Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Artificial Intelligence 2026

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

Poland

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

Trends and Developments
Agata Szeliga
Sołtysiński Kawecki & SzlęzakP

POLAND

Law and Practice

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

Contents

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

Sołtysiński Kawecki & Szlęzak is one of Poland's leading full-service law firms. With more than 200 attorneys, the firm provides the highest standard of legal services in all areas of business activity and is well known 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 developing 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 SK&S since 2009. 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 as well as on IP and AI-related matters in M&A transactions. She was a member of the European Commission's Expert Group on B2B data sharing and cloud computing contracts. She has published widely and is a regular lecturer on postgraduate programmes focusing on AI and data sharing.

Michał Kalinowski is an associate at SK&S 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 Wyszynski University in Warsaw, conducting research on AI creations from the perspective of copyright law.

Maciej Gil is a senior associate at SK&S. He joined the firm in 2017 and specialises in IT, AI, e-commerce and IP law, including industrial property, unfair competition and copyright. Maciej has experience in licensing, technology transfer, litigation and other IP/IT matters. He also advises on IP and AI-related matters in M&A transactions.

Sylwia Macura-Targosz is a senior counsel at SK&S, specialising 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.

Anna Tujakowska is a senior counsel and head of Legaltech & Innovation at SK&S. She advises and represents clients in international and domestic commercial arbitration disputes. Anna also has extensive experience in international and investment arbitration, and additionally serves as an arbitrator. She integrates her arbitration expertise with AI-related matters and supports clients in projects related to the use and implementation of AI.

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

Sołtysiński Kawecki & Szlęzak

Jasna 26 Street
00-054 Warsaw
Poland

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

1. 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; the "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 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-only 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) or potentially when it is treated as a tool performing creative human instructions.
- 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.

Experience has shown that 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).
- More sophisticated use scenarios to solve particular problems are growing: in particular, AI systems are increasingly applied in medical imaging and laboratory diagnostics or in defence products.

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 AI adoption are limited and include the following.

- AI Policy adopted by the Council of Ministers in 2020 to advance AI development for societal, economic and scientific benefits, updated in November 2025 as the Policy for the Development of Artificial Intelligence in Poland until 2030, aiming to build a co-ordinated national AI ecosystem.
- Financial support for AI factories, including Poland's AI factory (PIAST) at the Poznań Supercomputing and Networking Center, and efforts to secure one of five EU-funded AI gigafactories in Poland.
- Establishment of the PL/AI advisory group (early 2024); a letter of intent to launch the Artificial Intelligence Fund (approximately PLN1 billion, November 2024); and a Breakthrough Technology Development Fund proposed in a draft presidential bill to channel billions of złoty annually into strategic areas including AI.
- Activities of the National Centre for Research and Development (eg, grants and IDEAS NCBR); establishment of a Standing Subcommittee on AI innovation and the Ministry of National Defence's AI strategy to 2039 (August 2024). 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, the work on an act implementing the AI Act has been finalised at the government level – see **3.7 Proposed AI-Specific Legislation and Regulations**.

3.2 Jurisdictional Law

Under new legislation, mObywatel application – the Polish government digital services platform – is required to provide a virtual assistant functionality based on a general-purpose AI model (Article 3 (63) AI Act), with the explicit statutory restriction that it may not process the personal data of application users. This is the first binding regulation in Poland referring to the AI Act.

3.3 Jurisdictional Directives

Policy, Guidelines and Recommendations

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, the Ministry of Digital Affairs an published its recommendations on prohibited AI systems and associated provisions of AI Act.

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 tool.

AI Policy in Poland to 2030

The Policy published in 2020 has been updated in 2025. It sets out an action plan structured around five objectives:

- building a co-ordinated AI ecosystem;
- developing societal AI competences;
- deploying AI in public administration;
- driving AI adoption in key economic sectors; and
- ensuring trustworthy, human-centred AI in compliance with the EU AI Act and GDPR.

Implementation will be co-ordinated by the Minister for Digitalisation with a new national supervisory body.

Declaration of Principles for the Ethical Use of Artificial Intelligence Models

The "Solidarność" Trade Union of Judicial and Prosecutorial Employees has adopted a Declaration of Principles for the Ethical Use of Artificial Intelligence Models. The declaration focuses on human responsibility, data protection and privacy, integrity and transparency, balance between technology and experience, critical thinking and verification.

Guidelines on Artificial Intelligence for Public Administration

In March 2026, the Ministry of Digital Affairs issued its guidelines for public administration on the use of AI. It includes also the most common use cases and deployment recommendations.

3.4 EU AI Act

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 Approaches to Liability for AI**), in addition to sector-specific EU product regulations.

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 specific Polish laws have been introduced or amended in relation to data, information or content used for AI training. Implementation of the 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 May 2026, 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, such as GDPR, the Digital Services Act or the Data Act.

3.7 Proposed AI-Specific Legislation and Regulations

The draft Polish Act on AI Systems has been finalised at the government level and will now proceed to the Polish Parliament for further legislative work. The draft includes provisions on the following.

- Establishment of a national market surveillance authority for AI systems (AI Development and Security Committee), the administrative support of which shall be provided by the office of the minister responsible for digitalisation. The Committee will also act as a single point of contact within the meaning of the AI Act. A Social Artificial Intelli-

gence Board will be established as an advisory and consultative body to the Committee.
- Regulations concerning the oversight of the market for AI systems and general-purpose AI models.
- Procedures concerning infringement of the AI Act, including a settlement mechanism enabling extraordinary mitigation of sanctions (by between 20% and 90% depending on the circumstances) where the infringing party co-operates with the Committee and remedies the breach.
- Rules for imposing administrative fines for infringements of the AI Act.
- Provisions on 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; the opinion is binding on the Committee and other public authorities involved in its issuance.
- Regulations on regulatory sandboxes.
- Conditions and procedures for accreditation and notification of conformity assessment bodies.

See also **5. AI Regulatory Oversight**.

4. Case Law

4.1 Precedent-Setting Judicial Decisions

There has been one final decision related to AI in Poland. The National Appeal Chamber (KIO) ordered a roads authority to re-examine bids in a public tender for road maintenance after the winner had used AI to prepare its bid explanation, which cited non-existent tax rulings generated by AI. The KIO confirmed the contractor had used AI to draft its pleadings without verification, which was attributable to oversight rather than deliberate act. The firm's offer was excluded from the tender.

AI hallucinations and deepfakes presented as evidence constitute a growing problem in ongoing court proceedings.

There is also a reported dispute, the first known court case of its kind, concerning AI-generated voice cloning in advertising. A voiceover artist alleged that an AI system cloned his voice without consent, violating his personal rights and proprietary rights. The court is expected to determine whether synthetic voice generation constitutes unlawful use of a person's image or personal characteristics, how liability should be allocated among the AI tool user, the system provider and the publisher, and whether consent to professional voice cloning within a voice bank precludes unauthorised cloning by third parties.

Finally, in a February 2026 ruling, the Supreme Administrative Court (SAC) held that AI-driven trading services – where an algorithm autonomously analyses Warsaw Stock Exchange data and places orders without human intervention – are exempt from VAT on the same basis as traditional brokerage. The court reasoned that the economic substance of the service is identical to that of a human broker, and that VAT classification depends on the nature of the service, not whether it is performed by a human or a machine. The judgment is significant for agentic AI systems. The key emerging principle is functional: what matters is the economic effect, not the means of performance.

5. AI Regulatory Oversight

5.1 Regulatory Agencies

The following regulatory agencies have jurisdiction over AI in Poland (EU regulatory agencies are not discussed).

- AI Development and Security Committee – market surveillance authority under the AI Act, responsible for monitoring the AI market and supporting businesses in AI Act compliance. The Committee is also to act as a single point of contact (Article 70 of the AI Act). Its establishment is provided for in the draft Polish Act on AI Systems.
- Social Artificial Intelligence Board – an advisory and consultative body to the Committee, 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 to monitor and co-ordinate AI implementation in Poland.

- PL/AI Artificial Intelligence for Poland – advisory group of the Ministry of Digital Affairs developing recommendations on AI use in state operations.
- AI Hub Poland – a government-run national AI platform operated by the Ministry of Digital Affairs.
- Standing Subcommittee on AI and Transparency of Algorithms – a parliamentary subcommittee assessing AI's societal impact, opportunities and risks.
- Working Group on Artificial Intelligence (GRAI) – established by the Ministry of Digital Affairs to foster AI development in Poland's private, public and research sectors.
- Institute of IDEAS and AI Safety Research Center – R&D centres operating at NASK in the field of artificial intelligence.

See also **7.3 National Security**.

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

- Office of the Personal Data Protection Authority (UODO) – oversees AI involving personal data processing.
- Office of Electronic Communications (UKE) – oversees the telecom sector, including AI in telecom infrastructure and services.
- Polish FSA (KNF) – oversees the financial sector and is expected to issue recommendations on AI adoption.

5.2 Regulatory Directives

A legal definition of AI was adopted in the AI Act.(The following does not include guidelines issued by EU regulatory agencies.)

- Guidelines on Artificial Intelligence for Public Administration (2026) – non-binding guidance issued by the Ministry of Digital Affairs on adopting AI tools in the public sector consistently with the AI Act and data protection requirements.
- Guidance on Data Protection Impact Assessments (DPIAs) for AI systems (2025) – UODO guidance on conducting DPIAs in the AI context, covering risk indicators and the interaction between GDPR and AI Act conformity assessments.

See also **2.2Involvement of Governments in AI Innovation**.

5.3 Enforcement Actions

So far, the enforcement and other regulatory actions have limited scope. For instance, UODO is investigating a complaint about ChatGPT. The case concerns allegations that ChatGPT processes personal data unlawfully and non-transparently, generates false information about individuals, and that OpenAI failed to properly fulfil key GDPR rights such as access, rectification and required informational duties.

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 cooperation 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

Standards are generally voluntary but may be essential for credibility and reliability in certain sectors.

European

Harmonised technical standards will be key to operationalising the AI Act's requirements for high-risk AI systems. CEN-CENELEC JTC 21 is developing over 30 standards for the AI Act. However, standardisation is delayed – only draft prEN 18286 (Quality Management System for EU AI Act Regulatory Purposes) has been published for public enquiry, and none of the standards are expected to be finalised before August 2026, which is one of the principal reasons for the

proposed postponement under the EU Digital Omnibus package.

International

Key international frameworks include:

- the OECD Framework for the Classification of AI Systems (addressing bias, explainability and robustness);
- ISO/IEC 42001:2023 (a certifiable AI management system standard); and
- the NIST AI Risk Management Framework (a voluntary framework for incorporating trustworthiness into AI design, development and use).

7. AI and the State

7.1 Government Use of AI

Polish government is engaging with AI across various domains, including:

- Virtual Assistant – a GPT-based chatbot for the mObywatel app (digital official services);
- Virtual Civil Servant – advanced e-office software;
- PLLuM – a Polish large language model initiative by scientific institutions supported by the Ministry of Digital Affairs;
- Bielik – a Polish LLM developed by the Speakleash Foundation that works on-premise; and
- STIR – algorithmic analysis of data provided by financial institutions to tax authorities.

Poland is gradually digitalising civil procedure. Courts deliver documents electronically via the Portal Informacyjny. From March 2026, electronic filing will be optional; from March 2027, mandatory for attorneys-at-law. Electronic filings require a qualified electronic signature, trusted profile or personal signature. The system remains hybrid, as paper filings persist in some situations.

Digital Judicial Assistant

AI is not widely used in the justice system. Currently, the most common application is an AI-based legal information search system for judges and prosecutors. A digital judicial assistant supporting judges in administrative work and research is planned for 2026, with initial pilots already carried out in selected courts.

7.2 Judicial Decisions

Judicial decisions involving use of AI by government agencies is not currently applicable in Poland. In March 2025, the Ministry of Justice announced the launch of the "Digital Court" project, which will encompass introduction of the following:

- 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 AI in national security and encourages private-military co-operation. The recommendation to the National Security Strategy (2024) recognises AI as creating new development opportunities while generating risks, including loss of digital sovereignty, and highlights the importance of monitoring emerging technologies (AI, quantum) in the context of security and international relations, as well as promoting STEM education. In March 2025, Poland established an AI Centre under the Cyberspace Defence Forces (*Wojska Obrony Cyberprzestrzeni*, WOC), responsible for co-ordinating AI deployment within the armed forces and assessing commercial AI products for military applications through collaboration with industry and academia. The Centre forms part of the Ministry of National Defence's artificial intelligence strategy to 2039.

8. Generative AI

8.1 Generative AI: Key Legal Issues and Regulatory Approaches

Specific Issues in Generative AI

Key issues raised by GAI include:

- data protection;
- confidentiality and IP;
- sector-specific regulations (eg, banking, health);
- ethical concerns (eg, bias, discrimination);
- technical risks (eg, prompt injection, training data poisoning); and
- operational risks (eg, over-reliance, hallucinations, shadow AI, service disruptions, skills and resource gaps).

Copyright Protection

AI-generated results

Copyright protection of AI-generated output is limited since only humans can be authors under Polish law. Output may be copyrightable where human creative oversight was significant, as confirmed in the European Parliament resolution of 10 March 2026 on copyright and generative AI.

Derivative (neighbouring) rights (to video or sound recordings) may be allocated to individuals or companies. Output ownership depends on provider terms: eg, Microsoft® does not claim ownership of generative AI output. Some providers (eg, Microsoft®) offer IP indemnification subject to conditions and specify in T&Cs whether output is used for model training.

AI input

Input provided to AI systems may be copyright-protected if it meets originality and creativity requirements. T&Cs usually specify whether input will be used for model training.

AI system itself

An AI system itself can be protected as software under copyright law. In the EU, software is protected similarly to literary works. Computer programs may also receive patent protection.

Training data

Training data can be protected by copyright or database protection laws. Whether use of training data infringes copyright or falls within text and data mining exemptions under DSM Directive 2019/790 remains debated. Arguments exist that AI training resembles learning ideas or concepts not protected by copyright. No court cases have been raised in Poland against model developers.

Trade secrets; know-how

Input, training data, software and output can constitute trade secrets if they have economic value, are kept confidential, and appropriate security measures are maintained. This is particularly relevant where AI output cannot otherwise be protected.

Data Protection and Generative AI

Key data protection issues connected to GAI include the following.

- Lack of transparency of complex GAI models (the "black box" problem) and insufficient data minimisation during model training. Mitigation measures include anonymised data, regular reviews, internal policies and technical filters to prevent unintentional provision of personal data.
- Using personal data for training or fine-tuning may be inconsistent with original collection purposes; controllers should assess compatibility under Article 6 (4) GDPR.
- Data accuracy risks – AI may generate incorrect responses, including hallucinations.
- Data subject rights must be respected, with no specific exceptions for GAI.
- False personal data in outputs may still constitute personal data subject to rectification where it can be linked to an identifiable person. The European Data Protection Board (EDPB) opinion confirms this particularly applies where the AI provides conclusions about persons whose data was used for training.

Identifying and accessing personal data in AI models can be difficult. The right to rectification applies to both input and output data and must be considered at the AI design stage.

A complaint filed in Poland in September 2023 concerning data subject rights and transparency in ChatGPT remains ongoing; these issues are partially addressed by EDPB Opinion 28/2024.

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*) published in 2025 recommendations for attorneys-at-law on the safe use of AI in legal work, covering preparation, implementation and application of AI tools. The Supreme Bar Council (*Naczelna Rada Adwokacka*) published in 2025 Good Practices on Cybersecurity in the Operations of Law Firms and the Work of Attorneys, including guidelines on AI tools in the cybersecurity context.

There is no case law in this area.

Most law firms use standard AI tools (primarily ChatGPT and Microsoft 365® Copilot) for translation, summarisation, drafting and e-discovery. Other solutions (eg, litigation drafting support) are often not adjusted to Polish law and therefore less common. Larger law firms and legal departments increasingly rely on lawyer-specific software.

Legal practitioners must ensure that:

- AI-generated content is verified by a human;
- client data confidentiality is protected, with AI tools that use input for model training or lack appropriate safeguards generally prohibited; and
- internal procedures are implemented.

Legal advisers are obligated to observe professional secrecy and implement adequate technical and organisational safeguards.

10. Liability for AI

10.1 General Theories of Liability

Fault-Based Liability

The claimant must prove fault, damage and causation. In the AI context, this is difficult due to the opacity of AI models, which makes identifying the responsible person or cause challenging. Compliance with the AI manufacturer's instructions may shield users from fault, while altering AI code or using it for unintended purposes could attribute fault to the user.

Strict (Risk-Based) Liability

Polish law imposes strict liability on operators of enterprises powered by natural forces (steam, gas, electricity, liquid fuels) for resulting injuries or property damage. However, this does not apply to AI, as providers of AI systems or models do not qualify as such operators.

Risk liability also applies to vehicle possessors, but proving causation remains necessary, making its application difficult where damage is caused by an AI system integrated into a vehicle.

Liability for Defective Products

Under current rules implementing Council Directive 85/374/EEC, AI systems cannot be classified as "products" as the scope is limited to movable items. See **10.2 Regulatory Approaches to Liability for AI**.

Contractual Liability

A party using AI under a contract may claim damages for breach by proving the breach, damage and causation; the alleged perpetrator is presumed liable but may prove otherwise. The evidentiary difficulties outlined above also apply. Providers often offer additional measures such as IP indemnification for AI-generated output. In most B2B transactions, provider liability is capped (eg, at 12 months' remuneration). Liability limitations or exclusions are ineffective in consumer contracts or in B2B cases where damage is caused wilfully.

Liability for Infringement of Personal Interests

Fault-based liability applies to persons using AI systems or AI-generated content without proper verification or with false intent (eg, deepfakes). The plaintiff may claim financial compensation and request publication of a corrective statement in the media.

Insurance Position

There is no obligatory AI-specific insurance. Due to the opacity of model training, affordable insurance coverage is unlikely in the foreseeable future.

10.2 Regulatory Approaches to Liability for AI

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 should be implemented 9 December 2026. It will also cover 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). However, the application of the directive in the AI context may be limited. There is the risk of fragmentation of AI liability legislation in the EU.

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

The European Commission formally withdrew the proposed directive in mid-2025.

11. Agentic AI Systems and Autonomous Decision-Making

11.1 Agentic AI Systems: Legal Framework and Governance

Polish law contains no dedicated framework for agentic AI and the AI Act remains the key regulation applicable. AI agents do not have legal capacity and, therefore, only organisations/persons providing or using them could be responsible for damages caused by the use of AI agents.

Existing Legal Frameworks

The fault-based liability or liability for defective products may apply as a baseline (see **10.1 General Theories of Liability**). Strict liability is unlikely. Fault or defect may stem from deficient design, inadequate testing, defects in training of databases (eg, biased or incorrect information). However, allocating faults is extremely difficult due to the opacity of AI models supporting AI agents. Providers or users of AI agents may also be contractually liable.

Human Oversight

Polish law imposes no specific oversight duty. Human oversight is critical for liability management: greater autonomy makes it harder to exclude liability. Meaningful oversight mechanisms – monitoring, confirmation steps and stop/interrupt capability – serve as both substantive safeguards and evidentiary assets.

Cross-Organisational Accountability

Where an agentic system operates across multiple organisations, the key questions are which entity is liable and whether joint and several liability applies. Co-liable parties may each be pursued for the full amount; recourse claims are available, allocated by degree of fault and contribution. Contractual liability allocation, indemnities, limitation clauses and warranties across the value chain are therefore essential, though such arrangements are inter partes only and cannot affect the victim's rights.

Logging and Auditability

No duty to maintain AI-specific logs exists. However, logs are critical evidentially and should be retained for an appropriate length of time.

High-Risk Domains

Polish civil law creates no domain-specific restrictions on agentic AI deployment.

Multi-Agent Systems

No specific Polish rules exist for multi-agent systems. Key issues are:

- co-causation (normal-consequence test applied at each causal link);
- joint and several liability of multiple operators; and
- emergent behaviour, which complicates causation and defences.

11.2 Liability Allocation for Autonomous AI Systems

Allocation Amongst Developers, Deployers and Users

Polish law does not prescribe a fixed allocation of liability across the AI value chain. The liability within the value chain will be determined based on the fault liability or based on liability for defective products. See also **11.1 Agentic AI Systems: Legal Framework and Governance**.

Adequacy of Existing Liability Regimes

Existing Polish tort law was not designed for autonomous AI. It requires culpable human conduct and

adequate causal link causation. However, AI behaviour may not be traceable to any human decision. The black-box problem of lack of transparency makes it difficult to assign responsibility when harm occurs. Overall, these issues make the fault basis structurally inadequate.

AI-Specific Liability Frameworks

Polish law currently contains no AI-specific liability framework.

Contractual Liability Allocation

Contracts across the AI value chain should address liability allocation and limitation, documentation and log access, risk assessments, incident notification and, where applicable, audit rights. They should also define the parameters within which the AI agent may act (eg, concluding contracts, placing orders, committing resources).

Evidentiary Challenges

Evidentiary difficulty is acute in AI liability litigation. The burden of proof rests on the claimant, and the opacity of AI systems makes it structurally difficult to establish causation or for users (not being providers) to exclude their liability. Claimants unable to identify the specific cause may rely on factual presumptions and a high degree of probability – an approach affirmed by the Polish Supreme Court in medical liability cases and potentially applicable by analogy to AI disputes.

Comprehensive logs are the primary basis for reconstructing events, and organisations maintaining them are substantially better positioned in proceedings.

Cascading Failures in Multi-Agent Systems

Multi-agent systems present the most complex liability scenarios, as no single act may be sufficient cause. The adequate (normal) causal relationship test must be applied at each link in the causal chain, which may be genuinely indeterminate. Emergent behaviour means no single party may have designed, authorised or foreseen the harmful outcome, rendering fault-based and product liability structurally inapt. Where multiple operators are liable, joint and several liability applies, but recourse is complicated by the technical difficulty of disentangling respective contributions. Contractual frameworks should therefore define clear operational boundaries for each agent.

12. Specific Legal Issues With AI

12.1 Algorithmic Bias and Fairness

Bias Characterisations and Risks

Algorithmic bias happens when the system discriminates against a specific group or individual, resulting from various factors. For example:

- 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 **14. 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 and 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 the high-risk AI system is intended to be used. Even when an AI system is not 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.

12.2 Biometric Technologies and Emotion Recognition

The AI Act (effective February 2025) restricts real-time and retrospective facial recognition. Facial recognition constitutes "biometric identification" using "biometric data" under the AI Act. Biometric categorisation systems are prohibited (with law enforcement exceptions), as is real-time remote biometric identification in publicly accessible spaces for law enforcement (unless strictly necessary under the AI Act). Untargeted scraping of facial images from the internet or CCTV to create or expand facial recognition databases is also prohibited (Clearview AI case).

Many biometric systems are classified as high-risk (eg, emotion recognition, biometric categorisation based on sensitive attributes), as are post-remote identification systems – law enforcement may not base adverse decisions solely on their output. Deployers of emotion recognition or biometric categorisation systems must inform exposed persons. Member states may adopt stricter rules on facial recognition in public spaces. The Commission published non-binding Guidelines on prohibited AI practices in July 2025 (C(2025) 5052). These systems are also subject to GDPR and local laws implementing the Data Protection Law Enforcement Directive.

Key risks include the following:

- biometric data is uniquely personal and irreplaceable if compromised, with storage posing heightened cyber-attack risks (identity theft, unauthorised access);
- unreliable facial recognition results across different races, ethnic origins or genders;
- privacy infringements and discrimination;
- high misuse potential; and
- ethical concerns regarding surveillance and mass tracking.

12.3 Deepfakes and Synthetic Media

There are no national regulations aimed at deepfakes or synthetic media, but after the Grok AI case there is a lively discussion on combating abuses related to the creation of such content. Some of the provisions of Directive 2024/1385 on combating violence against women and domestic violence may directly apply to deepfakes once implemented at national level.

12.4 Transparency and Disclosure

Transparency is a fundamental principle of the AI Act and is applicable from 2 August 2026 (with a transition period for providers until 2 February 2027). Providers must ensure that AI systems interacting with natural persons inform users of the AI nature of the interaction, unless this is obvious to a reasonably well-informed person or exempted by law for criminal offence processing. High-risk AI systems must function transparently to enable proper comprehension and use of outputs.

Providers must mark AI-generated synthetic outputs (eg, audio, image, video or text) in a machine-readable format detectable as artificially generated, with exceptions for artistic activity or where systems do not significantly alter input data. Deployers must disclose artificially generated or manipulated deepfake content and inform persons exposed to emotion recognition or biometric categorisation systems (law enforcement exceptions apply). Deployers must also disclose AI-

generated text published to inform the public on matters of public interest, unless authorised by law for criminal offence processing or the content undergoes human review.

Providers of general-purpose AI models must make publicly available a detailed summary of training content, particularly text and copyrighted data. The AI Office is developing a voluntary Code of Practice on Marking and Labelling of AI-Generated Content (second draft published March 2026).

13. AI Procurement and Supply Chain Accountability

13.1 AI Procurement Standards and Contracting

AI procurement frameworks depend on the deployment mode (on-premise, cloud or container-based) and solution type (off-the-shelf versus customised). For standard AI systems, customers typically contract on the provider's standard terms with limited negotiation. Customised arrangements (fine-tuning or dedicated AI agents) are rare in Poland due to high costs. Most AI solutions are procured as SaaS, meaning standard cloud provider terms usually apply.

AI-Specific Risk Allocation, Service Level Agreements, Data Rights and Usage

The customer determines the purpose of use and data categories; providers generally do not perform AI Act or GDPR risk assessments on the customer's behalf. Customers must comply with the provider's responsible AI/acceptable use policies, and access may be suspended for violations. Service level agreements are typically availability-based; qualitative performance commitments (eg, stability of model behaviour) are rare. AI agreements should address:

- rights to input and output;
- whether the provider may use customer data for model training;
- controller/processor status;
- the customer's right to train its own models on output; and
- confidentiality.

IP Allocation, Compliance, Audit, Exit and Insurance

The agreement should determine whether the provider acquires IP rights or licences to customer inputs or outputs. As AI outputs often do not qualify for copyright protection, many providers (eg, Microsoft) confirm they do not claim ownership of customer outputs. Customers should verify whether IP indemnification is offered. The customer largely controls regulatory risk; providers usually exclude warranties regarding lawfulness of specific use cases or regulatory classification. Audit rights, exit, portability and liability caps are typically governed by standard cloud/IT clauses. Insurance requirements, if any, are general IT or cyber-risk insurance rather than AI-specific coverage.

13.2 AI Supply Chain Accountability and Due Diligence

AI Value Chain Obligations Under the AI Act

The AI Act establishes a layered accountability framework across the AI value chain, with most obligations on the provider. Under Article 25, any distributor, importer, deployer or other third party that places its name or trade mark on a high-risk AI system, makes a substantial modification, or changes its intended purpose to render it high-risk, assumes provider obligations. Providers of high-risk AI systems and third parties supplying tools, services, components or processes integrated into such systems must specify by written agreement the information, capabilities, technical access and assistance needed for the provider to comply with the AI Act. This does not apply to third parties offering tools or services under a free and open-source licence.

Due Diligence When Procuring AI Systems

No specific Polish due diligence obligations for AI procurement exist beyond the AI Act and the amended National Cyber Security System Act (NCSSA) (implementing the NIS2 Directive). In practice, organisations procuring potentially high-risk AI systems should conduct pre-procurement legal, technical and operational assessments. Under the amended NCSSA, key and important entities must address ICT supply chain security, including supplier-specific vulnerabilities, which extends to AI systems forming part of their ICT infrastructure.

Assessment of Upstream Providers' Compliance

The AI Act does not require deployers to audit upstream providers' compliance. However, deployers should verify completion of conformity assessments, CE marking, and availability of technical documentation (Articles 11 and 13), and apply general IT provider assessment practices (ie, financial standing, certifications such as ISO/IEC 27001, regulatory posture). Ongoing monitoring should cover post-market obligations (Article 72), serious incidents and substantial modifications. Where third-party components are incorporated, contractual assurances under Article 25 (4) should be sought.

Liability for Third-Party AI Components

No specific Polish regime governs liability for third-party AI components; general liability frameworks apply (see **10.1 General Theories of Liability**). Directive 2024/2853 on Liability for Defective Products (transposition by 9 December 2026) will extend product liability to software and AI outputs, relevant to third-party AI components integrated into products.

Contractual Mechanisms for Cascading Obligations

Absent specific Polish statutory requirements, supply chain accountability relies on contractual arrangements. Agreements should include:

- AI Act compliance warranties;
- notification obligations for substantial modifications or conformity assessment changes;
- incident notification aligned with AI Act and NCSSA timelines;
- indemnities for third-party claims arising from non-compliant AI outputs; and
- clarification of provider status under the AI Act.

14. Employment

14.1 Hiring and Termination Practices

Employers may not use AI to infer a job candidate's or employee's emotions, except for medical or safety purposes. AI systems used for the following are classified as high-risk under the AI Act, imposing additional obligations on employers:

- recruitment, selection;
- targeted job advertisements;
- filtering applications;
- evaluating candidates; or
- making decisions on work-related terms, promotion, termination, task allocation or performance monitoring.

Employers must demonstrate that final decisions are made by humans with documented reasoning. Employers most commonly act as "deployers" under the AI Act; however, significantly modifying a system or changing its intended purpose may result in reclassification as a "provider", entailing substantially more stringent obligations.

Irrespective of the AI Act, employers must comply with general anti-discrimination and privacy laws. Discrimination in employment, including through technology use, is prohibited, and employers are liable for discriminatory outcomes of the technology they deploy. Under the Polish Labour Code, technology use, including AI, must not violate privacy regulations governing personal data in hiring and employment.

14.2 Employee Evaluation and Monitoring

Employers use various digital tools, including AI, to evaluate performance, track working time and monitor employees' work. Email and activity monitoring must be introduced via internal policies, announced to employees, and must not infringe on the integrity of correspondence or employees' personal interests. The adoption of monitoring procedures requires agreement and/or consultation with company trade unions (if any); in their absence, no statutory consultation obligations apply. Breach of these rules may result in employees' claims for illegal monitoring and compensation and may constitute a breach of privacy laws.

15. AI in Industry Sectors

15.1 Digital Platform Companies

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

- In principle, providing GAI or solutions based on such models (eg, conversational solutions 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 **14. Employment**).

15.2 Financial Services

Financial services institutions (FSI) are actively adopting AI, including customer-facing chatbots, productivity tools (eg, Microsoft 365 Copilot) and automation of internal processes such as anti-money laundering and anti-fraud.

There are no AI-specific provisions for FSI, except that AI-based credit scoring systems may qualify as high-risk under the AI Act. However, financial services are highly regulated and introducing AI is subject to complex obligations.

- Where AI processes banking, insurance or other statutory professional secrets, outsourcing regulations (including non-EEA outsourcing) may apply. Following the repeal of the Cloud Communication, cloud-based AI solutions should be assessed against applicable outsourcing rules.
- Automated decision-making supported by AI is subject to additional restrictions under local legislation, particularly regarding creditworthiness assessment and credit risk analysis.
- For robo-advisory, the FSA position on robo-advisory services applies – see **3.3 Jurisdictional Directives**.
- FSIs should also consider EU-wide guidelines (eg, the EBA Discussion Paper on ML for IRB Models) and account for AI-specific risks such as bias (see **12.1 Algorithmic Bias and Fairness**) and opacity (see **12.4 Transparency and Disclosure**), as well as standard operational risks including confidentiality of professional secrets and business continuity.

15.3 Healthcare

AI and ML can assist in diagnosis, disease management, medical imaging, drug discovery, operations, telemedicine and wearable technology. However, in the Polish public sector, AI adoption in healthcare is limited by restrictions on cloud computing through which such solutions are often offered. Some restrictions were removed in October 2024 but work continues.

There are no regulations specific to AI in healthcare. The general regulations apply:

- the AI Act;
- GDPR, as supplemented by special Polish provisions on processing data in the medical context;
- provisions regulating medical secrets; and
- for cloud-based AI solutions, the Resolution of Council of Ministers on Common ICT Infrastructure of the State and Cybersecurity Standards for Cloud Computing.

AI may constitute a medical device subject to the MDR and IVDR; the burden is generally placed on the manufacturer/importer. Data sharing for healthcare delivery and AI training is covered by the Data Act and will be governed by the EU Regulation on European Health Data Space.

Key risks include:

- bias in AI decision-making significantly affecting patient life (see **12.1 Algorithmic Bias and Fairness**);
- over-reliance and difficulty verifying AI outputs;
- AI errors (eg, flawed data, hallucinations) causing misdiagnosis or harm during AI-assisted surgery (see **10. Liability for AI**); and

- privacy/security issues including misuse of patient data, breaches and cyber-attacks targeting medical records and live health data devices.

15.4 Autonomous Vehicles

Until late 2025, Polish law generally prohibited the use of autonomous vehicles on public roads, with a narrow exception for research testing limited to vehicles at Level 3 of automation. This framework has undergone a fundamental legislative transformation. On 21 November 2025, Poland's Parliament enacted the Act Amending the Road Traffic Act and Certain Other Acts (published in the Journal of Laws on 23 December 2025; entering into force in June 2026).

Definitions

The Act introduces into the Road Traffic Act statutory definitions of "automated vehicle" and "fully automated vehicle", as provided in EU Regulation 2019/2144 on vehicle type-approval. It also establishes six SAE-aligned levels of automation (Level 0 – no automation; Level 5 – full automation in all conditions), set out in a new Annex 3 to the Road Traffic Act (Article 65l).

Permits

Research testing of automated or fully automated vehicles on public roads requires a prior permit, issued by the National Research Coordinator by administrative decision, for a fee, upon written application. Permits cover up to five voivodeships and are valid for a maximum of three years.

No permit is required for research on vehicles below Level 3 automation.

The Director of the Motor Transport Institute has been designated as the National Research Coordinator, with responsibility for issuing and supervising research permits, maintaining a public register of permits, and co-ordinating with international bodies.

Liability

The holder of an automated or fully automated vehicle bears strict (risk-based) liability for damage caused by the movement of the vehicle. Mandatory third-party motor insurance is required.

Conducting research without a permit is subject to a financial penalty of PLN100,000–200,000. Breach of permit conditions is subject to a penalty of PLN20,000–100,000.

The automated vehicle owners need to hold a valid third-party insurance.

15.5 Retail and Consumer

Retailers using AI-driven ranking or personalised pricing must comply with transparency obligations under the Omnibus Directive's implementing provisions: consumers must be informed that pricing has been individualised through automated processing.

AI chatbots deployed in customer service must disclose their artificial nature under Article 50 of the AI Act, if they qualify as AI systems, not simple pre-automated chatbots.

The Polish Consumer Authority is very active in the field of e-commerce platforms and pays particular attention to price presentation and the use of dark patterns mechanisms. Recently it was announced that it is actively developing an AI-powered tool to detect dark patterns in e-commerce, following an EU-funded study covering over 300 Polish websites.

Retailers should audit AI systems against the AI Act's requirements, bearing in mind potential reclassification of the systems or their role if any changes are introduced.

15.6 Industrial AI and Robotics

Poland is experiencing significant growth in industrial AI and robotics adoption. Key industry applications include:

- predictive maintenance (ML models applied to vibration, temperature and current signals);
- computer-vision quality inspection (defect detection, measurement and traceability);
- process and energy optimisation;
- safety and operations monitoring; and
- intralogistics/warehouse automation, where AI is deployed for perception, grasping and exception handling.

Applicable Legal Framework

No specific regulations apply to AI in manufacturing or industrial robotics. The regulatory framework is layered and predominantly EU-driven, comprising the following key instruments.

- EU AI Act – industrial AI systems integrated into a safety component of a regulated product (eg, machinery) or critical infrastructure are classified as high-risk under the AI Act.
- Machinery Regulation (EU) 2023/1230 – replacing the Machinery Directive 2006/42/EC from 14 January 2027, this is the cornerstone of industrial robot safety. Industrial robots constitute "machinery" in most configurations, and compliance is a prerequisite for market placement or putting into service.
- GDPR and Polish Labour Code – where industrial AI involves monitoring of natural persons (eg, vision systems, wearable tracking, worker analytics or biometrics), GDPR and Polish labour law constraints apply.
- EU Data Act – governs access to and use of data generated by IoT-enabled machinery, sensors and robotic systems, enabling users to access and share such data, including for AI training, fine-tuning or verification. It also imposes data-sharing obligations on data holders and safeguards against unlawful international data transfers.
- Cybersecurity – The National Cyber Security System Act (NCSSA), as amended to implement the NIS2 Directive, intersects with AI risk management, particularly for critical services and infrastructure (see **19.1 Applicability of Cybersecurity Legislation to AI**).

Liability

Liability for AI-related harm in manufacturing falls under the general frameworks (see **10. Liability for AI**).

16. Intellectual Property

16.1 IP Protection for AI Assets

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.

Contractual Provisions

Non-disclosure arrangements and obligations not to use input and output to train or improve the models 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).

See **8.1 Generative AI: Key Legal Issues and Regulatory Approaches** for general remarks regarding the relation between IP and generative AI.

16.2 AI as Inventor/Author

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 copyrighted or protected by industrial property 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.

16.3 Copyright and AI Training Data

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 are not copyrightable because they are 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 regis-

tering 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.

In addition, recently the European Parliament adopted resolution of 10 March 2026 on copyright and generative AI in which it was stated that content fully generated by AI that does not meet the established criteria for copyright protection should remain ineligible for copyright protection, and that the public domain status of such outputs be clearly determined.

AI Training

There are discussions about whether the use of training data is an infringement of copyright or may be based on text and data mining (TDM) exemptions included in Polish Copyright Act, as the implementation of EU Directive 2019/790. It is worth mentioning that in the initial project the AI training was explicitly excluded from the TDM exception, but in the final version this exclusion has been deleted. AI companies rely on the TDM exception to train their models.

It is claimed that over-representation of specific data, which leads to memorisation and re-creation of training data, may be considered violation of copyright to such re-created works. Nevertheless, from the technical point of view, the memorisation effect is not the result of training data copies storage in the model, but the over-representation of such data at the training stage.

No court cases have been raised in Poland against the model developers.

ZAiKS (the main Polish collective rights management organisation for music) has proactively exercised the opt-out mechanism available under the text and data mining exception of the DSM Directive, opting all works of its members out of AI training use.

16.4 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 more in **16.3 Copyright and AI Training Data** and **8.1 Generative AI: Key Legal Issues and Regulatory Approaches**.

16.5 Foundation Models and Open-Source AI: IP Considerations

Licensing Models

The following models are used.

- Proprietary models (eg, Claude) withhold weights entirely, relying on copyright, trade secrets and contractual restrictions.
- Open-weight models (eg, Llama) release weights under bespoke licences that impose use restrictions – commercial caps, prohibited applications and attribution requirements – but are not truly "open-source".
- Open-source models released under licences such as Apache 2.0 or MIT grant broader freedoms. The AI Act provides different rules for open source AI systems, especially releasing model providers from some obligations if such models are provided under the open-source licence that allows for the access, usage, modification and distribution of the model, and whose parameters, including the weights, the information on the model architecture and the information on model usage, are made publicly available.

IP Implications of API Versus Self-Hosted Models

There is no separate licence regarding the models accessible via API – the term of use focuses on the general terms related to accessing the service via API and the use of outputs.

For self-hosted models, the AI model providers focus on full-range regulation, which covers also the model and its weights. As the model is deployed on the self-hosted infrastructure, the licences also cover the issues of model re-training, fine tuning, modifications and audit rights.

Self-hosted models are preferred by entities that focus on data protection or are additionally regulated – eg, the banking sector.

Derivative Works and Fine-Tuning

Whether a fine-tuned model is a derivative work is unresolved, turning on the unanswered question of whether model weights can receive copyright protection. In practice, fine-tuning rights are governed by licence:

- proprietary models generally prohibit it;
- open-weight licences permit it with conditions (eg, naming requirements, licence flow-down); and
- permissive open-source licences impose few restrictions.

The fine-tuning dataset itself carries independent infringement risk if unlicensed copyrighted material is used.

Another important issue arises in relation to the AI Act and potential reclassification of the AI system due to implemented changes or altered AI system intended purposes – which may lead to reclassification of the AI system from "normal" to high-risk, as well as reclassification of the entity from deployer to provider.

IP Risks in Commercial Use

Training data liability is the dominant risk: multiple high-profile cases allege infringement through unlicensed training. The EU AI Act and DSM Directive Article 4 require GPAI providers to respect rights reservations. Output liability may arise where models reproduce memorised training content. Users publishing AI-generated outputs commercially may be exposed to third-party infringement claims, even if such reproduction is unintentional.

Model Merging and Distillation

Merging weights from models under different licences creates compatibility problems — the most restrictive licence governs the merged output. On the other hand, it may be problematic when it comes to copyleft licences.

Distillation is expressly prohibited by most proprietary licences (including OpenAI's), which bar using outputs to train competing models. Even if under the licence terms the distillation may be lawful, training data infringement risks inherited from the teacher model still persist.

17. Data Protection

17.1 AI Training and Data Protection

Processing personal data for AI model training must comply with the GDPR. The EDPB addressed this in Opinion 28/2024 of 17 December 2024, providing guidance on key data protection aspects related to AI models.

Lawful Basis

With respect to non-special categories of data, legitimate interests (Article 6 (1)(f) GDPR) may serve as a legal basis for AI training, subject to a balancing test; mere commercial interest does not automatically suffice. Consent (Article 6 (1)(a)) is theoretically available but practically difficult to obtain, particularly for web-scraped data. Research exceptions (Article 89) cannot justify commercial model training. Special categories of personal data may be processed for training under consent or in limited situations – for reasons of substantial public interest (Article 9 (2)(g) GDPR) or scientific research (Article 9 (2)(j)). The AI Act imposes additional obligations for bias detection in high-risk systems. The EDPB highlighted that large-scale web-scraped datasets may inadvertently contain special category data; controllers must filter such data where no valid exception applies, and, where separation is impossible, Article 9 applies to the entire dataset. The EU Digital Omnibus package proposes a new legal basis for processing special categories of data for bias correction across all AI systems.

Purpose Limitation and Compatibility With AI Training

Under Article 5 (1)(b) GDPR, personal data collected for a specified purpose may not be repurposed for AI training without a compatibility assessment under Article 6 (4) GDPR. The EDPB emphasises that such repurposing may be incompatible with the original purpose. The purpose of processing must be determined at an early stage, and the deployment context must be considered even where not yet fully known.

Data Minimisation Principles

Controllers must assess whether training objectives can be achieved with less personal data or with anonymised or synthetic data and implement techni-

cal measures to reduce personal data processed to the minimum necessary (Article 5 (1)(c) GDPR).

Rights of Data Subjects Whose Data is Used in Training

The EDPB acknowledged practical challenges where personal data has been absorbed into model parameters. Controllers must assess whether retraining or other technical measures are necessary to give effect to erasure requests. The right to object under Article 21 GDPR must be ensured where legitimate interest is the lawful basis.

Anonymisation and Pseudonymisation Techniques

AI models trained on personal data are not automatically anonymous; anonymity must be assessed case-by-case. Key safeguards include regularisation methods and privacy-preserving techniques such as differential privacy. Pseudonymisation may be appropriate where actual content is not relevant, such as in training large language models.

Accountability and Documentation Requirements

Controllers must document AI training processing operations, including DPIAs, DPO advice, technical and organisational measures applied during model design and life cycle, evidence of resistance to re-identification attacks, and information provided to deploy controllers or data subjects. Privacy by design under Article 25 (1) GDPR is a fundamental safeguard in AI model development.

17.2 AI Deployment and Data Subject Rights

Lawful Basis for AI-Driven Processing

For non-special categories of data, legitimate interests (Article 6 (1)(f)) is most commonly invoked for AI but requires a three-step balancing test, in which reasonable expectations of data subjects are a key factor given the complexity of AI and its varied downstream uses. Controllers should document the lawful basis separately for each purpose within the AI life cycle.

Transparency Obligations for AI Processing

Controllers must provide information about processing purposes and, where applicable, the logic and consequences of automated decision-making under Article 22 GDPR. Reliance on the Article 14 (5)(b) exception for web-scraped training data is strictly limited.

Data Subject Rights in AI Contexts

Although the GDPR does not expressly provide a "right to explanation", Recital 71 indicates data subjects should be entitled to an explanation of automated decisions. Under Article 22, there are views supporting a "right to reasonable inferences" – the right to challenge both AI decisions and their underlying conclusions.

Automated Decision-Making and AI

Decisions based solely on automated processing producing legal or similarly significant effects are prohibited unless exceptions apply. Human oversight must be genuine. The AI Act imposes additional oversight, documentation and risk management requirements for high-risk systems, complementing Article 22 GDPR. Since AI currently mainly supports rather than replaces human decisions, GDPR restrictions on automated decision-making may not be frequently triggered in practice.

Data Retention and Deletion in AI Systems

Controllers must establish deletion deadlines differentiated by data category (training data, inputs, outputs, logs, prompts, feedback). Training data should be deleted or anonymised upon completion of training unless a separate legal basis justifies retention. The right to erasure in AI contexts may require consideration of whether personal data has been incorporated into the model itself ("machine unlearning"). Per EDPB Opinion 28/2024, a model may only be considered anonymous following a thorough assessment of identification and data extraction risks.

Children's Data in AI Applications

The AI Act prohibits AI systems from exploiting age-related vulnerabilities to materially distort behaviour causing significant harm. High-risk AI providers must account for children's vulnerabilities in impact assessments, and deployment processing children's data will generally require a DPIA under Article 35 GDPR.

17.3 AI Data Governance and Cross-Border Transfers

Under Article 10 of the AI Act, providers of high-risk AI systems must ensure training, validation and testing datasets are relevant, representative, error-free and complete.

Data Protection Impact Assessments (DPIAs)

DPIAs for AI must address AI-specific risks such as:

- data quality and bias;
- re-identification;
- explainability limitations;
- model drift;
- automated decision-making under Article 22 GDPR; and
- discriminatory effects.

DPIAs must cover the entire AI life cycle, be updated when the system evolves materially, and should be carried out primarily by deployers.

Data Protection by Design and by Default

Article 25 GDPR requires data protection to be embedded into AI systems from the earliest development stages, including limiting training datasets to necessary personal data, using anonymised or synthetic data where feasible, and providing for automated deletion upon completion of training.

Processor/Controller Relationships in AI Supply Chains

Correct GDPR role allocation across AI supply chains is critical. Data processing agreements must prohibit processors from using training data for their own purposes unless explicitly agreed. Unauthorised use of client data to improve a vendor's own models likely constitutes independent controllership; joint controllership may arise in co-development or fine-tuning scenarios.

Cross-Border Data Transfers for AI Training and Deployment

AI systems often involve transfers of personal data to third countries under Chapter V GDPR, applicable to all processing phases. Special attention is needed where models are trained outside the EU using EU personal data or may retain such data through memorisation or regurgitation effects.

18. Antitrust

18.1 Emerging Antitrust Issues in AI

The Office of Competition and Consumer Protection (UOKiK) has developed and is testing an AI tool designed to assist officials in detecting manipulative techniques (dark patterns) on e-commerce websites, such as urgency timers, misleading subscription mechanisms, and deceptive interface designs. UOKiK is also preparing internal guidelines on the use of AI in its supervisory activities. The tool was presented in March 2026.

19. Cybersecurity

19.1 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 entities that are part of this system. The amendment implementing the EU NIS2 Directive has already been adopted and published in the Journal of Laws on 2 March 2026 and is scheduled to enter into force on 3 April 2026. Once effective, the new regulations increase the level of cybersecurity in Poland by strengthening requirements relating to risk management, incident reporting and supply-chain security, and by extending obligations to key and important entities across a broader range of sectors. Although the framework is not AI-specific, it will also be relevant to providers and users as defined under NCSSA of AI-based solutions where they fall within the statutory scope, in particular if the AI solution forms part of regulated ICT services or infrastructure, while AI vendors outside the scope of NCSSA may still be affected indirectly through contractual and security requirements imposed by regulated entities.

20. ESG

20.1 ESG Dimensions of AI

ESG/sustainability reporting regulations in the EU and Poland do not prohibit the use of AI. However, given recent changes in the CSRD framework – including deferred reporting deadlines and new thresh-

olds under Directive (EU) 2026/470 – the number of ESRS-compliant reports remains limited, which may constrain the use of AI due to insufficient input data. Importantly, AI is both a tool supporting ESG compliance and an increasingly relevant subject of ESG disclosure.

AI may play a significant role in analysing ESG data across all three dimensions:

- environmental (energy use, carbon footprint, emissions from data centres and cloud computing);
- social (workforce impact, algorithmic fairness, with certain systems classified as high-risk under the AI Act); and
- governance (board oversight, including potential liability, and transparency obligations).

Organisations should note that the CSRD, the AI Act and the CSDDD create interconnected obligations, requiring an integrated approach to AI-related ESG risk management.

21. AI Governance and Compliance

21.1 AI Governance Frameworks and Implementation

Effective AI governance requires cross-functional collaboration across legal, compliance, IT and business teams. Organisations should adopt an internal AI policy assigning clear responsibility, through a dedicated AI Committee in larger entities or a designated AI Champion in smaller ones and maintain an up-to-date inventory classifying all AI systems by risk level, including a whitelist of approved tools.

Risk management should follow the EU AI Act's tiered approach (prohibited practices, strict obligations for high-risk systems, lighter-touch transparency for limited-risk tools), extending across the full AI life cycle with human oversight embedded at every stage and ongoing training on safe AI use. AI policies must integrate with existing data protection, information security and employment frameworks. High-risk deployments require fundamental rights and data protection impact assessments, and deployers must monitor vendor terms closely, as supply-chain obligations under the AI Act run deep.

Incident response protocols should cover reporting, escalation, remediation and documentation, with lessons feeding back into risk management. Governance should remain proportionate to the organisation's risk profile and operational reality. The principal implementation challenges – organisational resistance, the tension between innovation and control, technical complexity, and a rapidly evolving regulatory landscape – require clear internal policies, targeted training and continuous regulatory monitoring.

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 200 attorneys, the firm provides the highest standard of legal services in all areas of business activity and is well known 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 developing 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 a founding member of the New Technologies Association.

Author

Agata Szeliga has been a partner at SK&S since 2009. 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 as well as on IP and AI-related matters in M&A transactions. She was a member of the European Commission's Expert Group on B2B data sharing and cloud computing contracts. She has published widely and is a regular lecturer on postgraduate programmes focusing on AI and data sharing.

Sołtysiński Kawecki & Szlęzak

Jasna 26 Street
00-054 Warsaw
Poland

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

SOŁTYSIŃSKI KAWECKI SZLĘZAK

Implementing AI in Poland

Background

As in much of the world, 2025 was a year of growing adoption of AI in Poland. The Polish Minister of Digitalisation declared in 2025 that the Artificial Intelligence Fund will spend over PLN4.5 billion (EUR1 billion) on the development of digital technologies in Poland. The financing will come from the Polish National Centre for Research and Development. AI-driven expenditure in the private sector was also substantial. According to the Polish Main Statistical Office, 8.7% of Polish companies used AI in 2025, compared to 5.9% a year earlier. Furthermore, the first signs of the impact AI is having on the labour market are also being seen. In the ICT sector, very low levels of job offers to junior employees are already being observed, especially to those who are looking for their first job. As AI tools can, albeit with some supervision, write computer code or prepare tests or documentation, the tasks previously allocated to juniors are now conducted by AI. Most job offers in the ICT sector are directed toward experienced professionals, suggesting that companies seek individuals capable of handling complex tasks, with AI serving as a helpful resource. Surprisingly, the data from Eurostat shows that Poland is one of three EU member states, after Romania and Italy, with the lowest share of people aged 16–24 using generative AI tools. In Poland only 49.3% of this demographic are using AI tools, compared to the EU average of 63.8%. If this trend is maintained, it may be more and more difficult for young people to enter the labour market and find satisfactory jobs.

Focus on the public sector

There is a push from the authorities for the broader implementation of AI in the public sector. As most of the proposed solutions are based on the public cloud, the government first needs to remove legal and psychological barriers to cloud solutions.

In October 2024, the Polish government amended its Resolution on the Common IT Infrastructure of the State to permit the use of public cloud services, including for storing data within the EU, as well as for handling public systems and registers containing health data and other sensitive personal information (with exceptions for military and law enforcement bodies). However, the corresponding cybersecurity standards for cloud computing services were not updated until March 2025. Currently, these standards permit the processing of information covered by statutory secrecy obligations (eg, information that is subject to tax secrecy or attorney-client privilege), as well as classified information of the category marked as "restricted" in public cloud services hosted within the European Union or, where compliant with EU law, within the European Economic Area.

In March 2026, the Minister of Digitalisation also issued the Guidelines on AI for the public sector (the "Guidelines"). The Guidelines provide practical directions for public authorities on how to use AI responsibly and effectively in everyday administrative work. In these guidelines, AI is presented as a supporting tool, not a substitute for human judgment, capable of improving efficiency in areas such as document analysis, summarisation, drafting correspondence and providing general information to citizens. At the same time, the guidelines emphasise the need for critical assessment of AI outputs, awareness of system limitations (including errors and hallucinations), and continuous human oversight. Public officials are expected to understand what AI systems can and cannot do, and to use them selectively, particularly avoiding reliance on AI in complex, sensitive or high-impact decision-making processes.

The Guidelines focus on legal compliance and data protection, especially under the EU AI Act and the GDPR. They include lists of prohibited and high-risk processing activities from the perspective of public authorities. Amongst the high-risk activities for AI systems, the Guidelines include, in particular:

- systems used as a safety element in critical infrastructure, such as transportation, where failure can result in accidents and life-threatening conditions;
- solutions that affect access to learning, such as systems for automatic assessment of exams or selection of candidates for studies;
- systems that assess creditworthiness;
- systems that award key services, where access to important financial or public benefits depends on their outcome; or

- systems to support the work of courts and democratic processes, such as tools to help prepare draft judgments or decision-making materials.

Polish government and parliamentary activity

Poland is gradually proceeding with the implementation of the local laws necessary to fully apply the EU AI Act.

The work on the Polish Act on AI Systems, which aims to ensure effective implementation of the AI Act, crossed an important milestone. On 31 March 2026, the Council of Ministers approved the government draft, and it will now undergo review by parliament.

According to the draft, a national market surveillance authority for AI systems (the "AI Development and Security Committee") will be established. The administrative support for this Committee will be provided by the office of the Minister of Digitalisation. The Committee will also function as a single point of contact within the meaning of the AI Act. A Social Artificial Intelligence Board will be set up to advise and consult with the Committee.

The draft also includes:

- regulations concerning the oversight of the market for AI systems and general-purpose AI models;
- procedures concerning infringement of the AI Act, including a settlement mechanism enabling extraordinary mitigation of sanctions (by between 20% and 90% depending on the circumstances) where the infringing party co-operates with the Committee and remedies the breach;
- rules for imposing administrative fines for infringements of the AI Act;
- provisions on reporting serious incidents that have occurred in connection with the use of AI systems;
- provisions setting out the ability to obtain an individual opinion on the application of the AI Act or the Polish Act on AI Systems, which opinion is binding on the Committee and other public authorities involved in its issuance;
- regulations on regulatory sandboxes; and
- conditions and procedures for accreditation and notification of conformity assessment bodies.

Poland is working on the implementation of the Product Liability Directive 2024/2853, which should be finalised by 9 December 2026. The Ministry of Justice is currently carrying out evaluation and analysis, with the participation of the Polish Office of Competition and Consumer Protection. Though the draft law is not yet available, the Directive will be implemented through amendments to the product liability provisions in the Polish Civil Code and in the consumer protection regulations.

As most AI tools are delivered via the public cloud through a software as a service model, the recently announced plans of the Polish government to adopt a new law on cloud computing are of significance for AI adoption. The purpose of the Polish Cloud Act is to create a single, all-encompassing regulatory framework for the cloud. According to the government, the Act will be applicable to all cloud providers, irrespective of their ownership, and is not aimed at restricting the access of US providers to the Polish market. The Act is to introduce sovereignty requirements based on the EU Sovereign European Assurance Levels (SEAL) framework, which defines clear criteria and scoring methods to evaluate how providers meet EU sovereignty standards. Moreover, Poland intends to create data embassies, like those implemented by Estonia. The Ministry of Digitalisation is responsible for the legislative process and is carrying out market consultations. Work on the draft will continue in 2026.

AI governance and shadow AI

Based on the research project carried out by the Research and Academic Computer Network (*Naukowa i Akademicka Sieć Komputerowa*, or NASK), most employees have already used AI tools, but only 9.4% of enterprises have formally introduced AI tools for use by employees. Lack of officially implemented tools leads to a situation when almost 80% of employees use only the free version of AI tools, while only 4.5% use the paid version exclusively. Around 13% use both free and paid versions. At the same time, 68% of employees indicated that there are no internal guidelines on use of AI in the work environment.

This shows that most employees are using versions of AI tools that allow providers to train their models on both input and output data. This constitutes

a serious risk to the confidentiality of trade secrets and other sensitive employer information, as well as to the proper processing of personal data included in user inputs. Typically, such free tools do not offer an appropriate level of data and trade secrets protection, and frequently involve transfers of data to third countries, including China or India. This poses a serious threat to employers. First, the information may be leaked or accessed by third parties. Second, it may be used to train AI models, and its content may be indirectly disclosed to any other user of that AI tool. Consequently, enterprises may not only lose their own valuable assets, such as inventions or the results of research – and, consequently, business opportunities – but they may also incur liability towards their customers or regulators. Such liability may arise, for example, where confidential third-party information is disclosed or where personal data is not properly protected. The fact that the vast majority of employers have not introduced any rules on the use of AI means that it will be difficult to hold employees liable for such actions and even to undertake any disciplinary actions against those employees. The employer's inaction might also be seen as gross negligence in disputes with third parties or in regulatory investigations involving disclosed confidential information. This is because the risks associated with AI should already be well understood by prudent businesses.

These risks are not theoretical. There has already been a case in which the Polish National Centre for Research and Development (NCBR) rejected the grant application based on its expert opinion that the research project described in the application pertained to already existing and well-developed technology. It turned out that the employees of the Centre used a free version of an AI tool to assess the grant application and leaked the confidential information contained therein to the model. This information was apparently used in model training and improvement and as a result, subsequent questions to the AI model disclosed this information to anyone who asked. The Polish Patent Office also warned that using AI models which do not offer an appropriate level of security may lead to public disclosure of information and as a result, as the confidentiality of the invention is one of the conditions of granting patent protection, such disclosure will make it impossible to obtain a patent.

At the same time, the research shows that when companies made approved AI tools available to their employees, almost 80% of employees used such tools. This shows that employees opt for the tools offered by their employers, if available, even if they do not have official guidelines. Implementing this measure would substantially reduce AI-related risk, although it would not fully eliminate it.

AI governance, including clear instructions on what is allowed and how employees may use AI systems is also becoming obligatory if employers intend to mitigate AI-related risks.

Summary

AI adoption in Poland is accelerating, backed by significant public funding (including the planned PLN4.5 billion Artificial Intelligence Fund) and measurable private sector uptake. It is also possible to discern the first labour-market effects of AI, especially in the ICT sector, as demand is shifting away from junior ICT roles toward more experienced workers who can supervise and leverage AI for complex tasks. Poland is also working on implementation of the EU's AI Act and 2024 Product Liability Directive. Poland's draft Act on AI Systems (adopted by the Council of Ministers on 31 March 2026) indicates a move toward structured enforcement but it also envisages the settlement options in case of breach, interpretative opinions and regulatory sandboxes. Planned cloud legislation (the proposed "Cloud Act") aims to create a comprehensive framework, introducing sovereignty requirements aligned with the EU SEAL framework and exploring "data embassies", which could materially shape the operating model for cloud-based AI. For organisations, "shadow AI" is a primary near-term risk: widespread employee use of mostly free tools without policy coverage can trigger trade secret leakage, problematic international transfers, non-compliance with personal-data regulation, and weakened ability to enforce discipline. The strongest practical risk-reduction lever highlighted is to provide approved enterprise-grade AI tools and pair them with clear internal governance: what is allowed, how to use it, and where human review is mandatory.

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 Luke.Wilson@Chambers.com