judicial Decisions p.9

5. AI Regulatory Oversight p.9

5.1 Regulatory Agencies p.9

5.2 Regulatory Directives p.10

5.3 Enforcement Actions p.11

6. Standard-Setting Bodies p.11

6.1 National Standard-Setting Bodies p.11

6.2 International Standard-Setting Bodies p.11

7. Government Use of AI p.12

7.1 Government Use of AI p.12

7.2 Judicial Decisions p.12

7.3 National Security p.12

8. Generative AI p.13

8.1 Specific Issues in Generative AI p.13

8.2 Data Protection and Generative AI p.14

9. Legal Tech p.15

9.1 AI in the Legal Profession and Ethical Considerations p.15

10. Liability for AI p.16

10.1 Theories of Liability p.16

10.2 Regulatory p.17

11. Specific Legal Issues With Predictive and Generative AI p.17

11.1 Algorithmic Bias p.17

11.2 Facial Recognition and Biometrics p.18

11.3 Automated Decision-Making p.19

11.4 Transparency p.20

12. AI Procurement p.20

12.1 Procurement of AI Technology p.20

13. AI in Employment p.21

13.1 Hiring and Termination Practices p.21

13.2 Employee Evaluation and Monitoring p.21

14. AI in Industry Sectors p.21

14.1 Digital Platform Companies p.21

14.2 Financial Services p.22

14.3 Healthcare p.22

14.4 Autonomous Vehicles p.23

14.5 Manufacturing p.24

14.6 Professional Services p.24

15. Intellectual Property p.24

15.1 IP and Generative AI p.24

15.2 Applicability of Patent and Copyright Law p.24

15.3 Applicability of Trade Secrecy and Similar Protection p.25

15.4 AI-Generated Works of Art and Works of Authorship p.25

15.5 OpenAI p.25

16. Antitrust p.25

16.1 Emerging Antitrust Issues in AI p.25

17. Cybersecurity p.25

17.1 Applicability of Cybersecurity Legislation to AI p.25

18. ESG p.26

18.1 ESG Dimensions of AI p.26

19. AI Governance and Compliance p.26

19.1 AI Governance and Best Practice Compliance Strategies p.26

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, **Softysiński Kawecki & Szlęzak**

Softysiński Kawecki & Szlęzak is one of Poland's leading full-service law firms. With more than 180 attorneys, the firm provides the highest standard of legal services in all areas of business activity and is well-reputed for the quality of its work and innovative approach to complex legal problems. Since the 1990s, Softysiński Kawecki & Szlęzak (SK&S) has been closely associated with the ever-changing technology sector, especially the dynamically devel-

oping IT industry. The firm provides high-quality legal services to both individuals and companies, covering the full scope of TMT issues. The team works alongside the firm's fintech, IP/IT, privacy and tax teams to provide an innovative interdisciplinary service and to help businesses use state-of-the-art technologies in a safe, cost- and time-effective manner. SK&S was the founding member of the New Technologies Association.

Authors



Agata Szeliga has been a partner at Softysiński Kawecki & Szlęzak since 2009 and joined the firm in 1998. She specialises in new technologies, personal data protection, state aid, and

public procurement. Agata has advised on cloud computing for many years, especially in the financial sector. She also advises on AI and the sharing of data generated by devices and applications. Agata is a member of the European Commission's Expert Group on B2B data sharing and cloud computing contracts.



Michał Kalinowski is an associate at Softysiński Kawecki & Szlęzak and has gained experience in law firms providing services to Polish and foreign clients, where he specialised in

IT, e-commerce and IP law. He rejoined the firm in January 2022, and advises on drafting contracts relating to IT systems (implementation, maintenance, and development), as well as in the areas of AI, copyright and consumer protection law. He is a PhD student at Cardinal Stefan Wyszyński University in Warsaw, conducting research on AI creations from the perspective of copyright law.



Maciej Gil is a senior associate at Softysiński Kawecki & Szlęzak. He joined the firm in 2017 and specialises in IT, AI, e-commerce and IP law, including industrial property,

unfair competition and copyrights. He has experience in licensing, technology transfer, litigation and other IP/IT matters. Maciej also advises on IP and AI-related matters in M&A transactions. He is an author of several publications in the field of IP law.



Sylwia Macura-Targosz is a senior associate at Softysiński Kawecki & Szlęzak. She specialises in IT law, new technologies and e-commerce. She also supports clients on the

legal side in projects related to the use of AI and the sharing of device-generated data. Sylwia excels in the field of personal data protection and privacy. She is a member of the New Technologies Law Association.

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, Sołtysiński Kawecki & Szlęzak



Anna Tujakowska is a senior counsel at Sołtysiński Kawecki & Szlęzak. She joined the firm in 2008, and advises and represents clients in commercial arbitration disputes with SA KIG,

ICC, VIAC and UNCITRAL arbitration rules, with arbitration seats in Warsaw, Vienna and Paris. She also has extensive experience in international arbitration, representing both public and private investors in BIT investment arbitrations in the EU. Additionally, she serves as an arbitrator. Anna integrates her arbitration expertise with AI-related matters, leveraging AI to enhance dispute resolution processes.

Sołtysiński Kawecki & Szlęzak

Jasna 26 Street
00-054 Warsaw
Poland

Tel: +48 22 608 70 00
Fax: +48 22 608 70 01
Email: office@sklegal.pl
Web: www.sklegal.pl



Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, Sołtysiński Kawecki & Szlęzak

1. General Legal Framework

1.1 General Legal Background

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act; AI Act) applies directly in Poland. There are no general provisions of Polish law that would specifically apply to AI. However, the draft of the Act on Artificial Intelligence Systems is being prepared by the government in order to ensure full implementation of the AI Act.

AI is currently qualified as software, and in addition to the AI Act, the laws applicable to software will apply to AI. The following are examples thereof.

- Contracts made with the use of AI should be treated like those made with pre-programmed algorithms.
- No category of AI systems, agents or models can hold legal capacity or be legally liable.
- Tort liability for using AI vis-à-vis a third party should be attributed to users and/or providers of such AI.
- Privacy laws, including GDPR, apply to the processing of personal data by AI.
- There are no AI creations or inventions. As a rule, only a human being can be the author of copyrighted work or the inventor of inventions protected by industrial property law; however, AI may be covered by so-called derivative copyrights (eg, video or sound recordings).
- The use of AI in an employment context should respect all employment regulations

(including non-discrimination) and respect employees' rights.

- Consumer laws apply to the offering or use of AI by consumers (eg, to terms and conditions).

2. Commercial Use of AI

2.1 Industry Use

AI and machine learning (ML) have been applied in various sectors in Poland, but AI deployments are rather slow and focus on automation and efficiency.

From the authors' experience, key industry applications are now based on generative AI (GAI) and include the following.

- Chatbots and virtual assistants (both generally available chatbots and dedicated systems) – eg, internal chatbots that provide responses based on AI, grounded in a given entity's knowledge base.
- Supporting the back-office functions (eg, software development, summarisation of meetings or documents, drafting/reviewing, updating and verifying internal databases, and preparing marketing content).

There are multiple cross-industry initiatives concerning new technologies in Poland.

2.2 Involvement of Governments in AI Innovation

The Polish government's initiatives to facilitate and support the adoption and advancement of AI for industry use are limited and include the following.

- Adoption of an AI Policy by the Polish Council of Ministers in 2020, which is a strategic

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, **Softysiński Kawecki & Szlęzak**

plan to advance AI development for societal, economic, and scientific benefits.

- Establishment of a PL/AI Artificial Intelligence for Poland advisory group in early 2024 upon the initiative of the Deputy Prime Minister and Minister of Digital Affairs.
- Implementation of tax incentives for robotisation. In November 2024, several government institutions signed a letter of intent to launch the Artificial Intelligence Fund, with funding of around PLN1 billion.
- Activities of the National Centre for Research and Development to support AI innovation (eg, by awarding grants and IDEAS NCBR – an R&D centre).
- Establishment of a Standing Subcommittee on Artificial Intelligence and Transparency of Algorithms in the Polish Parliament.

See also 7.2 Judicial Decisions.

3. AI-Specific Legislation and Directives

3.1 General Approach to AI-Specific Legislation

There are no AI-specific regulations in Poland. However, work is in progress at the government level on an act implementing the AI Act – see 3.7 Proposed AI-Specific Legislation and Regulations.

3.2 Jurisdictional Law

No AI-specific legislation has been enacted in Poland yet.

3.3 Jurisdictional Directives

AI Policy

AI Policy focuses on creating transparent and accountable algorithms for use in public administration, enhancing data access, and applying

AI to healthcare and environmental protection. In February 2024, the works on update of the AI Policy started.

Position of the Polish Financial Supervision Authority (FSA) on the provision of robo-advisory services (2020)

The guidelines emphasise the user's control over AI use and responsibility for clear client communication. Humans should make the final decision.

Recommendations on AI in the financial sector (2022)

The Ministry's Working Group on AI – Subgroup for the Financial Sector – identified several barriers to using AI and provided its recommendations in the identified fields.

Recommendations for the use of AI in justice and law enforcement (2024)

The document suggests adopting AI to modernise and speed up the judicial system – including digitalising records, automating transcriptions, drafting orders, using chatbots, searching for case precedents, drafting decisions, and implementing electronic delivery and translation systems.

Guidelines on the responsible use of generative AI in research (2024)

In March 2024, the European Commission – together with the European Research Area countries and stakeholders – published guidelines focusing on research quality, honest GAI use, respect for participants, and accountability in research.

Recommendations on prohibited AI systems

In September 2024 Ministry of Digitalisation and the Research and Academic Computer Network – National Research Institute published their rec-

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, Sołtysiński Kawecki & Szlęzak

ommendations on prohibited AI systems and associated provisions of AI Act.

The publication aims to clarify the provisions of the Act regarding prohibited artificial intelligence systems, detailing the techniques, functions, and methods by which these systems operate.

Policy for the Development of Artificial Intelligence in Poland 2025–2030

Prepared by the Working Group on AI in December 2024 to develop trustworthy AI in Poland, focusing on four pillars: human capital, innovation, investment and implementation. The study also takes into account important areas of development, such as economic competitiveness and national security, and invites discussion on the future of AI in Poland.

Recommendations on how attorneys-at-law should use AI-based tools

Launched by the National Council of Attorneys-at-law in May 2025, the Recommendations are the first extensive document with guidelines for the Polish legal community on the use of AI. The document includes recommendations for three phases: preparation, implementation and use of AI tools.

3.4 EU Law

3.4.1 Jurisdictional Commonalities

Similar to other EU member states, the regulatory framework for AI in Poland is predominantly defined by the AI Act. This framework is further supported by the EU Directive on liability for defective products (see **10.2 Regulatory**), in addition to sector-specific EU product regulations.

3.4.2 Jurisdictional Conflicts

Poland currently has no AI-specific laws, resulting in an absence of potential inconsistencies

with EU law. The proposed Polish Act on AI Systems is to ensure enforcement of the AI Act in Poland (see **3.7 Proposed AI-Specific Legislation and Regulations**).

3.5 US State Law

This is only applicable to the US.

3.6 Data, Information or Content Laws

No special local Polish laws have been introduced or amended to foster AI development. Implementation of Directive on copyright and related rights in the Digital Single Market, introducing text and data mining exception, was delayed and came into force only in September 2024. Two separate exceptions are established: (i) for cultural heritage institutions and certain educational entities, and (ii) for any individual or entity, although rights-holders may opt-out in such case. As of now, no recognised national standard or recommendations concerning the opt-out mechanism have been developed.

While the EU's primary aim is to regulate AI through the EU AI Act, AI must also comply with all other EU regulations, ie:

- GDPR – both the AI Act and GDPR apply to AI solutions, leading to potential legislative overlap. Practices banned under the AI Act could also violate GDPR's rules on automated personal data processing. With its legal instruments, the AI Act enhances GDPR rights, emphasising transparency and effective human oversight of AI systems.
- Data Services Act – see section **14.1 Digital Platform Companies**.
- The Data Act specifies the basic data-sharing models and enables access to the data to train, fine-tune or verify AI models. The AI may also be needed to analyse vast amounts of data generated by connected products

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, Sołtysiński Kawecki & Szlęzak

and services – particularly to identify patterns, potential improvements or inventions earlier.

3.7 Proposed AI-Specific Legislation and Regulations

Works on the draft Polish Act on AI Systems are ongoing at the government level. The published draft of the Act includes provisions on the following.

- Establishment of a national market surveillance authority for AI systems (AI Development and Security Committee).
- Regulations concerning the oversight of the market for AI systems and general-purpose AI models.
- Procedures concerning infringement of the AI Act.
- Rules for imposing administrative fines for infringements of AI Act.
- Procedures for reporting serious incidents that have occurred in connection with the use of AI systems.
- Ability to obtain an individual opinion on the application of the AI Act or the Polish Act on AI Systems; compliance with the obtained opinion would shield the entity from penalties in this context.
- Regulations on regulatory sandboxes.
- conditions and procedures for accreditation and notification of conformity assessment bodies.

See also 5. AI Regulatory Oversight.

4. Judicial Decisions

4.1 Judicial Decisions

There have been no decisions related to AI in Poland. However, Poland is introducing new digital tools to support judges and improve the

efficiency of the court system. The main initiative is the Digital Judicial Assistant (DJA), which will help judges write the reasoning behind court decisions. DJA will be available in selected courts starting mid-2026, and judges will receive training on how to use it. DJA is initially foreseen to be used in the Swiss franc loan cases. The project also includes the so-called Settlement Calculator, ie, the tool that will automatically calculate what each side (the consumer and the bank) owes in mortgage cases, especially those involving Swiss franc loans. These innovations are part of a broader effort to modernise the Polish judiciary and make it more efficient, accurate, and user-friendly. Currently, DJA is tested in the District Court in Poznań but its function is limited to assist administrative secretaries.

5. AI Regulatory Oversight

5.1 Regulatory Agencies EU

- European Artificial Intelligence Office (“AI Office”) – the AI Office (established on January 24, 2024) will enforce the rules for general-purpose AI models, except high-risk models.
- European Commission (EC) – the EC regulates AI in the EU, emphasising ethical development, data protection, consumer rights, and competition to promote innovation and responsible use.
- European AI Board – the AI Act also provides for the establishment of the European Artificial Intelligence Board, comprising one representative from each member state, to support the Commission and member states in implementing the AI Act effectively.
- Scientific panel – this panel is composed of experts chosen by the Commission because of their current scientific or technical knowl-

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, **Softysiński Kawecki & Szlęzak**

edge in the AI domain. The scientific panel will advise and support the AI Office and member states.

Poland

- AI Development and Security Committee – market surveillance authority within the meaning of the AI Act. Committee key activity will be to monitor the AI market and support businesses in implementing the provisions of the AI Act, in particular to ensure the safe use of AI systems. The Committee is also to act as a single point of contact, as referred to in Article 70 of the AI Act. The establishment of this body is provided for in the draft Polish Act on AI systems.
- Social Artificial Intelligence Board – a body whose task is to express opinions and positions on matters referred to it by the Committee. The establishment of this body is provided for in the draft Polish Act on AI systems.
- The co-ordination of AI implementation is the responsibility of the Ministry of Digital Affairs.
- AI Policy Task Force established at the Committee of the Council of Ministers for Digital Affairs in order to effectively monitor, implement and co-ordinate the AI implementation in Poland.
- PL/AI Artificial Intelligence for Poland – advisory group of the Ministry of Digital Affairs tasked with developing recommendations for using AI to improve specific areas of state operations.
- Standing Subcommittee on AI and Transparency of Algorithms. The Polish Parliament formed a Subcommittee to discuss AI's societal impact and assess related opportunities and risks.
- Working Group on Artificial Intelligence (GRAI), established by the Ministry of Digital Affairs in Poland, aims to identify strategies to foster the right environment for AI develop-

ment in Poland's private and public sectors as well as scientific research.

- Institute of IDEAS, research and development centre operating at NASK in the field of artificial intelligence, whose mission is to support the development of this technology in Poland.

Additionally, several governmental bodies and institutions play roles in regulating aspects related to AI. Key entities are:

- Office of the Personal Data Protection Authority (UODO) – UODO regulates data protection in Poland and is vital in overseeing AI that involves personal data collection and processing.
- Office of Electronic Communications (UKE) – UKE oversees Poland's telecom sector, potentially regulating AI in telecom infrastructure and services to ensure data, privacy, and security compliance.
- Polish FSA (KNF) – KNF oversees Poland's financial sector. In the past, it regulated the use of new technologies by the financial sector (including cloud computing), and it is expected to issue some recommendations on embracing AI.

5.2 Regulatory Directives

A legal definition of AI was adopted in the AI Act.

The European Commission approved the content of draft:

- guidelines on prohibited artificial intelligence (AI) practices; and
- guidelines on AI system definition aimed at clarifying the definition of AI systems.

These guidelines are not legally binding and may be updated in the future in response to new practices and insights.

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, **Softysiński Kawecki & Szlęzak**

5.3 Enforcement Actions

So far, the enforcement and other regulatory actions have limited scope. For instance, UODO is investigating a complaint about ChatGPT (see **8.2 Data Protection and Generative AI**).

6. Standard-Setting Bodies

6.1 National Standard-Setting Bodies

The Polish Committee for Standardisation (PKN), which creates and approves Polish Standards (PN), established a separate Technical Committee on AI. It is the lead Polish committee for international co-operation in international standardisation committees: ISO/IEC JTC 1/SC 42 AI and CEN/CLC/JTC 21 AI.

Currently, the committee's work agenda mainly includes translations of existing international standards. In view of the standardisation works at the European level (in relation to AI Act requirements), the significance of national standards will most probably be limited.

See also information about the AI Policy – **2.2 Involvement of Governments in AI Innovation**.

6.2 International Standard-Setting Bodies

The standards are usually intended for voluntary use by businesses, but in some sectors, compliance with such standards is deemed essential for the credibility and reliability of products.

European

Due to abstract nature of requirements imposed on providers of high-risk AI systems under the AI Act, harmonised technical standardisation will play a key role in operationalisation of these requirements.

European Commission issued a standardisation request to the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC). A joint committee by CEN and CENELEC (CEN-CENELEC JTC 21) is planning to provide more than 30 technical standards in relation to the AI Act.

In view of the delayed standardisation works at the European level and the upcoming entry into force of obligations of providers of certain high-risk systems under the AI Act (August 2026), implementation of the expected technical standards may prove challenging, especially for startups and SMEs.

International

- OECD – Framework for the Classification of AI systems: the framework allows users to zoom in on specific risks typical of AI, such as bias, explainability and robustness, yet it is generic in nature. It facilitates nuanced and precise policy debate.
- International Organisation for Standardisation (ISO) – BS ISO/IEC 42001:2023 Information technology. AI Management system specifies a certifiable AI management system framework under which AI-based products or services can be developed as part of an AI assurance ecosystem. AI standards enhance transparency, data quality, and system reliability, mitigating risks and maximising rewards. The National Institute of Standards and Technology (NIST) – AI Risk Management Framework (AI RMF). The NIST AI Risk Management Framework (AI RMF) is intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into designing, developing, using, and evaluating AI products, services, and systems.

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, Sołtysiński Kawecki & Szlęzak

7. Government Use of AI

7.1 Government Use of AI

Polish government is engaging with AI across various domains, and the known examples include:

- Virtual Assistant – chatbot using the GPT model, which will assist citizens while using mObywatel app (a mobile app offering access to digital official services and electronic documents);
- Virtual Civil Servant – Information Systems for eGovernment, is an advanced software for e-offices;
- PLLuM (Polish Large Language Model) – an initiative of Polish scientific institutions supported by the Ministry of Digital Affairs, which aims to create a Polish large language model; and
- STIR – the system, which is a set of algorithms introduced with the aim of analysing provided data obligatory by financial institutions (including banks) to the Polish tax authorities.

Digital Judicial Assistant (See 4.1 Judicial Decisions) “*Bielik*” LLM was created as a result of the work of a team operating within the SpeakLeash Foundation and the Academic Computer Centre Cyfronet of AGH Academy of Science and Technology as Polish large language model. AI is not widely used in the criminal justice system, but its use is thought to be very widespread. Currently, the most common example of using AI in this area is a general legal information system at the disposal of judges and prosecutors. This system includes a search system (for rulings, literature, etc) based on AI algorithms.

7.2 Judicial Decisions

This is not applicable in Poland.

In March 2025 the Ministry of Justice announced launching the “*Digital Court*”, the project that will encompass introduction of:

- Digital Judicial Assistant;
- the Electronic Writ Proceedings 3.0 (*postępowanie upominawcze 3.0*);
- Digital Court for Competition and Consumer Protection;
- Development of the Central Court Registry System;
- Redesign of the Information Portal; and
- Digital Data Exchange with the Public Prosecutor’s Office.

7.3 National Security

The AI Policy (see 2.2 **Involvement of Governments in AI Innovation**) emphasises the importance of AI in national security and encourages co-operation between the private and military sectors to address defence needs.

According to the recommendation to the National Security Strategy of the Republic of Poland (2024), AI creates new development opportunities for Poland while generating previously unknown risks, including loss of digital sovereignty. The recommendation highlights the importance of monitoring and responding to the development of emerging technologies, such as artificial intelligence and quantum technologies, within the context of security and international relations. Additionally, it emphasises promoting STEM (Science, Technology, Engineering, and Mathematics) education to improve technological competencies.

8. Generative AI

8.1 Specific Issues in Generative AI

The GAI raises many issues, the key (at the moment) including:

- data protection;
- confidentiality and IP;
- sector-specific regulations (such as banking or other financial services regulations, health rules, etc);
- ethical concerns (eg, ensuring lack of bias or discrimination);
- technical risks (eg, prompt injection, training data poisoning, lack of proper training data, etc); and
- general operational risks (eg, over-reliance, hallucinations, possible service disruptions, lack of employees with AI skills and lack of technological resources).

Copyright Protection

AI-generated results

Copyright protection of AI-generated output is limited since only humans can be considered authors under Polish law (as in most countries). The AI output cannot be considered as copyrightable work.

It may be claimed that AI is only a tool and AI-generated output can be copyrightable work as long as human oversight in its creation was significant and that all creative choices and decisions were made by a human, as with photography. This can apply only to specific examples and should be assessed case by case.

It's worth noting that this perspective is gaining more support among legal practitioners compared to the early stages of this discussion.

With regard to derivative (neighbouring) rights, such as rights to recordings of video or sound (as protection may be granted, eg, to birds' sounds), the rights may be allocated to individuals or companies.

The position with respect to the output ownership depends on the market. For example, MidJourney T&Cs provide that users of the commercial (paid) version of the platform are the sole owners of the content, while free version users only receive the licence for the personal use of such content. Users are responsible for the input and are obliged to indemnify MidJourney if there is any third-party rights violation due to such non-compliant input. Microsoft® Product Terms state that Microsoft® does not own the output of Generative AI Services.

The output may infringe on copyrights, other IP rights, or third parties. Therefore, some providers are following Microsoft's® customer copyright commitment to offer indemnification should a third party raise a claim that AI output infringes their IP rights. Such indemnification is usually subject to certain conditions (eg, using filters or content monitoring tools).

Moreover, the providers usually specify in their T&C if they use the output for training the model.

AI input

The input provided to AI systems can be protected as a standard work under copyright law, as long as it meets all the copyright law requirements (eg, originality and creativity). T&Cs usually specify whether the input will be used to train model.

AI system itself

An AI system itself can be protected under copyright law as the software. In Poland, as in the

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, Sołtysiński Kawecki & Szlęzak

whole EU, software is protected similarly to literature works, with some necessary modifications due to the nature of the computer programs.

Training data

Training data can be protected by copyright or by databases protection laws. However, there are discussions about whether the use of training data will be an infringement of copyright or may be based on text and data mining exemptions (once implemented in Poland). There are arguments raised that training the AI models is similar to learning from a book and consists of learning ideas or concepts that are not protected by copyright. However, no court cases have been raised in Poland against the model developers.

Trade secrets; know-how

Input, training data, software, and output can be considered trade secrets as long as the definition of the trade secret is met (eg, they have economic value, are kept confidential, and security measures are introduced to maintain their confidentiality). This may be relevant in cases where AI output cannot be protected (eg, software output).

8.2 Data Protection and Generative AI

The main data protection issues connected to GAI are:

- Lack of transparency of complex GAI models (the “black box” problem), which does not allow data controllers to assess the processing (in particular, to explain the automatic decision-making under Article 22 of the GDPR). To a certain extent, this risk may be addressed by more information provided by the model’s developers.
- No data minimisation, especially at the phase of training the models. Proper training data,

including anonymised information, regular reviews of data used at a given stage of training to eliminate incorrect data may limit this risk not only during model training or fine-tuning, but also the use of the model. When using GAI, users should implement policies and, when feasible, use technical tools (eg, filters) to mitigate the risk that personal data will be provided to the model unintentionally.

- No purpose limitation. Using personal data for training or fine-tuning the models may not be consistent with the purposes for which such data were collected. The controllers should assess whether they may process the data for such purposes and, if necessary, comply with additional requirements (Article 6.4 of the GDPR).
- No data accuracy in AI is challenging due to the risk of generating incorrect responses, including hallucinations. It is important to design models based on correct data, with safeguards and output filters (instead of changing the model weights), and for businesses to verify outputs and train users on prompt creation.
- Data subject rights should be respected, and there are no specific exceptions for GAI. Some AI companies provide guidelines on how to perform data subjects’ rights using their technology.
- It seems that false personal data in outputs could still be considered personal data and rectified when requested. However, there are also opposing views stating that they are only some projections about the data subject based on probability. The key question is whether data generated by AI can be linked to an identifiable person. If this is possible, the data can be considered personal data, even if it is incorrect. The EDPB opinion confirms that this will particularly be the case if the AI is expected to provide conclusions

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, Sołtysiński Kawecki & Szlęzak

(eg, personal data) about the persons whose personal data was used to train the AI.

If possible, the rights of data subjects should be respected. However, the difficulty in identifying and accessing personal data used to train the AI or in some cases – stored in AI models can be difficult. The risk of not being able to exercise the rights of the data subject can be minimised by implementing measures such as keeping a special register of traceable data, maintaining a management system that allows tracking the use of data and implementing data minimisation techniques at an early stage of system design. In particular, a request to delete data should not entail the deletion of the whole model. However, the model should be reviewed in order not to create future output with false data or data of a person who requested to have their data deleted. The right to rectification applies to both system input and output data. Consequently, the possibility of exercising this right must be taken into account at the AI design stage to avoid the risk of retraining the AI based on non-rectified data.

Guidance in this scope is expected following a complaint filed in Poland in September 2023 claiming a lack of data subject rights fulfilment and transparency in ChatGPT.

9. Legal Tech

9.1 AI in the Legal Profession and Ethical Considerations

The National Bar Council of Attorneys-at-Law (*Krajowa Izba Radców Prawnych*) has prepared recommendations for attorneys-at-law on the safe use of AI in legal work, including recommendations on how to prepare for the use of AI tools, on the implementation and application of

AI tools. As planned, the recommendations will be published in mid-May 2025.

There are no case law so far.

As for AI solutions, most law firms use standard AI tools, particularly for translation purposes or for achieving efficiency and improving the quality of work (eg, summarisation of meetings, drafting clauses, etc). The most common seems to be Copilot (including Microsoft 365® Copilot). AI tools are also used in e-discovery to identify relevant documents. Other solutions (eg, supporting drafting litigation documents) are often not adjusted to Polish law and, therefore, are of limited use.

The legal practitioners should ensure that:

- any AI-generated content is verified by a human;
- the confidentiality of the client's data is protected, and AI tools that use the input to train the models or which do not offer an appropriate level of protection are generally prohibited; and
- appropriate procedures and policies are implemented.

A legal adviser is obligated to observe professional secrecy and ensure that appropriate technical and organisational measures are in place to safeguard against its disclosure. Legal advisers should therefore ensure that AI tools are safe, among other things, by selecting a reliable AI tool provider, as well as assessing whether the use of a particular AI tool requires additional arrangements with client.

10. Liability for AI

10.1 Theories of Liability

Currently, the use of AI is subject to standard liability rules set forth in national laws.

Fault-Based Liability

The aggrieved persons need to prove the fault of the liable person, the damage and the causation between the fault and the damage to successfully bring a liability claim. In the context of AI, reliance on this principle is difficult, as often it may not be easy to find the person responsible or the cause (taking into account the lack of access to the model's "*construction*"). Compliance with AI manufacturer's instructions may shield users from fault while altering an AI code or using it for unintended purposes could attribute fault to the user.

Strict (Risk-Based) Liability

In specific cases, Polish law attributes liability to certain persons without the need of the aggrieved person to prove fault. An individual who operates an enterprise powered by natural forces (such as steam, gas, electricity, or liquid fuels) is liable for injuries or property damage resulting from the operation without the necessity to prove the fault. However, this provision does not apply in the case of AI, as providers of AI systems or models will not qualify as operators of enterprises powered by natural forces.

The risk liability also applies to the vehicle's possessor, though it is still necessary to prove the cause. Thus, its application will still be difficult if the damage caused by the AI system is applied to the vehicle.

Liability for Defective Products

The current rules, based on the implementation of Council Directive 85/374/EEC, do not allow

considering AI systems themselves as "*products*" within the scope of provisions related to defective products as they are exclusively movable items. AI systems cannot be classified as a movable product. However, please see section 10.2 Regulatory.

Contractual Liability

If the aggrieved party is using AI based on the contract, it may potentially claim the damage for breach of contract; it has to prove the breach, the damage and causation. There is a presumption that the alleged perpetrator is liable for the damage. However, they may prove otherwise. The risks outlined above to claim the damage caused by AI also apply to the contractual liability. However, the provider of AI solutions often offers additional measures, such as indemnity for third-party claims related to the infringement of IP rights by output generated by provided AI. On the other hand, in most business transactions, the parties limit the provider's liability (eg, up to 12 months' remuneration). The limitations or exclusion of liability will not be effective in contracts with consumers or the case of B2B if the damage is caused wilfully.

Liability for Infringement of Personal Interests

This is a fault-based liability. It is attributable to the person who uses the AI systems or the creations of AI systems without proper verification or with a false intent, eg, using deepfake technology. Besides the typical financial claims, the plaintiff may request the infringer to publish a given statement in the media.

Insurance Position

At the moment, there is no obligatory insurance similar to that necessary for the use of vehicles. Due to the confidentiality of model training, it is rather unlikely that insurance coverage will be

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, Sołtysiński Kawecki & Szlęzak

an affordable standard solution in the foreseeable future.

10.2 Regulatory

Directive 2024/2853 on the Liability for Defective Products Repealing Council Directive 85/374/EEC

The directive entered into force on 8 December 2024 and member states should make their legal systems compliant by 9 December 2026. While similar to the existing Directive on defective products from 1985, it introduces changes that could significantly impact the liability of AI systems.

It will cover not only physical goods but also software (especially damages for destroyed or corrupted data). The burden of proof will be simplified, and the aggrieved party will be able to claim material and mental damages (confirmed medically).

The Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to AI

The European Commission decided to withdraw the proposal of Directive in February 2025, but some members of European Parliament criticised it and discussions continue. Thus, the proposal has not yet been formally abandoned.

11. Specific Legal Issues With Predictive and Generative AI

11.1 Algorithmic Bias

Bias Characterisations and Risks

Algorithmic bias happens when the system discriminates against a specific group or individual, resulting from various factors, eg, biased training data, discrimination in data collection, a biased training team or defective parameters in

the models, or inappropriate deployment. Bias has not been explicitly defined in the Polish legal system. AI bias can affect the personal interests and freedoms of individuals, for example, by discriminating against them in a recruitment process or credit scoring, which may lead to claims for compensation and erosion of consumer trust.

Regulations and Industry Efforts

The GDPR introduces a human oversight requirement for processes that qualify as automated decision-making unless required by law. Human oversight can take different forms:

- Human-in-the-Loop (HITL), which involves human intervention in every decision cycle of the system;
- Human-on-the-Loop (HOTL) allows human intervention during system design and monitoring; and
- Human-in-Command (HIC) enables overseeing the overall AI activity and deciding when and how to use it in specific situations.

See also 13. AI in Employment.

Under Article 10 of the AI Act, in the development of high-risk AI systems that use data for training, validation and testing, it is crucial to adhere to quality criteria, such as data governance, examination for biases that are likely to affect the health and safety of persons or have a negative impact on fundamental rights or lead to discrimination prohibited under EU law.

Training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. The data sets shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, Sołtysiński Kawecki & Szlęzak

the high-risk AI system is intended to be used. Even when an AI system isn't deemed high-risk, it remains crucial for organisations to carry out their own risk evaluations to mitigate any potential adverse outcomes, including bias.

Transparency requirements arising from Article 13 of the AI Act also aim to ensure clarity and minimise bias in AI.

Article 14 of the AI Act requires that high-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way as to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations (feedback loops), and to ensure that any such feedback loops are duly addressed with appropriate mitigation measures.

11.2 Facial Recognition and Biometrics Legal Issues – Liability

The AI Act provides restrictions on using real-time and retrospective facial recognition, effective from February 2025:

- Facial recognition fall within the definition of “*biometric identification*”, as the face image is considered as “*biometric data*” under AI Act. Biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation are prohibited (with some exceptions for law enforcement) and using real-time remote biometric identification systems in publicly-accessible spaces for the purposes of law enforcement is prohibited (unless the use is strictly necessary for the objectives enlisted in the AI Act and specific obligations are met). Also, AI systems that

create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage are prohibited (Clearview AI case).

- Many biometric systems are considered high-risk AI systems and are subject to specific rules (eg, emotion recognition biometrics, biometric categorisation based on sensitive attributes).
- Post-remote identification AI systems are considered high-risk AI systems and are subject to specific rules. Importantly, law enforcement authorities may take no decision that produces an adverse legal effect on a person based solely on the output of such post-remote biometric identification systems.
- As a rule, deployers of emotion recognition or biometric categorisation systems should inform the natural persons exposed thereto of the operation of the system.
- Member states are able to adopt stricter rules regarding facial recognition in public spaces. Current Polish legislation did not provide such solutions.

The use of such systems is also subject to GDPR and local laws implementing the Data Protection Law Enforcement Directive (LED).

Risks

- Biological biometric data are uniquely personal and irreplaceable if compromised. The storage of such data poses a heightened risk of cyber-attacks, leading to severe consequences of identity theft or unauthorised access to secure systems if the data is breached. This risk is lower in cases of behavioural biometric data.
- The current AI systems used for facial recognition may generate unreliable results, in particular with people of different races or

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, **Softysiński Kawecki & Szlęzak**

ethnic origins. Also, the systems may not work properly with women.

- Use of facial recognition technology can lead to privacy infringements and discrimination.
- There is a high risk of misuse of such technologies.
- Ethical concerns over facial recognition involve debates on surveillance and mass tracking.

11.3 Automated Decision-Making

Automated Decision-Making (ADM) employs algorithms and AI systems to automate tasks traditionally requiring human insight, learning from data to predict outcomes.

Risks

In terms of risks, ADM systems can inherit biases (section 11.1 **Algorithmic Bias**). ADM models often lack transparency, leading to mistrust.

Applicable Rules – Article 22 of the GDPR

- GDPR restricts automated decision-making that produces legal effects or significantly affects individuals.
- Individuals have the right not to be subject to decisions based solely on automated processing. Exceptions exist, eg, a decision necessary to conclude or perform a contract.
- GDPR requires that a data protection impact assessment be carried out before data processing begins.
- There are views that the data subject has the so-called “*right to reasonable interferences*”, ie, the right to challenge the conclusions made by AI, and not just the decisions based on these conclusions. The basis for formulating such a right is to be a synthetic interpretation of the right to rectification, the principles of lawfulness, fairness and transparency, and the principle of accuracy.

- Failure to comply could result in liability under GDPR.
- Article 29 Data Protection Working Party Guidelines on Automated Individual Decision-making and Profiling for the purposes of Regulation 2016/679 specifies the rules resulting from the GDPR.

European Parliament Resolution on Automated Decision-Making Processes indicates that when consumers are interacting with ADM, they should be properly informed how it functions, how affects a human with decision-making powers, and about how the system’s decisions can be checked and corrected.

- Existing regulatory frameworks cover aspects relevant to services incorporating ADM, including consumer protection, ethics, and liability.
- Since the “*human-in-the-loop*” approach is currently being applied by AI developers, ie, AI is mainly used to support human decisions, not to replace them, in practice the restrictions imposed on ADM by the GDPR may not be applied very often at the moment.

DSA

- The DSA aims to enhance algorithmic transparency and accountability, targeting intermediary services with additional specific requirements for online platforms and VLOPs.
- Noncompliance may lead to liability under DSA.

AI Act

- Deployers must inform individuals when high-risk AI systems are used in decision-making that affects them, eg, those affecting the terms of work-related relationships.

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, **Softysiński Kawecki & Szlęzak**

- The AI Act is set under specific conditions – a right to a meaningful explanation when an AI system is used to make a decision.
- Non-compliance may lead to liability on the AI Act.

11.4 Transparency

The principle of transparency is one of the basic principles introduced by the AI Act. This principle will be applied from 2 August 2026.

- Transparency for AI systems:
 - (a) Providers must design AI systems that directly interact with natural persons in a way that informs users they are interacting with an AI system.
 - (b) Exceptions apply when it is obvious to a reasonably well-informed person that they are interacting with an AI system.
 - (c) Legal authorisation may exempt certain AI systems used for criminal offence detection, prevention, investigation, or prosecution.
 - (d) How a high-risk AI system functions should be transparent so that the user can comprehend and use the output suitably.
- Marking outputs:
 - (a) AI-generated outputs (such as audio, image, video, or text) must be marked in a machine-readable format and detectable as artificially generated. Some exceptions apply (eg, for an artistic activity or if systems used do not significantly alter input data). Legislators may also exempt certain AI systems; stricter rules apply to deepfakes.
- Text content for public information:
 - (a) Deployers must disclose if text content published with the purpose of informing the public on matters of public interest is artificially generated or manipulated.

- (b) Exceptions apply when authorised by law for criminal offence detection or if the content undergoes human review.

Providers of general-purpose AI models are required to make publicly available a detailed summary of the content used to train the model, particularly text and copyrighted data.

12. AI Procurement

12.1 Procurement of AI Technology

The procurement of AI technology in Poland can be implemented by two groups of entities: private entities or public entities.

Private Entities

In cases of private entities, the principle of freedom of contract applies. The current key issues which would have to be addressed in contracts for procurement of AI solutions include the following: whether the input or output data are used to train the models, ownership of output, liability and warranties, IP-related issues (in particular, dealing with third-party claims to the model or output), use of personal data (processor, controller, joint controller), data flows, location of input, output and model, abuse monitoring and content filtering, possibility of suspension of services in cases of abusing services or due to political tensions, supply chains.

Public Entities

Public entities may be obliged to conclude the contract for AI technology under public procurement rules, and they often provide a template contract in the contracting documents. As they are not experts in AI, the proposed contracts may not address relevant risks and may not be consistent with market standards. Therefore, it is recommended that public entities carry out two-

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, Sołtysiński Kawecki & Szlęzak

step procedures or negotiations to first precisely identify its goals and the way in which they may be achieved.

13. AI in Employment

13.1 Hiring and Termination Practices

Employers are not allowed to use AI systems to reach conclusions about a job candidate's/employee's emotions, except where it is intended to be put in place or into the market for medical or safety reasons.

The employer will have additional obligations when using following AI systems, which are classified as high-risk AI:

- AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates; and
- AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships.

Employers utilise tech and software for recruitment and termination processes to save costs and time. Notwithstanding the regulation of the AI Act, employers must adhere to general anti-discrimination and privacy laws:

- Discrimination in employment is prohibited, including during hiring or termination. Technology use must avoid any discrimination unrelated to work.

- Employers are responsible for the technology they use and can face claims for compensation or damages in discrimination cases if such use leads to that effect.
- The Polish Labour Code specifies that personal data is permissible in hiring and employment; technology use, including AI, must not violate privacy regulations.

13.2 Employee Evaluation and Monitoring

Employers use various digital tools to evaluate employees' performance, track working time, and review employees' work or use of resources. There are also AI tools that can provide real-time feedback on an ongoing basis, informing employees of their progress and areas for improvement. If the technology is used to monitor employees' email and/or activity, such monitoring should be introduced in a formal way via relevant internal policies and procedures, announced to employees, and applied within their frameworks. It cannot infringe on the integrity of correspondence or on an employee's personal interests.

The breach of the rules may result in employees' claims for breach of their rights by illegal monitoring and compensation. It may also constitute a breach of privacy laws.

14. AI in Industry Sectors

14.1 Digital Platform Companies

Using AI on digital platforms should be assessed in light of the Digital Services Act (DSA). Most of all, the following conclusions shall be kept in mind:

- In principle, providing GAI or solutions based on such models (eg, conversational solutions

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, Sołtysiński Kawecki & Szlęzak

such as chats) will not constitute an indirect service within the meaning of the DSA.

- However, to the extent that providers of indirect services are also suppliers or operators of AI systems, they may be obliged to take certain actions under the AI Act.
- Information generated or modified by AI that is not marked in accordance with the AI Act should be considered illegal content within the meaning of the DSA. Also, even if properly marked, information may be illegal under the DSA, particularly if it refers to content that is illegal or describes illegal activities.
- Due to varying requirements posed by the regulations, a risk analysis conducted under the DSA may not be sufficient under the AI Act.

There are no specific rules regarding employment in Digital Platform Companies (see also section 13. AI in Employment).

14.2 Financial Services

Financial services institutions (FSI) are very focused on innovation, including AI. For example, a Polish bank implemented a chat service for customers, which informs customers about the bank's services and analyses customers' transactional data. FSI are also interested in services that automate internal activities, eg, anti-money laundering and anti-fraud purposes.

There are no legal provisions regarding specifically AI in FSI (except for application of AI in credit scoring systems, which may fall into the AI Act high-risk systems rules). However, financial services are highly regulated and introducing new technologies is usually subject to complex obligations:

- If AI is used by FSI to process banking, insurance or other statutory professional secrets,

regulations regarding outsourcing (including potential non-EEA outsourcing) may be applicable. Outsourcing definitions vary across regulations in Poland's financial sector. After repeal of so-called Cloud Communication, the assessment of cloud based AI solutions should be carried out considering such outsourcing rules.

- Automated decision-making by an FSI (which can be supported by AI) is subject to additional restrictions resulting from local legislation, especially where it is made to assess creditworthiness and analyse credit risk. AI Act may apply to credit scoring systems using AI, if qualified as high risk systems (see Approval of the content of the draft Communication from the Commission – Commission Guidelines on prohibited artificial intelligence practices established by AI Act)
- In the scope of using AI for robo-advisory, the FSI should take into account the FSA position on the provision of robo-advisory services – see section 3.3 Jurisdictional Directives.
- EU-wide guidelines (eg, the EBA Discussion Paper on ML for IRB Models) may also be considered.
- FSIs that implement AI should take the risks related specifically to AI into account, including the risk of bias (see 11.1 Algorithmic Bias) or opacity and non-transparent decision-making (see 11.4 Transparency). On top of that, the FSI should take into account standard risks applicable to its operations, including ensuring the confidentiality of professional secrets and business continuity.

14.3 Healthcare

New technologies may be highly beneficial for the healthcare sector. ML algorithms may analyse big datasets and entail accuracy and speed in healthcare providers/health research activity. ML and AI can assist in diagnosis and disease

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, **Softysiński Kawecki & Szlęzak**

management, interpreting medical images, drug discovery, operations. Also, new technology may enable the use of new ways of collecting data and providing health assistance, eg, telemedicine/chats or wearable technology. However, especially in Polish public sector, the adoption of AI in healthcare is limited by the restrictions in using the cloud computing through which such AI solutions are often offered. Some restrictions in this area were removed in October 2024 but the works still continue.

Regulations and Main Issues

There are no regulations related specifically to using AI in healthcare and connected ML. The general regulations will apply, ie:

- The AI Act.
- The GDPR, as supplemented by special Polish provisions related to processing data in the medical context.
- Provisions regulating medical secrets.
- AI may constitute a medical device and, as a consequence, be subject to applicable regulations (eg, Medical Devices Regulation (MDR) and In Vitro Diagnostic Medical Devices Regulation (IVDR)). If the AI were to become a part of another medical device, then such a device would have to meet the regulatory requirements. The burden would generally be placed on the manufacturer/importer of such a device.
- Data sharing, including for better healthcare delivery and training AI, is covered by the Data Act and will be governed by the EU Regulation on European Health Data Space.

Risks

- Bias in AI – Risks related to bias are described in **11.1 Algorithmic Bias**. In healthcare, AI's decision-making can significantly affect patient life.

- Over-reliance and misuse – AI users may struggle to evaluate AI outputs, including their origins, hindering proper verification.
- AI errors causing patient harm and liability – AI errors (eg, stemming from flawed data or mistakes in its design) can cause misdiagnosis or incorrect medical interventions, potentially resulting in physical harm during AI-assisted surgery (see **10. Liability for AI**).
- Transparency and privacy/security issues – healthcare AI's main privacy risks include misuse of patient data, breaches exposing sensitive information, and harmful cyberattacks, especially with medical records and live health data devices.

14.4 Autonomous Vehicles

Polish law generally prohibits the use of autonomous vehicles (AVs); however, automation features under the supervision of a human driver can be used. There is an exemption for approved research testing on public roads, but not every type (level) of an AV can currently be tested on Polish roads – only vehicles at level 3 of automation can be tested in Poland. There are no AI-specific regulations, however the Road Traffic Act provides a definition for the purposes of conducting controlled AVs testing, under which AV means a motor vehicle fitted with systems which control the movement of the vehicle and enable it to move without intervention from the driver, who may take control of the vehicle at any time. The Ministry of Infrastructure intends to facilitate testing autonomous vehicles on all levels of automation and their equipment on public roads in near future.

Liability

The standard vehicle liability rules also apply to AVs (see section **10. Liability for AI**). Motor vehicle users are required to hold mandatory insurance for civil liability.

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, Sołtysiński Kawecki & Szlęzak

Significant Issues

In the AI Policy, it is acknowledged that AI-based systems used in autonomous transport can significantly lower the number of accidents – and, as a result – the number of fatalities. However, using AVs is linked to certain issues and risks, ie:

- Privacy and safety – AVs may collect a vast amount of personal data, which may pose risks to privacy. Also, the systems used in AVs may be subject to cyber-attacks, threatening the safety of users.
- Ethical concerns – AI in AVs may encounter scenarios requiring moral judgement, touching upon significant ethical concerns.
- Responsibility – assigning accountability for the decisions made by AI involves multiple parties.

14.5 Manufacturing

There are no specific regulations related to using AI in manufacturing – the rules related to liability are described in section 10. **Liability for AI** and the employment issues are described in section 13. **AI in Employment**. Data privacy applies. The rules regarding product safety are based on the Machinery Regulation, which generally aims to cover new technologies. AI may be beneficial to reduce the size of the workforce. However, as AI will automate certain activities, it may lead to layoffs, increased unemployment and loss of competencies. Manufacturers may be one of the key sources of data for training AI based on the Data Act.

14.6 Professional Services

There are no specific regulations related to using AI in professional services; thus, the rules related to liability described in section 10. **Liability for AI** will apply. Providing some professional services is covered by sector-specific regulations and ethical rules (eg, legal services) and using

AI should enable compliance with them. Most importantly:

- Confidentiality – providing professional services may be subject to specific professional secrecy rules (eg, lawyers). Professionals should ensure that they provide client data only to AI systems that ensure confidentiality (including the performance of legal obligations and compliance with engagement letters signed with clients) or refrain from providing such data in their prompts.
- Compliance – professionals may implement internal policies for their businesses to ensure proper AI usage.
- Need of supervision – professional services require knowledge and insights into the specific situation of a client. While it can be supported by AI, outputs provided by AI should be verified by humans.

15. Intellectual Property

15.1 IP and Generative AI

There are no binding laws or regulatory intentions with regards to IP and AI in Poland. There are also no administrative or judicial decisions in this respect. See 8.1 **Specific Issues in Generative AI** for general remarks regarding the relation between IP and generative AI.

15.2 Applicability of Patent and Copyright Law

There are no decisions in Poland relating to whether AI technology can be an inventor or co-inventor for patent purposes or an author or co-author for copyright purposes.

The prevailing view is similar to one presented already in the USA or other countries in the EU, ie, that AI-created works or inventions cannot be

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, **Sołtysiński Kawecki & Szlęzak**

copyrighted or protected by industrial property law.

Patent Law

With regard to patent protection, only a human can be an inventor. It was confirmed in the DABUS case in which both the European Patent Office and later the Board of Appeal refused patent protection for an AI system.

Copyright Law

In Poland, copyright protection arises by operation of law. There is no need to file an application, and there is no Copyright Office. Disputes relating to copyright infringements are decided by special IP departments of common courts.

Recently, in the EU, the first case regarding copyright ownership of AI creations was decided when a Prague court ruled that DALL-E creations aren't copyrightable as they're not human-made. Additionally, the Union of Authors and Composers for the Performing Arts in Poland, the largest copyright collective management organisation, has amended its regulation on submitting and registering works. Under this regulation, AI-created works are generally excluded, but it is possible to register a work co-created with AI. In such cases, the human creative input must be quantified by a percentage indicator.

15.3 Applicability of Trade Secrecy and Similar Protection

Contractual Provisions

Non-disclosure arrangements are the common legal instruments to protect AI technologies and generated content. However, it is limited to the parties and is not generally enforceable like IP protection, which applies to all potential violators.

Trade Secrets

AI technology, training data, input, or output may be protected as trade secrets, as they do not necessitate human authorship. As confidentiality is one condition of such protection, appropriate instruments must be in place (eg, non-disclosure contracts).

15.4 AI-Generated Works of Art and Works of Authorship

The prevailing view is that the creator of copyright-protected works can be human only; however, video or sound output may be protected as derivative rights. Additionally, AI systems can be regarded as tools in the creation process, provided that the human contribution is significant enough.

See 8.1 Specific Issues in Generative AI.

15.5 OpenAI

Using OpenAI while creating works and products is generally associated with the same risks as using other GAI systems.

16. Antitrust

16.1 Emerging Antitrust Issues in AI

The Polish authorities do not currently use AI in assessment of their cases. They have not seen AI-related transactions or practice either.

17. Cybersecurity

17.1 Applicability of Cybersecurity Legislation to AI

Currently in Poland, there is the National Cyber Security System Act (NCSSA), which defines the organisation of the national cybersecurity system and the tasks and responsibilities of the

Contributed by: Agata Szeliga, Michał Kalinowski, Maciej Gil, Sylwia Macura-Targosz and Anna Tujakowska, **Softysięski Kawecki & Szlęzak**

entities that are part of this system. The legislation is undergoing legislative work aimed at increasing the level of cybersecurity in Poland – including addressing challenges related to AI. The new regulations will be flexible and applicable to increasing the scope and speed of malicious actions, including those involving AI and LLMs usage. The amendments to the NCSSA are going to implement the EU NIS-2 Directive, which provides new cybersecurity requirements and extends obligations to many entities from various sectors.

18. ESG

18.1 ESG Dimensions of AI

ESG/sustainability reporting regulations in the EU and Poland do not prohibit the use of AI for the purposes of reporting itself. However, given that the reporting regulations are new and only a limited number of reports drawn up in accordance with the recently adopted standards have thus far been published, the usability of AI in the drafting of reports may be limited by insufficient input data.

AI may, however, play a significant role in the analysing of vast amounts of data involving environmental metrics (such as carbon emissions, energy consumption, and waste management figures), social metrics (like employee diversity, labour practices, and community engagement) and governance metrics (board composition, executive compensation, and ethical business practices). In this field, AI may assist companies in identifying trends, assessing risks, and making informed decisions, thereby enhancing their sustainability efforts.

19. AI Governance and Compliance

19.1 AI Governance and Best Practice Compliance Strategies

Based on market practice, the following best practices are usually adopted in organisations implementing AI solutions.

- Identification and understanding of use cases that involve the use of AI.
- The verification of potential AI solutions and terms and conditions of contracts for the use of such AI (see **15.3 Applicability of Trade Secrecy and Similar Protection**).
- Careful assessment of potential risks and the methods by which they may be mitigated.
- Regularly assessing AI systems for potential biases, particularly in high-impact use cases (eg, recruitment, lending, and public services).
- Introduction of policies and rules for using AI in an organisation.
- Implementing human supervision.
- Ensuring transparency, eg, providing information on the use of AI in the case of chatbots or within an organisation.
- Involving ethics boards or advisory committees to evaluate AI implementations, especially those affecting individuals' rights.
- Regular updates and re-evaluations of AI models to ensure continued performance and compliance.
- Comprehensive and continuous training for employees, ensuring that relevant staff understand how AI systems work, their limitations, and how to use them responsibly and effectively.

Trends and Developments

Contributed by:

Agata Szeliga

Sołtysiński Kawecki & Szlęzak

Sołtysiński Kawecki & Szlęzak is one of Poland's leading full-service law firms. With more than 180 attorneys, the firm provides the highest standard of legal services in all areas of business activity and is well-reputed for the quality of its work and innovative approach to complex legal problems. Since the 1990s, Sołtysiński Kawecki & Szlęzak (SK&S) has been closely associated with the ever-changing technology sector, especially the dynamically devel-

oping IT industry. The firm provides high-quality legal services to both individuals and companies, covering the full scope of TMT issues. The team works alongside the firm's fintech, IP/IT, privacy and tax teams to provide an innovative interdisciplinary service and to help businesses use state-of-the-art technologies in a safe, cost- and time-effective manner. SK&S was the founding member of the New Technologies Association.

Author



Agata Szeliga has been a partner at Sołtysiński Kawecki & Szlęzak since 2009 and joined the firm in 1998. She specialises in new technologies, personal data protection, state aid, and

public procurement. Agata has advised on cloud computing for many years, especially in the financial sector. She also advises on AI and the sharing of data generated by devices and applications. Agata is a member of the European Commission's Expert Group on B2B data sharing and cloud computing contracts.

Sołtysiński Kawecki & Szlęzak

Jasna 26 Street
00-054 Warsaw
Poland

Tel: +48 22 608 70 00
Fax: +48 22 608 70 01
Email: office@sklegal.pl
Web: www.sklegal.pl



Implementing AI in Poland

Background

Last year was a year of growing adoption of AI in Poland. In 2024, Polish companies spent more than EUR400 million on AI technologies and they declared plans to increase their expenditures for new technologies in the coming years. According to OpenAI, Poland is in the top five of users of Open AI models in Europe. According to the Eurostat study, Poland also significantly increased the use of cloud services (55.7% of enterprises bought such services in 2023 compared to 28.7% in 2021). However, there is a growing split between the use of AI in the private sector which has been faster to embrace AI technology, and the public sector which has been slower.

Poland as a part of the AI Continent

On 9 April 2025, the European Commission announced its AI Continent Action Plan to make the European Union a global leader in AI. The European Commission intends to spend EUR200 billion to boost AI development in Europe. The AI Continent Action Plan was finalised during Poland's EU Council presidency. Polish authorities stressed that they aim to speed up investments and promote AI development, in particular, through participating in this plan.

The AI Continent Action Plan focuses on five key areas:

- developing computing infrastructure,
- ensuring access to high quality data,
- accelerating AI adoption in key sectors and public administration,
- building AI skills and literacy, and
- properly implementing the AI Act to ensure safe and trustworthy AI across the EU.

Concerning computing infrastructure, the European Commission envisages establishing AI factories to provide computing resources for AI model development. These factories will integrate supercomputers, data resources, and human capital. The first AI factories will be hosted in 13 member states with one being established in Poznań, Poland (AIF Piast). There is also a plan to establish AI Gigafactories developing large-scale facilities with massive computing power dedicated to developing and training next-generation AI models containing trillions of parameters, with an aim towards Artificial General Intelligence (AGI). Gigafactories should promote collaboration between scientists based on the successful CERN model. The Commission also notes the need to increase current cloud and data centre capacity. The goal has been set to at least triple the EU's data centre capacity within the next five to seven years. The new legislative proposal, Cloud and AI Development Act, will support this initiative.

High quality data is essential for AI development. To ensure access to such data, the Commission plans to set up Data Labs which will be a part of the AI Factories initiative. The Data Labs will aggregate, clean, and enrich the data from different AI factories covering the same sectors; they will link various European data spaces and make the data available to AI developers.

The EU also plans to accelerate AI adoption both in public and private sectors through the Apply AI Strategy. The following private sectors were identified as having the highest potential for AI adoption: advanced manufacturing, aerospace, security and defence, agri-food, energy and fusion research, environment and climate, mobility and automotive, pharmaceutical, biotechnology, advanced materials design, robotics, electronic communications, cultural and

creative industries, and science. AI has the greatest potential to enhance public services in healthcare, justice, education, and public administration.

Within the initiative to build AI skills and literacy, the Commission will increase the overall provision of EU bachelor's and master's degrees and PhD programmes in key technologies, including AI. The Commission will also focus on increasing the number of AI experts working in the EU. To do so, it will make efforts to encourage European AI talents to stay or to return to the EU, as well as attract non-EU personnel to relocate to Europe. In co-operation with member states, the Commission intends to support the upskilling and reskilling of professionals in all fields in the use of AI.

As to the proper implementation of the AI Act, the Commission will launch the AI Act Service Desk. This will be a central information hub based on the AI Act and will allow interested parties to ask for assistance and receive tailor-made answers.

Polish government and parliamentary activity

Poland's activities seem to be rather modest when compared to the European Commission's plans. However, on the legislative front, some obstacles will be removed in developing and implementing AI, as well as preparing for the implementation of the AI Act.

In September 2024, the provisions allowing enterprises to conduct data and text mining were finally introduced into Polish Copyright Law with an opt-out option for copyright holders. However, the absence of technical standards currently makes it challenging to implement the opt-out option effectively. On the positive side, the initial proposal to prohibit the possibility to

apply this exemption in training AI models were abandoned during legislative work.

Poland has also adopted the Law on Electronic Communication which implements the Directive (EU) 2018/1972 establishing the European Electronic Communications Code. These provisions entered into force in November 2024 and remove some regulatory obstacles, eg, for conducting activities in non-public networks.

In October 2024, the Polish government also modified its Resolution on the Common IT Infrastructure of the State in which it allowed the use of the public cloud, ensuring the storage of data at rest in the EU to process public systems and registers containing health or other sensitive personal data (with exceptions for military and law enforcement agencies). This is perceived as a first step to allowing the use of AI solutions offered in software as a service mode in the public sector. However, public sector representatives stress that the Polish government document setting up the cybersecurity standards for cloud computing services still needs to be amended to enable the public sector to use public cloud services.

The Polish Act on AI Systems, aiming to ensure effective implementation of the AI Act, is still in progress. A new draft was proposed in February 2025. According to the initial plans, the Act on AI Systems was to be adopted by the end of the first quarter of 2025. As the second round of public consultation progresses, the timeline for the final adoption of the act remains uncertain.

The draft still provides that there will be a separate regulator in the AI field – the Committee of Development and Safety of AI. However, its composition was modified. Except for the chair and vice-chairs, it will include representatives of

seven other regulatory bodies (such as Financial and Telecom Regulators, or a representative of the Office of Competition and Consumer Protection which is also responsible for product safety in Poland). In January 2025, the Polish Data Protection Authority (UODO) raised several concerns about the compliance of the first draft with the AI Act principles. Some of UODO's comments have not been fully reflected in the second draft. Furthermore, following the amendments proposed in the second version of the Act, the Chair of the Committee will be appointed by the Lower House of the Polish Parliament (the *Sejm*), with the consent of the Upper House (the Senate). This will delay the process of appointing the Committee. Currently, there is no public information on potential candidates for this post.

The draft includes some measures which aim to support investments in the area of AI. One is the possibility of establishing regulatory sandboxes and granting providers or deployers consent to derogate from the AI Act's application by way of an individual decision of the Committee's chair. The participation of an entity in the regulatory sandbox for one project should last no longer than one year and can be extended once for no more than six months. The participation of micro, small and medium-sized enterprises in the regulatory sandbox will be free of charge. The fee for other entities' participation may not be higher than four times the minimum wage. Another instrument supporting AI investments involves the Ministry of Digitalization issuing recommendations on best practices for using artificial intelligence systems.

In April 2025, the Minister of Digitalization proposed an amendment which will allow a virtual assistant to be offered based on the general purpose AI model in the state digital app – mObywatel, which offers, in particular, access to digital ID

documents and other state services. However, the draft law states that virtual assistants cannot use application users' personal data. The Bill is currently under review by the Polish Parliament.

Impact on employment

With the rise of AI tools, more professionals worry that AI solutions may decrease employment. Various studies indicate that nearly half of the tasks performed by lawyers may be automated through AI. We can already see that deploying standard AI tools such as Microsoft 365® Copilot may significantly increase the effectiveness of lawyers and other professionals in their daily work.

The Polish Ministry of Digitalization has issued a draft list of endangered professions which included, amongst others, lawyers, developers and finance advisers. The list received significant criticism from various sources.

The approach towards AI in the legal community differs – from those who reject it to those who believe that it will not be possible to practice law without AI. The Polish National Council of Legal Advisors decided to take a pro-active approach, and, on 13 May 2025, it issued a recommendation on how legal advisers should use AI-based tools. The guidelines should help legal advisers to responsibly and safely apply AI tools to ensure the protection of client-attorney privilege. The recommendation will also indicate when the client should be informed about an attorney's use of AI, and when the client's consent should be obtained for such use. It is expected that the recommendations will be a living document, being adjusted as AI solutions develop.

AI solutions have been initially deployed in the judiciary. In particular, one Poznań court is testing an AI tool that supports administrative tasks

related to claims based on Swiss-denominated mortgage agreements.

It is expected that the wider application of AI tools may lead to a decreasing demand for junior lawyers and for lawyers who perform simple, repetitive work, for example, preparing statements of claims or responses in very similar cases. On the other hand, one may expect the demand for lawyers with AI skills to grow.

Impact on education

AI is slowly changing the education sector. Some technical universities, in particular, in Poznań or Cracow, opened new bachelor's degrees focusing on AI. AI also became part of standard programmes for training developers and experts in robotics, automation, or applied mathematics. Postgraduate studies focusing on building expertise in data science, AI, or machine learning are becoming evermore popular. The author does not yet observe education programmes being liquidated solely due to AI; however, in some cases, universities note reduced interest. AI is also changing teaching methods. AI-based chatbots may be used to answer students' questions. AI is increasingly used to create training materials. There are also challenges related to the examination standards.

Setbacks

Poland initially suffered a setback in AI development, not being included in the list of US-allies having full access to AI-related chips. Under US export control rules issued in January 2025, Poland was classified within the second-tier group alongside approximately 100 other countries. These nations will encounter restrictions in accessing the most advanced AI chips and other AI technologies. The Polish government has voiced its concerns about that decision, as has the European Commission. In May 2025, there was unofficial information that these restrictions will be waived. On the other hand, the Chinese model, Deepseek, has shown that access to the most advanced AI chips is not necessary to develop AI models that may compete with the most advanced models.

Summary

In general, the Polish authorities are supportive of AI. However, legislative action is rather slow and limited to ensuring compliance with EU legislation. Concerning business, AI use is growing. Companies are now focusing on standard models and solutions. Fine-tuning or creating large language models from scratch is still uncommon. The public sector is lagging behind as it has not often even adopted cloud technology and usually still works on documents using hard-copies.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com