Legal 500
Country Comparative Guides 2026

Poland
Artificial Intelligence

Contributor

Sołtysiński Kawecki &
Szlęzak

Agata Szeliga

Partner | agata.szeliga@skslegal.pl

Sylwia Macura–Targosz

Senior Counsel | sylwia.macura-targosz@skslegal.pl

Anna Tujakowska

Senior Counsel / Head of Legaltech & Innovation | anna.tujakowska@skslegal.pl

Maciej Gil

Senior Associate | maciej.gil@skslegal.pl

Katarzyna Wnuk

Senior Associate | katarzyna.wnuk@skslegal.pl

Sandra Słowik

Associate | sandra.slowik@skslegal.pl

Michał Kalinowski

Associate | michal.kalinowski@skslegal.pl

Poland: Artificial Intelligence

1. What is the legal definition of "artificial intelligence" in your jurisdiction, if any? If no definition exists, how do regulators or courts typically describe artificial intelligence?

Polish law does not contain an autonomous, national statutory definition of "artificial intelligence". The operative legal definition is that of an "AI system" set out in Article 3(1) of the EU AI Act which applies directly in Poland. Consequently, local legislation (see point 3), i.e., the AI Systems Act, deliberately refrains from creating its own definition.

Polish case law on AI remains limited and no court has yet attempted to define the concept. However, the decisions issued to date suggest that a pragmatic, functional approach is beginning to emerge, i.e., an approach focused on what an AI system does and on the reliability of its outputs, rather than on how it is built. In a judgment of 28 January 2026 (I FSK 800/23) concerning VAT taxation, the Supreme Administrative Court ("NSA") held that an AI algorithm autonomously trading financial instruments on behalf of clients performs a brokerage-type service and is entitled to the same VAT exemption as human brokers as the pertinent issue is the economic substance of the service, not whether it is provided by a human or a machine. In another decision, the NSA noted the growing use of AI by the legal profession but raised concerns about overreliance on its outputs and lack of verification of the results by the attorney-in-fact (judgment of 23 June 2026, case no. I FZ 104/26). The National Appeals Chamber (KIO) decision shows that using AI-generated content without verification may lead to a loss of a public procurement contract (KIO 3347/25, judgment of 17 October 2025).

2. Has your country developed a national strategy for artificial intelligence? If yes, what progress has been made in its implementation? Are there plans for updates or revisions?

Yes. Poland has adopted an AI national strategy. The first AI policy was adopted by the Council of Ministers in December 2020. In November 2025, it was comprehensively updated as the "Policy for the Development of AI in Poland until 2030" ("AI Policy"), establishing a coordinated framework for AI development. The Policy is structured around five core objectives:

(i) building a coordinated national AI ecosystem to develop economy and society wellbeing;

(ii) developing above average AI competences in society;

(iii) deploying AI in public administration;

(iv) driving AI adoption in key economic sectors as an active part of an AI Continent; and

(v) ensuring trustworthy, human-centered AI in compliance with the EU AI Act and the GDPR.

The Minister of Digitalization is responsible for coordinating the implementation of the AI Policy.

Based on Eurostat data, the rate of AI adoption among businesses has grown, reaching 8.4% of companies in 2025; however, it remains much below the EU average of 19.95%. Poland has developed two flagship large language models: PLLuM, an initiative developed by scientific institutions with support from the Ministry of Digital Affairs, and Bielik, developed by the SpeakLeash Foundation. Together, they form the foundation of Poland's strategy for building a sovereign AI ecosystem. In February 2025, the IDEAS Research Institute was established to conduct AI research and development at the highest standards of scientific excellence. Additionally, AI HUB Poland is being developed as a central platform for managing, developing, and deploying AI technology in the Polish public sector, with AI already deployed in citizen-facing services. For example, the mObywatel government application has integrated an AI-powered assistant enabling citizens to obtain information on administrative procedures and public services through a conversational interface. Two AI factories are also being established, i.e., the GAIA AI Factory in Kraków and the PIAST AI Factory in Poznań, with Poland further participating in the Baltic AI GigaFactory project aimed at strengthening European technological sovereignty.

On the legislative side, a draft AI Systems Act is currently progressing through the legislative process (see point 3 below). The AI Policy is subject to annual review and update.

3. Has your jurisdiction adopted any AI-specific laws, regulations, voluntary standards, or ethical guidelines? If so, please provide a brief overview. If not, which existing laws could be/are applied to artificial intelligence and the use of artificial intelligence, what are the main interpretive challenges, and are there any pending artificial intelligence legislative initiatives?

The EU AI Act is applicable. Further, Poland is adopting domestic AI legislation, i.e., the AI Systems Act, which will support the implementation of the EU AI Act into Polish law. Parliamentary work on the bill has concluded, and the bill has been submitted to the President. Once the President signs the bill, the AI Systems Act will enter into force in 14 days from publication (likely still in Q3 2026).

The AI System Act covers the following matters:

- establishing a dedicated national supervisory authority, i.e., the AI Development and Security Commission ("**KRiBSI**"; see question 16), and an advisory body, i.e., the Social Council for AI;
- regulations concerning the oversight of the market for AI systems and general-purpose AI models;
- procedures for EU AI Act enforcement and administrative fines, including a settlement mechanism enabling the extraordinary mitigation of sanctions (20% – 90% depending on the circumstances) for parties that co-operate with KRiBSI and remedy breaches; and
- provisions regarding creating regulatory sandboxes for testing AI technologies.

Further, Poland is working on the implementation of EU Directive 2024/2853 on liability for defective products. A draft implementing act has already been published and proposes changes to the Polish Civil Code and Code of Civil Procedure. The draft would replace the current Polish product liability regime which is based on the implementation of Directive 85/374/EEC, as the new Directive introduces substantial changes that cannot be accommodated through a simple amendment. The proposed reform expands the notion of a product to include software and software-enabled products, including AI systems, broadens the categories of potentially liable entities, extends the scope of recoverable damage, and introduces measures aimed at easing the claimant's burden of proof, including disclosure mechanisms and rebuttable presumptions.

Also, existing laws may be applied to AI, including privacy regulations (data processing), copyright regulations (copyright infringements, authorship of AI-generated outputs, and training of AI models on copyrightable models), and the Civil Code (general tort and contract liability).

Finally, many local guidelines have been issued to cover the use of AI in various sectors, including:

- Guidelines on AI for Public Administration by the Ministry of Digitalization (2026);
- Recommendations on AI for judges by the Polish Judges' Association Iustitia (2026);
- Recommendations on AI-based tools for attorneys-at-law by the National Council of Attorneys-at-law (2025);
- Recommendations on AI in justice and law enforcement by the Ministry of Digitalization's AI Working Group (2024);
- Recommendations on prohibited AI systems by the Ministry of Digitalization (2024);
- White Book on AI in Clinical Practice by the Polish Hospital Society (2022);
- Recommendations on AI in the financial sector by the Ministry of Digitalization's AI Working Group (2022); and
- The position of the Financial Supervision Authority on robo-advisory services (2020).

4. Are there legal requirements for artificial intelligence transparency, explainability, or audits? Are there obligations to disclose the use of artificial intelligence to customers/clients?

On the EU level, the EU AI Act includes transparency rules which will be applicable from 2 August 2026 (with a transition period for providers of AI systems generating synthetic audio, image, video, or text content that have been placed on the market before 2 August 2026; those providers must take the necessary steps to comply with Article 50(2) by December 2026). Individuals must generally be informed when they are interacting with an AI system, and providers of systems generating AI-created content must ensure that such content is identifiable and detectable as artificially generated or manipulated. Deployers must also disclose the use of emotion recognition and biometric categorization systems, as well as the use of deep fakes and certain AI-generated text published on matters of public interest, subject to limited exceptions. All required disclosures must be provided clearly, be accessible, and be no later than the first interaction with, or exposure to, the AI-generated content or system.

In June 2026, the European Commission published a

Code of Practice on the Transparency of AI-Generated Content and a set of icons for deployers of generative AI systems to label their AI-generated content. This document is now subject to verification and further complementation. Once positively assessed, signatories may rely on the Code to demonstrate compliance with the AI Act's transparency requirements.

The Polish AI Systems Act does not introduce AI transparency obligations beyond those under the AI Act and the GDPR. However, it does require participants in regulatory sandboxes to inform affected users and third parties of their participation and its terms. Also, in respect to courts, the draft implementation of EU Directive 2024/2853 requires the publication of appeal court judgments issued in proceedings under the Directive.

5. Are there legal requirements or best practice expectations for human oversight and human-in-the-loop in artificial intelligence systems?

The main source of human oversight and human-in-the-loop requirements is the EU AI Act, especially Art. 4 regarding so-called AI Literacy, as well as Art. 14 on human oversight.

The AI Systems Act does not impose any additional obligations in this regard. However, under the AI Systems Act, by 31 March of each year, KRiBSI is required to publish an annual information report containing examples of good practices for how entrepreneurs and public sector entities should implement and use AI systems. Therefore, it may be expected that such soft-law recommendations will be published in the future.

The March 2026 "Guide to AI for Public Administration" sets out a core principle that each use of AI systems in decision-making should always be subject to human oversight. The recommended workflow is described as follows:

1. an employee identifies a specific issue or problem to be resolved and submits it in the form of a prompt (i.e., a question or description of the issue) to the AI system;
2. the AI system prepares an analysis, summary, or draft response;
3. a human expert reviews, corrects, and approves the response; and
4. the information on what has been accepted, rejected, or amended is recorded and may be used to further improve the model.

6. Are there specific legal or regulatory requirements addressing algorithmic bias, discrimination, or fairness in AI systems (including gender bias)?

Neither the AI Systems Act nor other national regulations impose specific requirements addressing algorithmic bias, discrimination, or fairness in AI systems. These matters are addressed at the level of the AI Act, in particular, under Article 10 regarding data and data governance or in the GDPR.

The only tangentially related provision is the requirement for KRiBSI to cooperate with the Polish Data Protection Authority ("PUODO") on matters concerning fundamental rights. However, this constitutes an organizational rule rather than a substantive requirement targeting bias or discrimination.

7. What legal frameworks apply to AI-related harm and defective artificial intelligence systems? Who can be held liable (developer, deployer, victim of the damage, others), how is liability allocated, and what burden of proof applies to victims?

There are no separated, tailor-made regulations related to liability connected to the use of AI systems. Thus, standard civil law rules apply. Depending on the specific scenario, we may consider:

- general tort liability;
- strict liability;
- product liability; and
- contractual liability.

Under general tort law, a claimant must establish three elements, i.e. wrongful conduct (fault), harm, and a causal link between the two. Applying this framework to AI-related damage is challenging as the complexity and lack of transparency of AI models often make it difficult to identify the party at fault or the mechanism of harm. A user who follows the provider's guidelines may demonstrate absence of fault, whereas modifying the AI code or deploying the system beyond its intended scope may constitute fault on the user's part.

Polish law provides a strict liability rule for enterprises or facilities that are set in motion by forces of nature, such as steam, gas, electricity, or liquid fuels. Operators of these enterprises bear liability for any personal injury or property damage arising from their operations, regardless of fault. These rules may apply for instance when the AI

system is used in running a railway transport company or factory, and damage occurs.

Under the existing Polish product liability regime, which transposes Council Directive 85/374/EEC, the notion of a "product" is confined to tangible movable goods. As a consequence, AI systems – whether deployed as standalone software or as a service – fall outside the scope of this framework and cannot currently give rise to product liability claims. This rule has changed under the new Directive 2024/2853 which considers software to be a "product" under product liability rules. This definition extension has been adopted in the project of Polish implementation of this Directive which is currently subject to the legislative process. See Question 3.

Under contractual liability, the aggrieved party may seek damages for non-performance or the improper performance of the contract. To succeed, the party must demonstrate a breach, harm, and a causal link between the two. Polish law presumes fault on the part of the party alleged to have caused the damage, which must prove its absence to be exonerated. The transparency challenges described above apply equally in this context. In practice, providers typically cap their aggregate liability vis-à-vis deployers, and deployers do likewise vis-à-vis end clients. However, contractual limitations or exclusions of liability are unenforceable in consumer contracts, and where the damage results from intentional misconduct in business-to-business relationships.

8. What cybersecurity obligations apply to AI systems?

The AI Systems Act does not provide any additional cybersecurity obligations on AI system providers or operators. However, the Act creates a coordination framework linking AI oversight with the national cybersecurity architecture. KRiBSI is tasked with countering security threats to AI systems and is required to cooperate with the Government Plenipotentiary for Cybersecurity and the three national CSIRT [PorSim1.1]teams (CSIRT GOV, CSIRT MON, and CSIRT NASK) concerning incident response and information exchange. Additionally, it amends the Act on the National Cybersecurity System to impose a reciprocal duty of cooperation with KRiBSI on entities within that system. These provisions are organizational in nature and do not create enforceable obligations for private-sector AI developers or deployers.

At the most general level, the principal piece of Polish cybersecurity legislation is the Act on the National Cybersecurity System ("NCSSA") which establishes the institutional framework for national cybersecurity and sets out the obligations incumbent upon the entities falling within its scope. On 3 April 2026, amendments transposing the EU NIS2 Directive became effective. These amendments significantly elevate cybersecurity standards by introducing more stringent risk-management measures, enhanced incident-notification duties, and reinforced supply-chain security obligations, while simultaneously broadening the categories of key and important entities subject to the regime across additional sectors. While the NCSSA does not specifically target AI, it nonetheless carries implications for providers and users, within the meaning of the NCSSA, of AI-driven solutions that fall within the Act's regulatory perimeter, particularly where such solutions constitute or are integrated into regulated ICT services or infrastructure. Moreover, AI vendors that are not themselves subject to the NCSSA may nevertheless be indirectly affected as regulated entities frequently cascade compliance and security obligations onto their suppliers through contractual arrangements.

There is no soft law on a national level in this scope. The main reference is the "Guidelines for secure AI system development" published by the NCSC (UK) and CISA (USA).

At the level of government bodies, general cybersecurity obligations also arise under the Act on Crisis Management, although that legislation does not contain any AI-specific provisions.

9. Is the use of artificial intelligence insured and/or insurable in your jurisdiction, including with cyber policies? Are there market trends, or limitations?

In Poland, AI-related risks are generally insurable, though no standalone AI insurance product currently exists. Coverage is instead channeled through existing lines, i.e., principally cyber insurance, professional indemnity (E&O), product liability, and D&O policies, with AI treated as a risk-aggravating factor rather than a distinct coverage category. However, the market is adapting, albeit slowly and reactively. Some insurers have begun extending cyber policy wordings to address AI-specific scenarios, including model errors, adversarial attacks, and data poisoning, while underwriting questionnaires increasingly require disclosure of AI deployment as part of risk assessment. However, significant limitations persist. The absence of historical loss data and actuarial benchmarks makes AI risk difficult to price accurately, resulting in conservative coverage limits, broad exclusions, and

inconsistent policy wordings across insurers. Consequently, the scope of coverage for any given AI-related incident may remain uncertain until a claim is actually made.

10. Can artificial intelligence be named as an inventor in a patent application filed in your jurisdiction? If not, what is the current legal position?

No. Under Polish law, AI cannot be named as an inventor in a patent application.

Poland's primary patent legislation is the Act of 30 June 2000 on Industrial Property Law ("IPL"). Article 8 IPL grants inventors, as persons, the right to obtain a patent, receive remuneration, and be named in official registers. The term twórca (inventor/creator) used throughout the IPL presupposes a natural person; the statute contains no mechanism for designating an AI system in that role or any rules defining who should be entitled to obtain a patent for an invention created by an AI system. This is reinforced by the implementing regulations to the IPL which require the patent application to include the surname, first name, and residential address of the inventor, i.e., data that by their nature can only pertain to a natural person. As of the date of this guide, the Polish Patent Office has not issued formal guidance specifically addressing AI inventorship.

Poland is a contracting state to the European Patent Convention. The EPO Board of Appeal in J 8/20 confirmed that only a natural person may be designated as inventor, rejecting the argument that the DABUS AI system could qualify. The Board reasoned that a machine, lacking legal personality, cannot transfer rights to the applicant.

Importantly, inventions developed with AI assistance are not excluded from patentability. A human contributor may be designated as the inventor if they made a sufficient creative contribution. This requires a case-by-case assessment, considering factors such as: (i) whether the human formulated the technical problem; (ii) the degree to which the human configured the AI tool and its parameters; and (iii) whether the human refined the AI-generated output.

11. Do images or works generated by and/or with artificial intelligence benefit from copyright protection in your jurisdiction? If so, who is the authorship attributed to, and under what conditions?

Under Polish law, copyright protection arises by operation of law; there is no requirement to file an application, and no Copyright Office exists. The Act on Copyright and Related Rights of 4 February 1994 ("Copyright Act") defines a work as any manifestation of a creative activity of an individual nature. This definition rests on three cumulative requirements: creativity, individuality, and fixation. Crucially, under Polish law, only humans can be recognized as authors. Content generated autonomously by AI without meaningful human creative input cannot satisfy the requirements of creativity and individuality, as these presuppose subjective choices made by a natural person. Consequently, content autonomously generated by AI falls outside the statutory definition of a work and does not attract copyright protection.

A more nuanced question arises where humans and AI interact in the creative process. Where a human actively shapes the output through iterative selection, arrangement, and correction, the result may qualify as a copyrightable work with authorship attributed to the human, treating AI as a tool. Where AI operates autonomously, no protection arises.

This approach is reflected in the practice of ZAiKS, the largest copyright collective management organization in Poland, which has amended its regulations, i.e., AI-generated works are generally excluded from registration, though works co-created with AI may be registered if the human creative contribution is quantified by a percentage indicator.

It should also be noted that the Copyright Act regulates related rights (neighboring rights), including the rights of producers of phonograms and videos, broadcasters, and performers. Unlike copyright, certain related rights do not require creative input by a natural person and may therefore, in principle, extend to AI-generated content, e.g., where an AI-generated recording qualifies as a phonogram or video, the producer's related rights may arise irrespective of the absence of a human author.

As of the date of this guide, there is no Polish case law directly addressing the issues discussed above.

12. What are the main issues to consider when using artificial intelligence systems in the workplace? Have any new regulations, or guidelines, been introduced regarding AI-driven hiring, performance assessment, or employee

monitoring?

Poland has not introduced legislation or official guidelines specifically addressing the use of AI in the workplace. Accordingly, employers using AI must ensure compliance with the applicable legal framework, including the AI Act, the GDPR, and the Polish Labor Code. Discussions during the 2026 Data Protection and New Technologies Congress co-organized by PUODO emphasized that AI should support, rather than replace, human decision-making in employment-related processes and that appropriate risk assessments under both the GDPR and the AI Act should precede deployment.

Employers should first determine whether the AI Act applies to the intended use of the AI system and if yes, to what extent. The AI Act prohibits the use of AI systems to infer the emotions of individuals in the workplace, subject only to narrow exceptions relating to medical or safety reasons (Article 5(1)(f)). Many AI systems used in employment are likely to qualify as high-risk AI systems under Article 6(2) in conjunction with Annex III of the AI Act. This includes, for example, AI systems intended for recruitment or selection, as well as those used to make decisions affecting the terms of employment, promotion or termination, task allocation, or monitoring and evaluating employees' performance and behavior. Employers must therefore comply with the applicable obligations relating to such high-risk AI systems. In addition, the AI Act provides for transparency obligations in relation to certain AI systems (Article 50), meaning that requirements may also arise even where an AI system is neither prohibited nor classified as high-risk.

From a data protection perspective, employers must also ensure compliance with the GDPR. Among other obligations, the deployment of AI may require carrying out a data protection impact assessment ("DPIA"). In this respect, PUODO has expressly indicated that the processing of personal data in connection with the deployment of high-risk AI systems is highly likely to result in a high risk to individuals' rights and freedoms and therefore requires a DPIA. Other key considerations include identifying the relevant legal basis for processing, complying with the principles of purpose limitation, data minimization and transparency; ensuring appropriate data security; and meeting the requirements relating to solely automated decision-making (Article 22).

In certain cases, the use of AI in the workplace may also constitute employee monitoring under the Polish Labor Code. Such monitoring is permissible only for the purposes expressly provided for in the Labor Code. Employers must also, among other things, regulate the purposes, scope, and methods of such monitoring in the work regulations and comply with the applicable information obligations under the Labor Code and the GDPR. The legal basis for processing personal data collected through such monitoring will typically be the employer's legitimate interest under Article 6(1)(f) of the GDPR which requires employers to carry out and document a legitimate interest assessment (LIA).

Beyond the applicable legal requirements, employers should also be aware of the growing practical challenges associated with the use of AI in the workplace. According to a recent study published by the Polish National Research Institute, NASK (available at: https://cyberpolicy.nask.pl/miedzy-optymizmem-a-niepewnoscia-spoleczne-postawy-wobec-cyberbezpieczenstwa-w-polsce/), more than 70% of employees using generative AI at work rely on private AI tools for work-related tasks, while nearly 30% do so without their employer's knowledge, highlighting the growing phenomenon of "Shadow AI". These findings demonstrate that internal AI governance has not kept pace with the widespread use of AI, exposing employers to increased risks relating to regulatory compliance, information security, and potential liability arising from employees' use of unauthorized AI tools.

13. What are the main privacy/data protection issues arising from artificial intelligence development and use (including training data)? Have data protection authorities issued guidelines or rulings on artificial intelligence, and what are the key takeaways?

The Polish Data Protection Authority (*Prezes Urzędu Ochrony Danych Osobowych*, PUODO) is investigating a complaint against ChatGPT alleging the unlawful, unfair, and non-transparent processing of personal data, including the generation of inaccurate information and failures to comply with GDPR data subject rights. The case remains pending and may clarify key privacy issues related to AI.

Apart from that, PUODO has been active in the AI space, primarily through legislative opinions and educational activities. It has emphasized the continued applicability of the GDPR to AI systems and its role as the competent authority for personal data protection in the AI context. In 2025, PUODO published guidance on Data Protection Impact Assessments in the context of AI. In 2026, it also published a report on organizations' readiness for responsible AI deployment under the GDPR and AI Act, identifying priority areas for PUODO's future AI-related

activities. Moreover, PUODO has increasingly focused on the risks posed by AI-generated deepfakes, particularly those affecting children and vulnerable individuals. It has called for stronger legal and enforcement measures, including rapid removal mechanisms for harmful deepfake content and other unlawful online content involving personal data. PUODO has also promoted educational initiatives on AI-related risks and supported the inclusion of deepfake-related topics in school curricula.

However, PUODO has not yet issued comprehensive AI-specific guidance.

On the EU level, AI privacy issues are also addressed in the European Data Protection Board's ("**EDPB**") Opinion 28/2024. The EDPB clarified that AI models trained on personal data are not automatically anonymous and must be assessed on a case-by-case basis under the GDPR.

The main privacy issues arising from AI are:

- **Lawful basis for training data.**AI training involving personal data requires a valid GDPR legal basis, most commonly legitimate interests or consent (however, the latter may be difficult to obtain). Special category data may be used only under limited Article 9 GDPR exceptions and must otherwise be filtered out; where separation is not feasible, Article 9 GDPR may apply to the entire dataset. The proposed Digital Omnibus package would introduce a new legal basis for processing special category data for AI bias mitigation.
- **Purpose limitation.**Using personal data for training or fine-tuning may be inconsistent with original collection purposes. Controllers should assess compatibility under Article 6(4) GDPR. The processing purpose must be specified early in the development lifecycle, and the expected deployment context should be considered even where the final use case is not yet fully known.
- **Transparency / "black box" and accountability.**Complex AI models make it difficult to fulfil information obligations and explain processing to data subjects. Reliance on the Article 14(5)(b) exception for web-scraped training data is strictly limited. AI training must be documented, with privacy by design (Article 25 (1) GDPR) implemented throughout the model lifecycle.
- **Data minimization during training.** Large-scale processing of personal data during training creates tension with the minimization principle. Controllers must consider whether the training purpose can be achieved with less personal data or alternative datasets, such as anonymized or synthetic data, and ensure that only the personal data necessary for that purpose is processed (Article 5 (1) (c) GDPR).
- **Data subject rights.**Rights of access, rectification, erasure, and objection apply with no specific AI exemptions. Controllers must determine whether retraining or other technical measures are needed to honor erasure requests. Further, AI-generated outputs may be false. Where they relate to an identifiable person, they may constitute personal data subject to rectification and data subject rights may apply.
- **Automated decision-making.**AI-driven profiling and solely automated decisions with legal or similarly significant effects are restricted under Article 22 GDPR which requires a lawful exception, appropriate safeguards, and a right to human review. However, Article 22 GDPR is unlikely to apply where AI only supports decisions.

14. How is data scraping regulated in your jurisdiction from an IP, privacy and competition perspective? Are there recent precedents addressing the legality of data scraping for training of artificial intelligence systems?

Data scraping in Poland is not governed by a single statute. Its legality depends, among other things, on the nature of the scraped content, the method of access, and the purpose of use.

From an IP perspective, scraping may infringe copyright where it involves the reproduction or use of protected works under the Copyright Act. It may also infringe sui generis database rights under the Polish Database Protection Act of 27 July 2001 where the scraped material forms part of a database in which the producer made a substantial investment. The DSM Copyright Directive, as implemented in Poland, introduced TDM exceptions, e.g., a mandatory exception for scientific research and a broader exception for commercial TDM, unless the rightsholder has effectively reserved its rights. This is particularly relevant for AI training as datasets are often created through large-scale scraping. The EU AI Act reinforces this framework by requiring GPAI model providers to comply with EU copyright rules, including TDM rights reservations.

Where scraping involves personal data, the GDPR applies alongside with the Polish Personal Data Protection Act of 10 May 2018. Together, this constitutes personal data processing, and therefore a legal basis under Articles 6 or 9 GDPR is required, as well as compliance with the principles set out in Article 5 GDPR, including lawfulness, fairness, transparency, data minimization, and accuracy. Key issues include identifying a lawful basis, transparency, purpose limitation, data minimization, storage limitation, data subject rights, and processing special category data. The most significant Polish case is the March 2019 decision of the President of the Personal Data Protection Office in the Bisnode case, imposing a fine of approximately EUR 220,000 for scraping publicly available data without fulfilling Article 14 GDPR obligations (the information obligation). The Warsaw Regional Administrative Court partially set aside the decision (annulling the fine and the order insofar as it concerned individuals who had ceased trading), but upheld the finding of the Article 14 GDPR infringement in respect of active sole traders. The Supreme Administrative Court dismissed the company's cassation appeal in its judgment of 19 September 2023 (III OSK 2538/21), holding that the "disproportionate effort" exception under Article 14(5)(b) GDPR cannot, in principle, apply where data from public registers are processed for commercial purposes, as such processing does not pursue a public interest, and that the public availability of data in official registers does not relieve the controller of its transparency obligations. Notably, the Bisnode ruling stands in contrast to PUODO's earlier decision concerning the ePaństwo Foundation's Rejestr.io service which aggregated data from the National Court Register (KRS) for public-interest transparency purposes. In that case, PUODO accepted that the disproportionate effort exception under Article 14(5)(b) GDPR could apply, given the civic nature of the processing and the lack of direct contact data for all data subjects.

At the EU level, the EDPB Opinion 28/2024 confirms that legitimate interests require a full balancing test, that the reuse of scraped data for AI training must comply with purpose limitation rules, and that AI models should not automatically be treated as anonymous. The EDPB also stated that the development phases of AI models may involve the collection of large amounts of data from publicly available sources (such as web scraping techniques), reliance on the exception under Article 14(5)(b) GDPR is strictly limited to situations where the requirements of that provision are fully met. Furthermore, on 7 July 2026, the EDPB adopted Guidelines 03/2026 on web scraping in the context of generative AI (the version for public consultation) which set out practical expectations for private entities scraping data to train generative AI models. In particular, the Guidelines require controllers to satisfy a three-step legitimate interest test, including the adoption of concrete mitigating measures such as excluding high-risk website categories, facilitating opt-out mechanisms, and limiting memorization and regurgitation risks. Controllers are expected to apply data minimization safeguards both before collection (e.g., defining precise scraping criteria, using robots.txt exclusions, and filtering out unnecessary data categories) and after collection (e.g., replacing personal data with synthetic data, and applying pseudonymization or anonymization). As regards transparency, the Guidelines clarify when the disproportionate effort exception under Article 14(5)(b) GDPR may apply. On special categories of personal data, the Guidelines indicate that the CJEU ruling in GC & Others (C-136/17) may justify the incidental collection of such data if the controller deploys technical and organizational safeguards, including pre-collection filters, the prompt deletion of identified sensitive data, output filtering, and ongoing monitoring, within the framework of its responsibilities, powers, and capabilities.

Scraping may also constitute an act of unfair competition under the Unfair Competition Act where the conduct is contrary to law or good practice, and threatens or infringes the interests of another undertaking or a customer. In particular, free-riding on a competitor's investment or undermining its revenue model may be regarded as contrary to good practice. As regards competition law, there are currently no decisions of the President of the Office of Competition and Consumer Protection addressing scraping for AI training purposes. Finally, the AI Act prohibits AI systems that create or expand facial recognition databases through untargeted scraping of facial images from the internet or CCTV. It also imposes data governance obligations on providers of high-risk AI systems.

15. To what extent is the prohibition of data scraping in the terms of use of a website enforceable?

A prohibition of data scraping in a website's terms of use may be enforceable in Poland, but its practical strength depends on how the terms were incorporated and whether the prohibition is supported by additional statutory rights.

Website terms may form a binding agreement where they are effectively incorporated and made available to the user in accordance with the Polish Civil Code ("CC"). If a user scrapes a website in breach of an express

prohibition, the operator may rely on contractual remedies, including damages under Article 471 CC, and may seek injunctive relief to compel the cessation of such conduct. This route may be particularly important where the scraped material does not qualify for copyright or sui generis database protection. The CJEU confirmed in Ryanair v PR Aviation (C-30/14) that contractual limitations may be enforceable under national law even in relation to databases falling outside the scope of the Database Directive.

Terms of use can also serve as a rights reservation for the purposes of the commercial TDM exception if the reservation is expressed in an appropriate manner, including in a machine-readable form. Where such opt-out is validly made, commercial scraping for AI training may require authorization from the rightsholder.

A scraping prohibition may further support an unfair competition claim under the Unfair Competition Act (as discussed in Question 14 above).

Overall, enforceability is the strongest where several bases converge, e.g., properly incorporated contractual terms, statutory IP or database protection, a valid TDM opt-out, and evidence of unfair competition.

16. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence? What are its powers and enforcement tools?

As noted in response to Question 3, parliamentary work on the AI Systems Act envisages the establishment of AI Development and Security Commission (Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji, "KRiBSI") as Poland's national market surveillance authority within the meaning of Article 70(1) EU AI Act. KRiBSI will also serve as the single point of contact referred to in Article 70(2) of that Act.

KRiBSI will consist of a Chair, two Deputy Chairs, and four members. The Chair will be appointed by the Lower Chamber of Polish Parliament (Sejm), with the consent of the Upper Chamber (Senate), for a five-year term. The Deputy Chairs will be appointed by the Chair of KRiBSI for five-year terms following an open and competitive recruitment procedure. The four members will be designated respectively by the President of the Office of Competition and Consumer Protection (UOKiK), the Polish Financial Supervision Authority (KNF), the National Broadcasting Council (KRRiT), and the President of the Office of Electronic Communications (UKE). KRiBSI's meetings may also be attended, in an advisory or observer capacity, by representatives of other public bodies and experts with relevant specialist knowledge. In addition, the Social Council for AI (Społeczna Rada ds. Sztucznej Inteligencji) will operate alongside KRiBSI as an advisory and consultative body composed of 9 to 15 experts in AI, including cybersecurity, data protection, and human rights.

Although KRiBSI will operate within the organizational structure of the Ministry of Digital Affairs, which will provide its administrative support, the AI Systems Act expressly guarantees the independence of its Chair, Deputy Chairs, and members in the exercise of their functions.

KRiBSI's tasks will include, in particular:

- supervising compliance with the EU AI Act and the AI Systems Act;
- taking measures to promote the proper functioning of the EU internal market for AI systems;
- supporting and monitoring the development, innovation, and competitiveness of AI research and the deployment of AI systems;
- taking measures to counter threats to the security of AI systems;
- participating in the preparation and review of draft government documents relating to artificial intelligence, including draft legislation;
- issuing decisions in proceedings concerning infringements of the EU AI Act and the AI Systems Act;
- performing the tasks and exercising the powers of a market surveillance authority under the EU AI Act;
- issuing individual opinions on the application of the EU AI Act and the AI Systems Act in specific cases, as well as general explanations on the application of those instruments;
- preparing and publishing AI-related publications, implementing educational programs, and carrying out information and awareness-raising activities; and
- establishing and managing regulatory sandboxes.

KRiBSI will be authorized to conduct remote or on-site inspections and issue post-inspection recommendations requiring the rectification of identified irregularities. Moreover, KRiBSI may initiate infringement proceedings ex officio, including on the basis of information gathered during inspections or complaints concerning alleged infringements of the EU AI Act or the AI Systems Act. In

infringement proceedings, KRiBSI may issue warnings specifying remedial measures, including measures such as blocking access to an AI system and fulfilling information obligations towards specified categories of persons. Where an AI system poses a direct risk to life, health, safety, or the fundamental rights of natural persons, KRiBSI may order the operator to cease using the system or withdraw it from the market or from use. Such decisions may be declared immediately enforceable. KRiBSI may impose administrative fines in accordance with Chapter XII of the EU AI Act. The AI Systems Act also introduces a settlement mechanism allowing fines to be reduced by between 20% and 70% (or by between 30% and 90% in self-reporting cases) if the party cooperates with KRiBSI and remedies the infringement. Decisions of KRiBSI will be subject to judicial review before the Competition and Consumer Protection Court of the Regional Court in Warsaw (Sąd Okręgowy w Warszawie – sąd ochrony konkurencji i konsumentów).

17. How widespread is the adoption of artificial intelligence in businesses in your jurisdiction, and which sectors are leading?

Based on Eurostat data, the adoption of AI technologies in Poland remains below the EU average. In 2025, 8.4% of Polish enterprises used AI technologies, compared to an EU average of 19.95%. It is worth noting that adoption across the EU is accelerating, having increased by more than 6 percentage points year-on-year, with the figure reaching 55% among large enterprises. Two sectors stand out as clear leaders: the information and communication sector, where 62.5% of enterprises use AI, and professional, scientific and technical activities at 40.4%; across all other sectors, the share remained below 25%, with construction recording the lowest adoption rate at 10.8%.

A separate Polish National Research Institute (NASK) study breaks down GenAI adoption by occupational group, revealing a pattern closely tied to the nature of work. Adoption is highest among knowledge-intensive roles: professionals lead at 45%, followed by managers and senior officials (38%), with clerical support workers (33%) and technicians and associate professionals (31%) also exceeding the 30% threshold. Use falls progressively among more manual or operational roles: elementary occupations (26%), plant and machine operators (23%), service and sales workers (22%), craft and trades workers (21%), and agricultural workers (20%). This occupational gradient is consistent with the sectoral picture emerging from Eurostat data: the sectors recording the highest AI adoption rates, e.g., ICT and professional, scientific, and technical activities, are precisely those in which knowledge-intensive occupations predominate, while sectors such as construction, where manual roles dominate, report the lowest rates of uptake.

18. How is artificial intelligence used in the legal sector, by lawyers and/or in-house counsels? Are AI-driven legal tools widely adopted, and what are the main regulatory concerns?

AI has moved from experiment to everyday tool in Poland's legal market, though adoption is uneven and governance is only now catching up. Three independent surveys, i.e., Wolters Kluwer's AI Trust Index 2026, C.H. Beck's LegalTech Report 2025, and Supesu's Legal Market Report 2025/2026, paint a consistent picture, i.e., headline usage is rising sharply, but it sits alongside persistent knowledge gaps, largely absent internal regulation, and mounting liability concerns.

As to AI adoption, 81% of Polish legal professionals use AI regularly, with 57% doing so daily, and the Supesu survey puts the figure higher still, with 87% of respondents declaring daily use of AI-supported tools, primarily for research, document analysis, and automation of repetitive tasks. However, a significant structural gap persists, i.e., around 35% of law firm lawyers use AI compared to almost 59% of in-house counsel, with in-house lawyers also significantly ahead on AI knowledge (40% positive self-assessment vs. 20% in law firms) and on drafting use (50% vs. 15%).

Use cases are concentrated in support tasks, e.g., translation, contract drafting and analysis, document summaries, and legal research. Many dedicated Polish-law tooling has appeared on the market, and Polish courts are piloting a "digital judge's assistant" for high-volume Swiss franc mortgage litigation. Predicting outcomes before Polish courts or producing unsupervised legal opinions remain widely regarded as unsafe; the civil-law system's thinner structured case-law base means the professional standard is firmly "AI suggests, lawyer decides".

The main barriers to wider use are hallucination risk (32%) and information security concerns (31%). Trust in outputs remains cautious: only 32% consider AI results reliable, while 33% regard it as unreliable. Verification is near-universal, 67% always verify AI-generated answers, but the governance infrastructure lags badly behind: 76% of organizations have not introduced internal AI rules and have no plans to do so, and 45% of AI users rely on free-tier tools that do not guarantee data confidentiality.

AI and LegalTech training is now the second most-attended professional development category in the Polish legal market, and the absence of internal AI policies in most organizations is a material risk; further regulatory intervention cannot be excluded if passivity continues. The prevailing norm across all three surveys is consistent, i.e., AI is mainstream for drafting, research, review, and translation, but full personal responsibility for the output remains with the lawyer.

In the case of attorneys-at-law (radcy prawni), the National Bar of Attorneys-at-Law (KIRP), together with Microsoft and the law firm Sołtysiński Kawecki & Szlęzak, published joint guidance entitled "AI in the Work of a Legal Attorney". The recommendations are detailed and practice-oriented: rather than confining themselves to general principles, they walk the practitioner through the entire lifecycle of AI adoption in a law practice, from the selection of an appropriate tool (including due diligence on the provider, data processing arrangements, and security safeguards), through implementation within the firm's organization and workflows, to day-to-day use, verification of outputs, and ongoing oversight. The guidance is currently being revised to reflect the rapid evolution of technology, which itself illustrates a broader point: professional standards in this area will require continuous updating rather than one-off adoption. As to advocates (adwokaci), the Bar of Advocates (Adwokatura) amended the Code of Advocates' Ethics directly. Under the new provision, the AI tools may only be of a supporting nature and must not lead to a violation of the law, the rules of professional ethics, or the dignity of the profession.

19. What are the 5 key challenges and the 5 key opportunities raised by artificial intelligence for lawyers in your jurisdiction?

Five key challenges

1. **Regulatory complexity:** Lawyers in Poland must navigate an increasingly complex framework combining the AI Act, the GDPR, cybersecurity rules, data governance legislation, sector-specific regulations and traditional liability regimes, often without settled national guidance, as Polish implementing legislation and supervisory structures for the AI Act are still taking shape.
2. **AI governance, risk management, and organizational readiness:** Lawyers are increasingly expected to help clients build governance structures capable of identifying, classifying, and monitoring AI systems throughout their lifecycle, but also use of AI within their organizations. Most Polish organizations are still at an early stage which creates tangible risks, e.g., "shadow AI" deployed by employees without oversight, the unclear allocation of responsibility when AI-driven decisions cause harm, and the inability to manage the risk associated with AI. These gaps are compounded by widespread shortages of AI literacy and technical expertise, both within client organizations and in the legal profession itself. Concentration among a small group of AI providers compounds these risks further. Vendor lock-in, abrupt model deprecation, usage-based pricing volatility, and the possibility of a risk of data transfers outside the EEA all require mitigation, both contractually (exit rights, notice periods, and data-residency commitments) and operationally (fallback procedures and multi-vendor architectures).
3. **Confidentiality and privilege:** The use of AI tools in legal practice raises concerns regarding the disclosure of client information, confidential business data, and communications protected by professional secrecy which, under Polish law, is a strict statutory duty of advocates and attorneys-at-law.
4. **Professional responsibility and over-reliance on AI:** AI-generated output may contain hallucinations, including fabricated case law and legal arguments. Growing reliance on such tools does not shift responsibility away from the lawyer. On the contrary, Polish courts increasingly expect professionals to demonstrate critical verification of AI-assisted work, and uncritical use of AI may amount to a breach of professional standards and ethical duties.
5. **Evolution of client relationships and pricing model:** AI is reshaping the economics of legal practice. As routine tasks are automated, the traditional billable-hour model comes under pressure, accelerating the shift towards value-based, fixed-fee, and subscription arrangements. This may allow outside counsels to reposition themselves from time-sellers to strategic advisers, with client relationships built around outcomes and ongoing counsel rather than hours logged. At the same time, this transformation brings a structural challenge: much of the routine work now being automated has traditionally served

as the training ground for junior lawyers, and firms will need to develop new, deliberate models of mentoring and skills development to prepare the next generation of practitioners. Also, there may be less work for lawyers in general if AI takes over the routine tasks.

Five key opportunities

1. **AI can automate repetitive legal work:** AI tools can help with document review, first drafts, legal research enabling lawyers to focus on strategic advice and complex legal analysis, and allowing smaller Polish firms to handle matters at a scale previously reserved for large practices.
2. **Better access to legal knowledge**: AI legal tools improve access to case law, precedents, templates, know-how, and regulatory materials. This is particularly valuable in Poland where lawyers must track a rapidly evolving body of national and EU legislation alongside extensive administrative and court jurisprudence.
3. **More efficient litigation strategy**: In litigation and arbitration, AI can substantially reduce the time required for reviewing evidence, analyzing documents, and preparing chronologies, leading to lower costs for clients and making complex, document-heavy disputes more manageable. Beyond efficiency, analytics based on large volumes of published case law increasingly allow lawyers to assess the prospects of a claim, identify persuasive lines of argument, and estimate the likely duration of proceedings, supporting a more informed, data-driven litigation strategy.
4. **New legal services and practice areas:** The AI Act – and now its national implementation – has created substantial demand for advisory services relating to AI governance, compliance, procurement, contracting, and risk management, including representation in future proceedings before the new national supervisory authority. AI law is emerging as a distinct practice area for Polish lawyers.
5. **Transformation of legal operations**: AI enables more scalable legal-service delivery models, enhanced contract lifecycle management and better collaboration between legal, compliance, and business teams, allowing both law firms and in-house departments to reposition themselves as strategic partners rather than cost centers.

20. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months? Are there any ongoing initiatives that could reshape AI governance?

The most significant legal developments over the next 12 months will arise from the transition from policy-making to active implementation and enforcement.

First, Poland has completed the parliamentary stage of its national framework for the application of the AI Act. The Polish AI Systems Act, at the time of writing, awaits presidential signature. Once enacted, one of the most significant practical challenges will be the establishment and operationalization of KRiBSI, building its institutional capacity, staffing, procedural frameworks and enforcement practice from the ground up. KRiBSI's early decisions, including its approach to market surveillance, guidance, and first enforcement actions, will set the tone for AI compliance in Poland for years to come.

Second, we expect increasing interaction between AI regulation and other legal fields, particularly data protection, cybersecurity, intellectual property, product liability, and consumer protection. Practical compliance questions are increasingly arising at these intersections, and businesses will need to navigate overlapping regulatory regimes and, potentially, the competing competences of several supervisory authorities.

Third, the debate over digital and AI sovereignty is gaining momentum both at the EU level and in Poland. This trend is no longer purely political: Poland is developing national large language models (the state-backed PLLuM), the community-driven, open-source Bielik, and is investing in domestic computing infrastructure, including two EU-backed AI Factories and a bid for an AI Gigafactory. The sovereignty agenda is closely linked to cybersecurity. In 2026, Poland is set to spend a record amount of over PLN 5 billion on cybersecurity from various sources, reflecting its position as the most cyber-attacked country in the EU. For businesses, these developments carry practical consequences such as growing compliance expectations around data localization and supply-chain security, procurement requirements, or the proposals of rules introducing preferences favoring European or domestic solutions (particularly in the public sector and regulated industries).

Looking ahead, we expect the next wave of challenges to be driven by the growing adoption of agentic AI which puts existing professional standards under considerably greater strain than generative tools used as mere

assistants. The "supporting nature" requirement and the lawyer's personal role become harder to preserve where a system acts autonomously across an entire workflow; verification duties become more demanding where the output is not a single document but a chain of decisions and actions; and questions of attribution and liability arise where an autonomous agent makes an error, exceeds its mandate, or discloses privileged information when interacting with external systems. Similar questions will confront courts, regulators, and clients alike, including whether, and to what extent, tasks performed by AI agents must be disclosed, supervised, and billed. The situation will become more complex with deployment of tools for AI contracting allowing to negotiate, conclude, and assess how AI tools perform contracts.

Contributors

Agata Szeliga
Partner
agata.szeliga@skslegal.pl

Sylwia Macura–Targosz
Senior Counsel
sylwia.macura-targosz@skslegal.pl

Anna Tujakowska
Senior Counsel / Head of Legaltech & Innovation
anna.tujakowska@skslegal.pl

Maciej Gil
Senior Associate
maciej.gil@skslegal.pl

Katarzyna Wnuk
Senior Associate
katarzyna.wnuk@skslegal.pl

Sandra Słowik
Associate
sandra.slowik@skslegal.pl

Michał Kalinowski
Associate
michal.kalinowski@skslegal.pl

