Legal 500
Country Comparative Guides 2025

Poland
TMT

Contributor

Osborne Clarke LLP

Piotr Kaniewski

Counsel | piotr.kaniewski@osborneclarke.com

Kamil Prokopowicz

Associate | kamil.prokopowicz@osborneclarke.com

Olga Cabak

Associate | olga.cabak@osborneclarke.com

Aleksandra Gajda

Junior Associate | aleksandra.gajda@osborneclake.com

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Poland.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Poland: TMT

1. Software – How are proprietary rights in software and associated materials protected?

In Poland, the main legal framework for safeguarding proprietary rights in software and related materials is copyright law. The system is regulated by the Polish Copyright Act, which defines two categories of copyright: moral rights and economic rights.

Moral rights safeguard the personal bond between the author and their work, including attribution rights. These rights are perpetual and inalienable (meaning they cannot be transferred or waived), although it is common practice in commercial contracts for the author to commit not to exercise their moral rights.

Economic rights grant the exclusive right to use the work, effectively covering the entire commercial sphere of the software and associated materials. Unlike moral rights, economic rights are fully transferable and licensable.

Additionally, the Polish Copyright Act recognises rights to derivative works such as translations, adaptations, or other transformations of existing copyrighted works, requiring authorisation from the original creator to transfer rights or otherwise exploit a derivative work.

The protection of a work is granted automatically from the moment of its "fixation", which occurs when the work is manifested in any form that makes it perceptible. No registration or formalities are required.

It is important to note that the Polish Copyright Act follows the idea/expression dichotomy, protecting the expression of a work rather than underlying ideas, procedures, methods, or mathematical concepts. For software, this means copyright protects the specific code written by programmers but not the functions performed or algorithms implemented. However, IT solutions with unique functions, valuable technical information, or business methods may qualify for trade secret protection.

2. Software – In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

Unless otherwise specified in the contract, the default owner of all copyrights in a work is its creator (author).

However, Polish law provides a notable exception to this general rule for works created by employees – unless the employment contract states otherwise, an employer whose employee has produced a work as part of their duties obtains the economic rights to that work upon acceptance, with an exception for software (code). Specifically for software, this transfer is immediate and automatic, and no work acceptance is necessary unless the employment contract indicates otherwise.

It is important to note that, despite the transfer of economic rights, employees retain all moral rights. The employer owns the software commercially but does not become its 'author'. Employees retain attribution rights and other personal authorship rights. However, employment contracts typically include a contractual commitment from employees not to exercise their moral rights.

3. Software – Are there any specific laws that govern the harm / liability caused by Software / computer systems?

There is no specific law in Poland that governs liability or harm caused by software. Instead, liability is determined by several legal acts, including the Polish Civil Code, the Polish Copyright Act, or the Polish Penal Code.

Legal recourse depends on the relationship between the parties involved and the nature of the harm, with a distinction between contractual liability (arising from breach of contractual obligations) and tort liability (arising from unlawful acts).

Contractual liability applies when there is a contract between the software provider and the claimant and is assessed according to contract terms and principles of the Polish Civil Code. Tort liability is relevant in the absence of a contract or if the damage exceeds the scope of the contractual relationship.

Liability claims generally require proving fault (negligence or intent) both for contractual and tort claims. However, parties can modify contractual liability through specific

terms in their agreement.

4. Software – To the extent not covered by (3) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

The Polish Copyright Act governs the legal use of software and prohibits the unauthorized reproduction, distribution, and modification of computer programs. It also provides for civil and criminal liability for copyright infringement.

Furthermore, the Polish Penal Code criminalises specific forms of software use (and misuse). These include crimes such as hacking (unauthorised access to a system), data interference (destroying, altering, or deleting data without authorisation), system interference (disrupting the functioning of a computer system) or computer fraud.

Additionally, the AI Act regulates the deployment and use of AI systems, establishing prohibited uses and compliance obligations for high-risk AI applications.

5. Software Transactions (Licence and SaaS) – Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

In Poland, there is no single, comprehensive law specifically regulating software or cloud technology transactions. The provision of software is covered by interconnected legal frameworks, with specific obligations depending on the type of software and the cooperation model between a software vendor and the customer.

Relevant legal areas include copyright law, consumer protection, data protection/governance, outsourcing regulations and underlying principles of contract law. An important aspect, particularly for cloud technologies, involves data transfers outside the European Economic Area.

Moreover, European Union legislation directly influences software transactions through several key regulations. The Digital Services Act (DSA), Digital Markets Act (DMA), and Data Act introduce new rules for digital service providers and large online platforms, which may apply to specific software vendors and cloud providers.

The Data Act is especially important for cloud technology as it tackles vendor lock-in issues. The AI Act complements these rules by setting detailed requirements for AI solutions providers, with stricter duties for high-risk AI.

6. Software Transactions (License and SaaS) – Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

Liability caps are a common industry practice. The specific cap amount is open to negotiation, usually between 100-200% of the contract value. However, some sectors face regulatory restrictions that prevent the limitation of liability (including caps), with the banking sector being a notable example.

7. Software Transactions (License and SaaS) – Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

1. **Confidentiality breaches.** Liability for a breach of confidentiality is typically excluded from liability caps and subject to contractual penalties.
2. **IPR infringement claims. Liability for intellectual property rights infringement is usually unlimited or subject to a very high cap. It is a common market practice for vendors to offer a comprehensive indemnity covering legal defence costs, damages, and settlement amounts.**
3. **Data protection breaches; data security breaches (including loss of data); breaches of applicable law; regulatory fines.** Certain entities (e.g. the insurance sector) will typically demand unlimited liability due to sector-specific regulations, while other entities may accept substantially enhanced caps. The approach varies based on the customer's industry and risk profile.
4. **Wilful or deliberate breaches.** Under the Polish Civil Code, liability for wilful misconduct cannot be limited

and any contractual provision attempting to exclude or limit such liability is void. It is a standard market practice to extend unlimited liability to also cover gross negligence.

8. Software Transactions (License and SaaS) – Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

Source code escrow is used solely for business-critical, custom-built systems where operational disruption could severely impact the business. This approach is usually taken when there are concerns about vendor stability or continuity, especially with smaller suppliers that lack an established market presence or financial robustness.

Escrow arrangements involve depositing source code with independent third parties, including notarial services or dedicated escrow providers. No equivalent service is available for cloud-based software.

9. Software Transactions (License and SaaS) – Are there any export controls that apply to software transactions?

Following the invasion of Ukraine in February 2022, the European Union introduced sanctions against the Russian Federation, including export controls. The core of these measures is Council Regulation (EU) No 833/2014, which has been substantially amended through successive sanctions packages. The regulations prohibit the sale, supply, transfer, or export of specific categories of software to any person or entity in the Russian Federation or for use within Russia.

10. IT Outsourcing – Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

In Poland, public law requirements regarding IT outsourcing are spread across various acts that comprehensively regulate the activities of specific types of entities. The most rigorous outsourcing requirements must be met by entities in the financial sector, such as banks, payment institutions, insurance and reinsurance companies, or investment firms.

Due to the above, when entering into specific transactions, it is necessary to thoroughly familiarise oneself with the requirements imposed on the given entity when it wants to transfer part of its IT operations externally. Market supervisory authorities may additionally develop the statutory requirements through various types of instructions and guidelines.

Moreover, requirements regarding outsourcing, understood broadly as the use of IT services, may be subject to cybersecurity regulations. The most significant source of law at the EU level, which affects numerous sectors, is Directive 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2).

11. IT Outsourcing – Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

In Poland, certain instances of outsourcing may be regarded as a transfer of an employment establishment or part of it to another employer, according to the provisions of the Labour Code Act of 26 June 1974.

According to judicial rulings, such a situation occurs when the transferred set of enterprise components, whether tangible, intangible, or mixed, can be regarded as an independent employment unit which, after the transfer, retains its identity and continues its activities.

If outsourcing meets the criteria for transferring an employment establishment to another employer, the new employer will, by law, become a party to the existing employment relationship, and the employee will acquire special rights to terminate the contract.

12. Telecommunications – Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

In Poland, the principal laws regulating the telecommunications market are the Electronic Communications Act as of 12 July 2024.

The provisions of the Electronic Communications Act are comprehensive, covering principles for conducting

business by telecommunications entrepreneurs, supervision regulations, telecommunications fee payments, consumer rights, and more. Key groups affected by the Electronic Communications Act include not only traditional telecommunications service providers but also providers of online text and audiovisual communication services.

The shape of the Electronic Communications Law is closely dependent on EU law, implementing the provisions of Directive 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code, as well as Directive 2022/2380 of 23 November 2022 amending Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment.

13. Telecommunications – Please summarise any licensing or authorisation requirements applicable to the provision or receipt of telecommunications services in your country. Please include a brief overview of the relevant licensing or authorisation regime in your response.

In Poland, conducting telecommunications activities can be carried out provided that an entry is obtained in a special register of telecommunications entrepreneurs. The public authority responsible for maintaining this register is the President of the Polish Office of Electronic Communications. The entry is made upon the request of the interested entity and is completed within 3 days from the date of submission of the application (provided it does not contain formal deficiencies).

14. Telecommunications – Please summarise the principal laws (present or impending) that govern access to communications data by law enforcement agencies, government bodies, and related organisations. In your response, please outline the scope of these laws, including the types of data that can typically be requested, how these laws are applied in practice (e.g., whether requests are confidential, subject to challenge, etc.), and any legal or procedural safeguards that apply.

In Poland, the principal laws governing access to communications data by law enforcement bodies are the Electronic Communications Act, as of 12 July 2024.

In accordance with the provisions of the Electronic Communications , a telecommunications entrepreneur is obliged to ensure the technical and organisational conditions for access and recording of electronic communications and data by entities indicated in court or prosecutor's orders. The rules for issuing such orders are strictly regulated by the provisions of the Act of 6 June 1997 – Code of Criminal Procedure.

Based on a specific example, under the provisions of the Polish Code of Criminal Procedure, the court, upon the prosecutor's request, may order the monitoring and recording of the content of telephone conversations. The telecommunications entrepreneur must comply with the order by providing the appropriate tools for monitoring and recording such conversations, without the possibility of challenging it.

15. Mobile communications and connected technologies – What are the principle standard setting organisations (SSOs) governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

In Poland, no single entity exclusively defines standards for mobile communications and connected technologies. Key authorities include:

Ministry of Digital Affairs – field of “new technologies”.

Ministry of Infrastructure – traffic regulations.

President of Office of Electronic Communications – electronic communication.

President of the Personal Data Protection Office – matters concerning the processing of personal data.

Polish Committee for Standardization – applicable standards in Poland.

Supreme Medical Chamber – ethical guidelines applicable to medical practitioners.

Additional authorities may be relevant for specific Internet of Things products or services, depending on their particular characteristics.

16. Mobile communications and connected technologies – How do technical standards

facilitating interoperability between connected devices impact the development of connected technologies?

Polish technical standards have limited direct impact on connected technology development, focusing mainly on regulatory compliance rather than broad interoperability.

Notably, the Ministry of Infrastructure is developing national autonomous vehicle legislation (still in process) due to the absence of EU provisions, as current law only permits autonomous vehicles during testing.

17. Data Protection – Please summarise the principal laws (present or impending), if any, that govern data protection, including a brief explanation of the general purpose of those laws.

In addition to the GDPR, the protection of personal data in Poland is regulated by the Act of 10 May 2018 on the Protection of Personal Data and the act transposing the LED directive. There are also various sectoral regulations on data protection.

Furthermore, databases are protected by law under certain conditions, regardless of the nature of the data. Copyright protects data that constitutes works or parts thereof, including software, while trade secrets protect data of economic value to businesses. Ideas and algorithms, which are not covered by copyright, may qualify for protection as trade secrets.

18. Data Protection – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

Polish supervisory authority can impose fines of up to the maximum amount set out in the GDPR. Certain data processing violations are also subject to criminal sanctions under Polish law.

19. Data Protection – Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

Polish technology contracts typically include GDPR compliance clauses and data processing agreements, if needed. References to other non-EU regulations only appear in specific circumstances, such as when foreign entities or cross-border processing are involved, or when parties specifically require compliance in this regard. This is not common.

20. Cybersecurity – Please summarise the principal laws (present or impending), if any, that govern cybersecurity (to the extent they differ from those governing data protection), including a brief explanation of the general purpose of those laws.

In Poland, the principal laws regulating cybersecurity issues are the Act of 5 July 2018 on the National Cybersecurity System (“**UKSC**“).

Currently, government work is underway to adopt a final draft amendment to the UKSC to implement the provisions of the new Directive 2022/2555 of 14 December 2022 on measures for a high standard level of security of network and information systems across the Union (“**NIS2**“). NIS2 aims to further strengthen the level of digital security in the EU by imposing specific cybersecurity obligations on entities meeting sectoral and size criteria.

In addition, specific cybersecurity provisions apply to financial market participants under the EU Regulation 2022/2554 on digital operational resilience for the financial sector (“**DORA**“). The act implementing selected provisions of DORA is currently undergoing legislative debate in the Polish Parliament.

21. Cybersecurity – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable cybersecurity laws?

According to the most recent draft amendment to the Act of 5 July 2018 on the National Cybersecurity System, the amount of the financial penalty imposed on an essential entity cannot exceed the equivalent of EUR 10,000,000 expressed in Polish zloty or 2% of the revenues generated in the previous financial year. For important entities, the maximum penalties are PLN 7,000,000 or 1.4% of annual revenues, respectively.

On the other hand, according to the latest regulations implementing the provisions of DORA in Poland, a financial institution may face a penalty of PLN 2,170,650 or the equivalent of 0.5% of total annual revenue. Additionally, penalties may be imposed on individuals

responsible for the violations.

22. Artificial Intelligence – Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

Currently, there is no dedicated body responsible for the regulation of artificial intelligence in Poland.

Poland is in the process of establishing national supervisory bodies to implement the EU AI Act, with ongoing legislative work. The proposed Polish Act on AI Systems designates the Commission for the Development and Safety of Artificial Intelligence (KRiBSI) as the central authority responsible for market supervision.

23. Artificial Intelligence – Please summarise the principal laws (present or impending), if any, that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

The most significant legal framework is the AI Act, which will be directly enforced in Poland. Its purpose is to provide a legal framework for artificial intelligence, ensuring that AI systems are safe, transparent, non-discriminatory, and respect fundamental rights. The regulation's central pillar is a risk-based approach that tailors regulatory intensity to the level of potential harm an AI system could cause and the specific role of the entity involved, such as provider, deployer, or importer of an AI system.

The fundamental purpose of the proposed Polish Act on AI Systems is to ensure the proper application and enforcement of the AI Act in Poland.

24. Artificial Intelligence – Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI (including agentic AI)?

While Polish law does not yet have specific provisions for LLMs or generative AI, the AI Act contains provisions governing such technology. AI Act regulation covers 'general-purpose AI models' ('**GPAI models**') and 'general-purpose AI Systems' (AI systems based on general-purpose AI models).

The GPAI model is defined as an AI model trained with a large amount of data, which displays significant generality and is capable of competently performing a wide range of distinct tasks. The AI Act recitals suggest that models with over a billion parameters are likely to be considered GPAI models.

GPAI models are subject to specific obligations to ensure risk management and comprehensive transparency. These include extensive documentation, systematic risk assessment protocols, and mandatory incident reporting mechanisms. Furthermore, AI systems incorporating GPAI models must comply with transparency requirements (e.g. labelling AI-generated content).

25. Artificial Intelligence – Do technology contracts in your jurisdiction typically contain either mandatory (e.g. mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

Currently, in Poland, there are no mandatory statutory provisions that require technology contracts to include specific clauses addressing AI risk. However, it is becoming a recommended best practice to address such risks contractually due to the legal ambiguities surrounding AI and extensive obligations arising from the AI Act.

The primary issues and risks that should be addressed through contractual provisions encompass intellectual property protection and ownership of AI-generated outputs, data protection and GDPR compliance, cybersecurity and liability allocation.

Most significantly, contracts should establish clear performance standards to ensure compliance with AI Act requirements, including provisions for algorithm transparency, bias mitigation, ongoing monitoring, and prohibited AI practices. Given that administrative fines under the AI Act can reach up to EUR 35 million or 7% of a company's global annual turnover, this is crucial.

26. Artificial Intelligence – Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

In Poland, technology contracts involving AI are

increasingly including provisions regarding intellectual property rights and the ownership of outputs. The legal complexity arises from the current uncertainty regarding copyright protection of AI-generated outputs.

Given the absence of a definitive legal solution on AI-generated content ownership, well-drafted contractual terms become essential for providing legal certainty and adequate risk allocation between contracting parties.

27. Blockchain – What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

In Poland, blockchain technology and the crypto-assets market are regulated through EU legislative initiatives, such as Regulation 2022/858 of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology ("**DLTR**"), as well as Regulation 2023/1114 of 31 May 2023 on markets in crypto-assets ("**MiCAR**").

The provisions of DLTR mainly facilitate the dematerialisation and trading of financial instruments on blockchain infrastructure. MiCAR, by contrast, is a regulation that governs the issuance and trading of specific groups of crypto-assets, as well as the provision of crypto-asset services by providers holding special authorisations (CASPs).

The DLTR was introduced in Poland through the Act of 16 August 2023, amending certain laws to promote the development of the financial market and safeguard investors. On 26 June 2025, the draft Act on the crypto-assets market, which incorporates the provisions of MiCAR, was submitted to Parliament and is awaiting further legislative action.

28. Search Engines and Marketplaces – Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

Search engines and marketplaces are primarily governed by EU regulations, with national law limited to alignment and transposition.

Digital Services Act (DSA) – applies to online intermediaries including search engines, marketplaces, social networks, and content-sharing platforms.

Digital Markets Act (DMA) – targets "gatekeepers"—large online platforms with a significant impact on the internal market (including search engines and marketplaces).

European Accessibility Act (EEA) – ensures equal access for people with disabilities to digital tools and platforms.

Artificial Intelligence Act (AIA) – comprehensive regulation for safe, transparent AI use across the EU, including in search engines and marketplaces.

GDPR also applies, establishing general principles for personal data processing.

29. Social Media – Please summarise the principal laws (present or impending), if any, that govern social media and online platforms, including a brief explanation of the general purpose of those laws?

Social media is governed by the same EU regulations as search engines and marketplaces, with the DSA and DMA requiring special emphasis due to their direct focus on social media and online platforms.

30. Social Media – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable online safety laws?

DSA sanctions for social media providers may reach 6% of annual worldwide turnover.

DMA sanctions for gatekeepers may reach 10% of annual worldwide turnover.

AIA sanctions for violations of harmful AI practice bans face fines up to EUR 35 million or 7% of annual worldwide turnover (whichever is higher).

31. Spatial Computing – Please summarise the principal laws (present or impending), if any, that govern spatial computing, including a brief explanation of the general purpose of those laws?

Currently, no Polish or EU regulations specifically address spatial computing, VR, AR, or the metaverse. These technologies are governed by broader regulations, primarily GDPR and copyright law.

32. Quantum Computing – Please summarise the principal laws (present or impending), if any, that govern quantum computing and/or issues around quantum cryptography, including a brief explanation of the general purpose of those laws?

Currently, no separate Polish or EU legislation exists for quantum computing. The European Commission recently unveiled a quantum technologies strategy, signalling a "Quantum Act" project for 2026.

33. Datacentres – Does your jurisdiction have any specific regulations that apply to data centres?

Both at the EU and national levels, there is no single comprehensive source of law dedicated to data centres, and the applicable regulations are dispersed. Most regulations are not specific to data centres due to the relatively innovative nature of this business activity.

Specific references to data centres can be found in the EU Directive 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, known as NIS2 (still in the implementation stage in Poland).

Additionally, at the EU level, there is also Directive 2023/1791 of 13 September 2023 on energy efficiency, which imposes certain reporting obligations on selected data centres. The publication of the draft act implementing the provisions of this directive in Poland is planned for the third quarter of 2025.

34. General – What are your top 3 predictions for significant developments in technology law in the next 3 years?

Firstly, the development of technology law in Poland will continue to depend on the most critical legislative initiatives created at the EU level in the coming years. Despite widely signalled deregulatory sentiments, the amount and complexity of regulations will continue to increase.

Secondly, the main regulatory and supervisory focus will be on regulations concerning artificial intelligence, autonomous machines, decentralised information processing, and digital resilience. The GDPR is of particular note, as its relevance has increased significantly with the introduction of the AI Act.
Thirdly, technological legislative initiatives will encounter increasingly complex and lengthy legislative processes due to their specific links with social issues, the interests of large tech corporations, and geopolitical tensions. Consequently, stakeholders will need to prepare for more intricate negotiations.

35. General – Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

Implementing provisions to address sustainability / net-zero obligations or similar environmental commitments in technology contracts is still not common in Poland. This is primarily due to the lack of a clear legal requirement to include such provisions. However, it is suspected that including provisions referring to ESG issues may become more frequent in the future, with the increasing number of companies wanting to be perceived as environmentally responsible.

Contributors

Piotr Kaniewski
Counsel
piotr.kaniewski@osborneclarke.com

Kamil Prokopowicz
Associate
kamil.prokopowicz@osborneclarke.com

Olga Cabak
Associate
olga.cabak@osborneclarke.com

Aleksandra Gajda
Junior Associate
aleksandra.gajda@osborneclake.com