Legal 500
Country Comparative Guides 2026

Poland

Technology Outsourcing

Contributor

APLaw Artur Piechocki

Artur Piechocki

Radca prawny / Attorney-at-law / Founder | artur.piechocki@aplaw.pl

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

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

Poland: Technology Outsourcing

1. Market overview: Please provide a high-level overview of the outsourcing market in your jurisdiction (e.g. who are the key players and in what sectors (public and private) are you seeing outsourcing services being adopted)?

Based on our observations, outsourcing in Poland is most visible at two opposite ends of the market. On the one hand, it is commonly used by large enterprises, including state-owned or state-controlled companies, whose internal legal, compliance, IT or procurement departments often need external support due to the lack of highly specialised in-house expertise in particular areas.

On the other hand, outsourcing is also used by small businesses which do not have sufficient internal resources to handle specialised legal, IT, cybersecurity, HR, accounting or regulatory matters internally. In this segment, however, the use of outsourcing is often dependent on available budget and tends to be more ad hoc or project-based rather than continuous.

Medium-sized companies frequently rely more heavily on their own internal resources and are often more selective in outsourcing, usually engaging external advisers or service providers only for more specialised, high-risk or cross-border matters. Overall, outsourcing is particularly relevant in IT, cloud services, cybersecurity, compliance, data protection, finance, HR, payroll and specialised legal or regulatory support.

2. Procurement: Are there specific procurement-related laws or regulations governing outsourcing by public sector or government bodies?

Outsourcing by public sector and government bodies in Poland is generally governed by the Polish Public Procurement Law. This regime applies to public contracting authorities and, in certain cases, sectoral contracting entities, and regulates the procedure for awarding contracts for services, supplies and works, including outsourcing arrangements.

The public procurement system also includes a specialised review mechanism before the National Appeals Chamber (Krajowa Izba Odwoławcza, KIO).

Contractors may challenge certain actions or omissions of the contracting authority during the procurement procedure before the KIO.

Decisions of the KIO may be further challenged before the competent court. As a result, public sector outsourcing in Poland is subject not only to formal procurement rules, but also to a structured system of legal remedies and judicial review.

3. Procurement: Are there specific procurement-related laws or regulations governing outsourcing by private sector organisations?

As a rule, private sector organisations in Poland are not subject to specific public procurement rules when outsourcing services, unless particular sector-specific or funding-related requirements apply.

In practice, however, larger private entities often have their own internal procurement policies, including group-wide purchasing rules, vendor onboarding procedures, approval thresholds, competitive tender requirements, compliance checks and rules on conflicts of interest. These internal procedures may significantly affect the timing and structure of outsourcing projects, even though they do not generally result from mandatory Polish procurement law.

Entities with a mixed public-private character, or companies with state ownership or public-sector links, may also apply procedures similar to those under the Polish Public Procurement Law, even where the statutory regime does not strictly apply. This is often done for transparency, auditability, internal governance or public accountability reasons.

4. Laws and Regulations: Are there any other specific laws or regulations that apply to outsourcing? If not, what key general laws and regulations are most relevant?

There is no single Polish act regulating outsourcing as such. The applicable legal framework depends mainly on the sector, the type of outsourced services and the nature of the data, technology or infrastructure involved.

In regulated sectors, specific outsourcing requirements may apply, for example in banking, insurance, payment services, investment services, telecommunications, energy, healthcare, public sector, defence and critical infrastructure. These rules may concern regulatory approvals or notifications, access and audit rights, subcontracting, business continuity, cybersecurity, incident reporting, data location, exit plans and supervisory authority access to outsourced functions.

For IT, cloud and cybersecurity outsourcing, key regulations may include the GDPR, the Polish Data Protection Act, the Act on the National Cybersecurity System, the NIS2 framework implemented into Polish law, DORA for financial entities, the Data Act, Electronic Communication Law and, where relevant, export control, dual-use and defence-related licensing rules.

Where no sector-specific regime applies, outsourcing contracts are mainly governed by general laws, including the Polish Civil Code, copyright and industrial property law, unfair competition and trade secret rules, labour law, tax law, data protection law and general corporate governance rules. In practice, the contract remains the key instrument for allocating operational, financial, compliance and legal risks.

5. Laws and Regulations: Do any specific regimes apply to outsourcing arrangements in particular sectors (e.g. financial services)?

Please see above.

6. Competition law: To what extent might outsourcing arrangements require notification or approval under merger control rules?

Please see below.

7. Competition law: To what extent are the terms of outsourcing agreements the subject of restrictions under competition law?

Outsourcing agreements are not subject to specific competition law restrictions as such. However, their terms must comply with general EU and Polish competition rules, in particular the prohibitions on anti-competitive agreements, abuse of dominance and unlawful information exchange.

In practice, competition law issues may arise where outsourcing arrangements include exclusivity, long-term lock-in, non-compete obligations, restrictions on customers or suppliers, pricing coordination, market-sharing elements or access to competitively sensitive information.

8. Intellectual property ('IP') rights: What IP (registrable and non-registrable) is typically created in the course of an outsourcing arrangement?

Polish law does not provide for a general registration system for "IP rights" as such. Registration is available mainly for industrial property rights, such as trade marks, patents, utility models, industrial designs and geographical indications, which are protected under the Polish Industrial Property Law.

By contrast, copyright protection does not require registration. Works, including software, documentation, databases or other creative materials, are protected under the Polish Act on Copyright and Related Rights from the moment they are established in any form, provided that they are individual and creative in nature.

In outsourcing arrangements, it is therefore important to regulate IP ownership and licensing expressly in the contract, particularly as regards newly created deliverables, software, documentation, source code, modifications, pre-existing materials, open-source components and the transfer or licensing of economic copyrights. Confidential information and know-how should additionally be protected through contractual confidentiality obligations and, where applicable, trade secret rules.

9. Intellectual property ('IP') rights: In an outsourcing arrangement, would any contractual terms or formal steps be required to vest supplier-created IP in the customer?

In Polish outsourcing arrangements, IP rights are usually addressed through either a licence or an assignment of rights. The contract should clearly specify whether the customer only obtains the right to use the relevant deliverables, software, documentation or materials, or whether the economic copyrights are transferred to the customer.

The contract should expressly identify the fields of exploitation covered by the transfer (or right to use). In case of transfer, economic copyrights are transferred only within the fields of exploitation specified in the agreement. This is especially relevant for software,

source code, documentation, databases, graphics, websites, marketing materials and other deliverables created under an outsourcing arrangement.

The contract should also regulate the moment of transfer of rights, for example whether rights pass upon creation, acceptance of the deliverable, payment of remuneration or another agreed milestone. From a customer's perspective, linking the transfer to acceptance and/or payment is common, while suppliers often seek to retain rights until full payment.

If a licence model is used instead of an assignment, the agreement should define whether the licence is exclusive or non-exclusive, territorial scope, duration, permitted users, sublicensing, modification rights, use within the customer's group, use by subcontractors and exit or transition rights.

In both models, the contract should also deal with pre-existing materials, third-party components, open-source software, moral rights, source code access and post-termination use.

10. Intellectual property ('IP') rights: How are confidential information, know-how and trade secrets protected in your jurisdiction?

Polish law does not provide a separate, self-standing proprietary right in confidential information or know-how comparable to registered industrial property rights. In practice, such information is protected primarily through contractual arrangements, including NDAs, confidentiality clauses, access restrictions, non-use obligations, audit rights and post-termination obligations.

In addition, confidential business information may be protected as a trade secret under the Polish Act on Combating Unfair Competition, provided that the information has commercial value, is not generally known or easily accessible, and the holder has taken reasonable steps to keep it confidential. Unlawful acquisition, disclosure or use of trade secrets may give rise to civil liability, including injunctions, damages, surrender of unlawfully obtained benefits and other remedies.

Therefore, in outsourcing arrangements, protection of know-how and confidential information should be addressed expressly in the contract, including the scope of protected information, permitted disclosures, subcontractor access, security measures and consequences of breach.

11. Data: What is the regime in your jurisdiction for regulating the protection and processing of personal data and what are the main implications for outsourcing arrangements?

The Polish data protection legal services market is entering a more mature and risk-oriented phase. Clients no longer look only for formal GDPR documentation or one-off compliance checks, but increasingly expect strategic advice on accountability, risk management, data governance, cybersecurity and the use of new technologies, including artificial intelligence. This reflects a broader change in the way organisations understand data protection: not as a purely legal or administrative obligation, but as an element of operational resilience, trust, compliance and business continuity.

A particularly important market trend concerns the clarification of the role of the Data Protection Officer. Organisations are increasingly aware that the DPO should remain as independent as possible from the controller and should not be treated as an outsourced compliance department or as a substitute for the controller's own responsibilities. In practice, this means that the DPO should advise, monitor, inform and provide recommendations, but should not take over operational tasks such as making breach notifications on behalf of the controller, maintaining the controller's record of processing activities, deciding on legal bases for processing, approving risk decisions or implementing security measures. These responsibilities remain with the controller. This distinction is becoming increasingly important in advisory work, internal governance models and outsourcing arrangements.

At the same time, controllers are becoming more aware of the importance of risk analysis and its role in the proper functioning of an organisation. GDPR risk assessments, DPIAs, legitimate interest assessments, vendor risk reviews and breach impact assessments are now increasingly linked with broader enterprise risk management, cybersecurity governance and AI governance. This is particularly visible where organisations deploy AI tools, marketing technologies, profiling mechanisms, cloud services, automation or complex data-sharing models. As a result, privacy advice is increasingly interdisciplinary and must take into account not only GDPR, but also cybersecurity regulations, NIS2/KSC requirements, AI Act obligations and sector-specific compliance frameworks.

The enforcement priorities announced by the Polish Data Protection Authority also have a significant impact on market demand. In its sectoral inspection plan for 2026,

the UODO indicated, among other areas, marketing entities, in particular with respect to the legal bases for the processing of personal data for marketing purposes. The plan also covers, among others, entities processing data in large-scale EU systems, healthcare entities using video surveillance, entities operating Public Information Bulletins and online delivery platforms.

This regulatory focus is likely to increase demand for legal advice on marketing databases, consent mechanisms, legitimate interest assessments, profiling, lead generation, cooperation with agencies, call centres, marketing automation providers and online platforms. It also strengthens the need for practical audits of data flows, evidence of consent, information obligations, processor arrangements and accountability documentation.

Overall, the Polish privacy market is moving from formal GDPR compliance towards a more sophisticated model of data, technology and risk governance. This creates significant opportunities for specialised law firms capable of combining legal expertise with practical understanding of technology, cybersecurity, AI, marketing models and organisational risk. It also raises client expectations: legal advice must be not only technically correct, but also operationally useful, defensible before regulators and aligned with the organisation's broader compliance and business strategy.

12. Data: What is the regime in your jurisdiction for regulating the processing of non-personal data and what are the main implications for outsourcing arrangements?

Polish law does not provide for a single, comprehensive regime equivalent to the GDPR for the processing of non-personal data. In practice, non-personal data is regulated through a combination of EU law, sector-specific regulation, contractual arrangements and general Polish rules on confidentiality, trade secrets, intellectual property and unfair competition. At EU level, the key instruments are the Data Act and the Regulation on the free flow of non-personal data.

The Data Act, applicable in most respects from 12 September 2025, is particularly important for outsourcing, cloud, SaaS, IoT and data-driven services. It regulates access to and use of data generated by connected products and related services, introduces rules on B2B and B2G data sharing, and contains important cloud-switching and interoperability obligations for providers of data processing services. This may affect contract terms on data access, portability, exit assistance, migration, switching fees, technical interoperability, metadata and vendor lock-in.

In Poland, there are also several "local" legal regimes which may apply to non-personal data depending on its nature. Business, technical, commercial or operational data may be protected as a trade secret under the Polish Act on Combating Unfair Competition. Databases may benefit from copyright protection or sui generis database protection. Sector-specific confidentiality obligations may also apply, for example in banking, insurance, telecommunications, public procurement, energy, healthcare, defence or regulated infrastructure. Cybersecurity legislation, including the Polish Act on the National Cybersecurity System and sectoral rules such as DORA in the financial sector, may impose security, incident-reporting, audit and outsourcing-control obligations even where the relevant data is not personal data.

For outsourcing arrangements, the main implications are that contracts should clearly regulate ownership and permitted use of non-personal data, access rights, confidentiality, trade secret protection, database rights, audit rights, security standards, subcontracting, data localisation, cloud migration, exit assistance, interoperability and return or deletion of data.

13. Cyber: Does your jurisdiction have specific cybersecurity legislation or regulations and what are the main implications for outsourcing arrangements?

The Polish legal services market is currently undergoing a phase of strong specialisation and structural change. Clients, including public entities and companies with State Treasury participation, are increasingly looking for advisers specialised in specific regulatory areas, rather than only for law firms providing broad general legal support. The strongest increase in demand is visible in the areas of personal data protection, new technologies, cybersecurity, compliance, IT contracts and EU regulatory frameworks.

Since the turn of 2024/2025, following political and institutional changes in Poland, there has also been a significant shift in the way legal services are procured by a broader group of state-related entities — both strictly public institutions and companies with State Treasury participation. This part of the market has become more open to specialised law firms which previously did not always have access to such clients. This applies not only to formal procurement procedures, but also to requests for proposals, implementation projects, audits and expert

advisory work.

The implementation of NIS2 and the amendment to the Polish Act on the National Cybersecurity System are having a particularly important impact on the market. The new rules expand the scope of obliged entities, introduce the categories of essential and important entities, and impose obligations relating to cybersecurity risk management, incident reporting, implementation of technical and organisational measures, and management accountability.

As a result, an increasing number of public, infrastructure and regulated entities require not only traditional legal support, but comprehensive advisory services combining law, technology, compliance and risk management. Broader access for specialised law firms to the provision of services to entities covered by NIS2/National Cybersecurity System requirements represents a significant change in the Polish legal outsourcing market. It creates new opportunities for law firms with practical experience in data protection, cybersecurity, new technologies and sector-specific regulations, while at the same time raising client expectations regarding the quality, specialisation and interdisciplinary nature of legal advice.

14. Technologies: To what extent are certain technologies commonly used in outsourcing arrangements (e.g. artificial intelligence, robotic process automation, cloud computing and blockchain/distributed ledger technologies) the subject of specific regulations?

The Polish AI legal services market is still at an early stage of development. Although AI Act awareness is growing quickly, practical implementation projects remain relatively limited. Most organisations in Poland are not yet deploying their own high-risk AI systems at scale. Instead, they mainly rely on general-purpose AI tools, especially LLM-based solutions such as chatbots, assistants, document automation tools, translation tools and embedded AI functionalities in existing software.

As a result, current legal support in AI is still focused primarily on governance, internal policies, risk mapping, acceptable-use rules, vendor assessment, data protection, confidentiality, IP issues and employee guidance. Full AI Act implementation projects concerning high-risk AI systems are still relatively rare and mainly concern larger organisations, regulated entities, financial institutions, HR technology providers, healthcare, infrastructure, public sector bodies and companies developing or integrating AI into core business processes.

This means that the Polish AI legal market is currently divided into two segments. The first and broader segment concerns the practical use of GPAI and LLM tools by ordinary organisations, where the key issues are compliance, data protection, cybersecurity, trade secrets, procurement and responsible use. The second, narrower segment concerns providers, deployers and importers of high-risk AI systems, where advice is more technical and regulatory, including classification, conformity assessment, documentation, risk management, human oversight, data governance and post-market monitoring.

In Poland, the AI Act will also be supported by national legislation. The Polish act related to the artificial intelligence systems will be particularly relevant from a compliance and regulatory perspective. It is expected to establish the national supervisory framework, procedures, institutional responsibilities and enforcement mechanisms necessary for the practical application of the AI Act in Poland.

Overall, demand for AI-related legal advice in Poland is growing, but it is still more focused on preparedness, governance and risk management than on full-scale high-risk AI compliance. The market is likely to develop significantly as organisations move from experimental use of GPAI and LLM tools towards more structured AI deployment, and as the Polish supervisory and enforcement framework under the Act on Artificial Intelligence Systems becomes operational.

15. Employment law: Do your jurisdiction's employment laws and regulations have specific implications for outsourcing arrangements?

Polish employment law may be relevant to outsourcing arrangements, particularly where the outsourcing involves taking over an existing function, team, assets or organised part of the customer's business. This is especially important in IT outsourcing, for example where an internal IT helpdesk, software development team, infrastructure team or cybersecurity function is moved to an external provider.

If the arrangement qualifies as a transfer of an undertaking or part of an undertaking, Article 23¹ of the Polish Labour Code applies. In such case, the new employer becomes, by operation of law, a party to the existing employment relationships with the transferred employees. The transfer itself is not a valid reason for termination of employment.

Whether an outsourcing, insourcing or change of IT service provider triggers such transfer rules must be assessed case by case. The key issue is whether there is a transfer of an organised economic entity or function which retains its identity, rather than a mere purchase of services. Relevant factors may include the transfer of staff, assets, know-how, management, tools, infrastructure, customer-specific processes and continuity of the outsourced activity.

Where Article 23¹ applies, employees transfer automatically to the new employer and there is no need to sign new employment contracts. The current and new employer must also comply with applicable information and consultation obligations towards employees or trade unions, and the employees may terminate their employment within the statutory period if they do not wish to continue with the new employer. In IT outsourcing contracts, these issues should be addressed through detailed employee-transfer, cooperation, liability, information, transition and exit provisions.

16. Employment law: How are employees transferred under an outsourcing arrangement?

Please see above.

17. Cross-border: Do cross-border or multi-jurisdictional outsourcing arrangements raise any specific challenges or concerns in your jurisdiction (e.g. relating to export control or data transfer laws)?

Cross-border and multi-jurisdictional outsourcing arrangements may raise several Poland-specific and EU-law issues, particularly where the outsourced services involve personal data, regulated sectors, cybersecurity-sensitive infrastructure or technology with a potential military or dual-use application.

From a data protection perspective, transfers of personal data outside the EEA must comply with the GDPR transfer regime, including adequacy decisions, Standard Contractual Clauses, transfer impact assessments and, where necessary, supplementary measures. This is particularly relevant for cloud, SaaS, IT support, remote access, helpdesk, cybersecurity monitoring and software development arrangements involving non-EEA service providers or group companies. The European Commission's SCCs and the EDPB recommendations on supplementary measures remain the key reference points for such transfers.

Export control issues may also be relevant. Under EU Regulation 2021/821, dual-use items include not only physical goods, but also software and technology which may have both civil and military applications. The EU dual-use regime controls exports, brokering, technical assistance, transit and transfers of dual-use items. This may capture certain IT outsourcing arrangements.

In Poland, trade in dual-use products may require an authorization depending on the nature of the technology, recipient, destination and end-use.

Additional licensing requirements may arise where the outsourcing concerns products, software or technology intended for military or police use. In such cases, a Polish concession for “special trade” may be required, covering the manufacture of and trade in explosives, weapons, ammunition and products or technologies intended for military or police purposes. This may be relevant not only to traditional defence products, but also to certain IT systems, software, technical assistance or integration services supplied to defence-sector customers, depending on classification and use.

18. Liability: Are there limits on what liabilities can be contractually excluded in your jurisdiction (e.g. are there certain liabilities which cannot be limited or excluded by law)?

Under Polish law, contractual liability may generally be limited or excluded, subject to the principle of freedom of contract and its statutory limits. In B2B contracts, parties may therefore agree caps on liability, exclusions of indirect or consequential losses, liquidated damages, sole-remedy clauses or other contractual risk allocation mechanisms. This freedom is limited where the exclusion would be contrary to mandatory law, the nature of the contractual relationship or principles of social coexistence/fair dealing.

A key statutory restriction is Article 473 §2 of the Polish Civil Code, under which a contractual clause excluding liability for damage caused intentionally is invalid.

There are also specific statutory regimes where exclusions or limitations are restricted or ineffective. For example, liability for damage caused by a dangerous product cannot be excluded or limited, and certain limitations of liability towards consumers, including exclusions of liability for personal injury, may be treated as abusive and non-binding.

Where the parties agree contractual penalties/liquidated damages, these usually replace compensation calculated

under general damages rules for the relevant breach, unless the contract expressly provides that the creditor may claim damages exceeding the contractual penalty. This follows from Articles 483–484 of the Polish Civil Code: a contractual penalty may be stipulated for non-performance or improper performance of a non-monetary obligation, and damages exceeding the penalty may be claimed only if expressly reserved by the parties. Polish courts may, however, reduce a contractual penalty if the obligation has been substantially performed or the penalty is grossly excessive.

19. Disputes and enforcement: How are contractual disputes in outsourcing arrangements typically resolved in your jurisdiction and what remedies are commonly available in relation to contractual breaches?

Contractual disputes in outsourcing arrangements in Poland are most commonly resolved before state courts. In technology, software and IP-related disputes, claims may also fall within the jurisdiction of specialised intellectual property courts, including the Intellectual Property Court in Warsaw, which is often relevant for more complex IT, software, copyright, trade secret or unfair competition matters.

In larger or more complex outsourcing contracts, the parties sometimes choose arbitration, in particular where confidentiality, technical expertise or cross-border enforceability are important. In such cases, it is necessary to include a valid arbitration agreement in the contract, or to sign a separate arbitration clause/agreement. Without such an agreement, the dispute cannot be resolved by an arbitral tribunal.

Common remedies for contractual breaches include claims for performance, damages, payment of contractual penalties/liquidated damages, termination or withdrawal from the contract, injunctive relief, return of materials or data, and enforcement of confidentiality, IP, non-solicitation or exit-assistance obligations. Where contractual penalties are agreed, damages exceeding the penalty may generally be claimed only if expressly reserved in the contract.

20. Disputes and enforcement: What, if any, other enforcement measures are typically relevant to outsourcing arrangements (e.g. regulatory fines and other sanctions)?

In practice, the most relevant regulatory sanctions in outsourcing arrangements are often GDPR-related administrative fines, particularly where the outsourced services involve the processing of personal data.

Such fines are frequently imposed on the controller/customer, rather than the processor/service provider, especially where the issue concerns insufficient vendor selection, inadequate data processing agreements, lack of proper instructions, weak supervision over the processor or failure to implement appropriate security measures. Other sector-specific sanctions may also apply, depending on the regulated area, but GDPR enforcement is usually the key practical risk.

Contributors

Artur Piechocki
Radca prawny / Attorney-at-law / Founder
artur.piechocki@aplaw.pl