Legal 500
Country Comparative Guides 2026

Poland
TMT

Contributor



Sołtysiński Kawecki & Szlęzak

Agata Szeliga

Partner | agata.szeliga@skslegal.pl

Marta Kupczak-Strzelecka

Senior Counsel | marta.kupczak-strzelecka@skslegal.pl

Sylwia Macura-Targosz

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

Maciej Gil

Senior Associate | maciej.gil@skslegal.pl

Michał Kalinowski

Associate | michal.kalinowski@skslegal.pl

Alicja Maciążka

Associate | alicja.maciazka@skslegal.pl

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



Poland: TMT

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

The Polish Act on Copyright and Related Rights includes a specific chapter dedicated to the protection of computer programs.

Computer programs are afforded the same protection as literary works, subject to certain modifications specific to software, including with respect to fields of exploitation, the rights of lawful users, moral rights and limitations on fair use. In line with CJEU case law, copyright protection extends to the expression of the program in the form of source code and, potentially, object code. The latter remains a matter of doctrinal debate: some commentators argue that sequences of zeros and ones preclude the requisite element of creative expression, while opponents contend that conversion of source code into object code is analogous to translating a text into Braille.

Elements of a computer program not taking the form of programming code – such as graphical user interfaces – are not protected as computer programs but under separate provisions as graphic works (CJEU, Bezpečnostní softwarová asociace v Ministerstvo kultury [2010] Case C-393/09).

Copyright protection does not extend to the ideas and principles underlying a program, its collection of functions, the programming language used, or the format of data files employed within the program (CJEU, SAS Institute Inc. v World Programming Ltd [2012] Case C-406/10).

Computer programs therefore constitute works of a mixed nature, the various elements of which are subject to different protection regimes under copyright law – as is particularly evident in video games, where the programming component (game engine) is of equal importance to the visual elements (character models, textures, dialogue).

A matter specific to Polish law is the duration of licence agreement, which may be concluded for a maximum term of five (5) years. Any agreement entered into for a longer period is deemed to have been concluded for a definite term, meaning it may be terminated at any time subject to the statutory notice period of one year, effective at the end of the calendar year. According to established case law, this right of termination cannot be waived in advance, as doing so would create perpetual contractual obligations. This is particularly problematic for long-term software licence agreements where the customer invests significant resources in implementation and customisation. The typical solution involves comprehensive contractual guarantees whereby the supplier undertakes not to terminate the agreement, reinforced by substantial contractual penalties.

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?

The answer depends on the contractual relationship. For employment contracts governed by the Polish Labour Code, the Act on Copyright and Related Rights provides for automatic vesting of economic copyright in the employer, provided the program was created within the employee's duties. The employer acquires rights by operation of law, without additional formalities. In practice, however, it is advisable to ensure that employee-developed software is deposited in a dedicated repository to facilitate verification of the scope of software created.

For other civil law contracts, such as contracts for a specific work (umowa o dzieło), acquisition of economic copyright requires express transfer provisions. The transfer agreement must be concluded in writing (handwritten or qualified electronic signature), on pain of nullity, and must specify the fields of exploitation and regulate derivative works rights.

The above rules apply to software created by the humans. In case the software is fully created by the AI without meaningful human intervention, most likely it will not be protected by copyrights.

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

 © 2026 Legalease Ltd

computer systems?

Liability for software-related harm is assessed under the general regimes of the Civil Code, supplemented by new EU product liability law and the Act on Copyright and Related Rights. For criminal and sector-specific regimes on the (mis)use of software, see the response to question 4 below.

Contractual liability

Where software is supplied under a contract, the supplier's liability for defects is governed by the general rules on non-performance or improper performance of obligations (Article 471 of the Civil Code) and, where applicable, the statutory warranty for defects (rękojmia, Articles 556 et seq.) or contractual guarantee.

Where the software is a copyrighted work, Article 55 of the Act on Copyright and Related Rights provides a specific regime: the commissioning party must first give the author a deadline to remedy defects before withdrawing or seeking a price reduction, and may withdraw and claim damages for legal defects. Claims for defects (not legal defects) expire on acceptance.

Parties commonly address performance through SLAs backed by contractual penalties. B2B parties also have broad freedom to limit liability (e.g. to direct loss, a monetary cap or exclude statutory warranty and offer limited guarantees); such limitations are more restricted vis-à-vis consumers.

Non-contractual (tort) liability

Independently of any contractual relationship, general fault-based tort liability under Article 415 of the Civil Code applies to harm caused by defective software. The claimant bears the burden of proving fault, damage and an adequate causal link between them.

Product liability

Title VI¹ of the Civil Code (Articles 449¹-449¹) establishes strict, no-fault producer liability for damage caused by a dangerous product, implementing the former Product Liability Directive 85/374/EEC. So far, the software not embedded in another product has not been regarded as a 'product'.

This is now resolved at EU level: Directive (EU) 2024/2853, repealing Directive 85/374/EEC, expressly treats software – including operating systems, firmware, applications and AI systems – as a 'product' regardless of how it is supplied, and treats its developer or producer (including AI system providers under the EU AI Act) as a manufacturer. Free and open-source software supplied outside a commercial activity remains outside its scope.

EU Member States, including Poland, must transpose the Directive by December 2026. Poland has already prepared the draft of new product liability rules.

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?

Beyond general civil liability, Polish law addresses software and computer-system misuse principally through criminal law and sector-specific regulatory regimes.

Criminal Code

Chapter XXXIII of the Criminal Code ('Offences against the protection of information') criminalises the core forms of software misuse, such as unauthorised access to an IT system (Article 267).

Sector-specific and other regulatory regimes

The National Cybersecurity System Act (the 'NCS') imposes, among others, incident-reporting and security obligations on operators of essential services and digital service providers, implementing the EU NIS/NIS2 framework. A software failure causing a personal data breach may also trigger liability under the General Data Protection Regulation (EU) 2016/679 (the 'GDPR') for the controller. Depending on sector, additional regimes may apply – including telecommunications, financial services, medical devices, the EU AI Act, and consumer protection rules on digital content – each potentially giving rise to independent liability or administrative sanctions.

Separately, infringement of copyright in computer programs (Act on Copyright and Related Rights) and of sui generis database rights (Act on the Protection of Databases) each give rise to distinct civil and criminal remedies.

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?

Software supply in Poland is governed by a combination of general and sector-specific regimes:

 © 2026 Legalease Ltd

- **Contract law framework.** See our response to question 3 above.
- **Consumer protection.** For consumers, contracts for digital content – expressly including software – are governed by a dedicated chapter of the Consumer Rights Act (Chapter 5b), covering delivery, conformity, remedies and the burden of proof.
- **Copyright and licensing.** Governed by the Act on Copyright and Related Rights, whose dedicated provisions on computer programs apply – see our response to question 1.
- **Electronic services law.** Where software is supplied as an information society service, the Act on Providing Services by Electronic Means imposes information obligations and requires terms of service, implementing the EU e-Commerce Directive.
- **Cloud-specific regulation.** There is no dedicated 'cloud act', but cloud providers fall within the national cybersecurity framework. Under the amended NCS, providers of cloud, data centre, content delivery networks and managed (security) services face risk-management and incident-notification obligations depending on their classification as key or important entities. The Polish Ministry of Digitalization announced that it intends to adopt Polish Cloud Act to regulate cloud services, but the works are at the early stage.
- **EU Data Act.** Imposes cloud-switching, interoperability and vendor lock-in mitigation obligations on data processing service providers.
- **Data protection.** Software or cloud arrangements involving personal data are additionally subject to the GDPR, including processor/controller data processing agreements and, where relevant, international transfer restrictions for cloud infrastructure outside the EEA.

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?

Yes, capping a software vendor's aggregate financial liability is standard market practice in B2B software transactions in Poland and is generally enforceable. A clause excluding liability for intentional damage is void, and sector-specific statutes may override contractual freedom – for example, Polish banking law states that the liability of the service provider rendering outsourcing services towards the bank for the damages caused to bank's clients due to non performance or improper performance of such outsourcing agreement between provider and the bank cannot be excluded. Such liability, however, may currently be limited.

Liability caps are far more constrained in consumer contracts, where a clause excluding or materially limiting liability for non-performance is presumptively an unfair contractual term.

Market practice for IT implementation and software supply contracts typically sets the aggregate cap at 100% of total net fees payable under the agreement or, for multi-year or recurring contracts, fees invoiced in the preceding 12 months. Liability for lost profits and other consequential or indirect losses is typically excluded. Certain liabilities are commonly carved out from the cap, as discussed in question 7 below.

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; (h) claims arising out of or in relation to artificial intelligence.

Parties to a negotiated B2B software transaction have broad freedom to structure liability caps and carve-outs, subject to the mandatory constraints discussed in question 6 above. Polish market practice distinguishes three tiers: (i) a general aggregate cap; (ii) enhanced sub-caps for specified risk categories; and (iii) areas of unlimited liability.

Carve-outs from the general cap (or enhanced sub-caps) are common for confidentiality breaches other than those applicable to customer data in cloud services (a) and for the IPR infringements (d). The liability for confidentiality (a), data protection (b) and data security breaches (c) for cloud processed or stored data is usually subject to the

 © 2026 Legalease Ltd

general limitation cap. For the regulatory fines (f) there is no one unified practice – some providers include it in carve outs but the largest limit their liability. The breaches of applicable law (e) are are not typically carved out as a standalone category, overlapping materially with (b), (f) and (g). Wilful or deliberate breaches (g) attract unlimited liability by operation of law: intentional damage cannot be excluded or limited in advance under the Civil Code, and parties often extend this to gross negligence. For AI-related exposure, some providers offer unlimited liability in case of IPR claims to the AI-generated output provided that certain conditions (e.g. the input does not violate the third party copyrights). The AI solutions are regarded as products thus they will be covered by IPR infringement carve outs.

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?

Yes, for the bespoke software or business critical software in regulated sector. It is not that common for the standard, off the shelf solutions. There is no dedicated statutory regime; escrow is usually structured as a trilateral contract (developer/licensor as depositor, licensee as beneficiary, and an independent escrow agent) based on freedom of contract.

Typically, the developer deposits the source code, technical documentation and materials necessary for compilation with the escrow agent, retaining ownership. The licensee obtains a contingent right to release only on specified triggering events, most commonly the licensor's insolvency, cessation of business, or material breach of the licence or support agreement.

Escrow can be arranged as: a physical deposit, an electronic deposit, a hybrid of the two, or a deposit with automatic updating via a repository integration.

Typical escrow providers in the Polish market include both specialised technical/IT escrow agents and notaries public.

For bespoke cloud-based/SaaS software, an equivalent service is offered, although the scope of a SaaS escrow arrangement is broader: it typically extends to build and deployment scripts, configuration data, infrastructure-as-code and third-party dependency information needed to redeploy the service on alternative infrastructure, together with customer data export mechanisms. Triggering events are correspondingly adapted, commonly including prolonged unavailability or discontinuation of the hosted service.

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

Poland has no single, dedicated statute regulating 'IT outsourcing' as a distinct category. Outsourcing arrangements are instead governed by the general contract law framework referred to in our response to question 1 above, supplemented by sector-specific regimes that apply where the outsourcing customer or the outsourced function falls within a regulated sector.

The most developed sector-specific regime applies to financial sector entities, including banks. Under Banking Law, a bank may only outsource IT and other operational functions to a domestic or foreign entrepreneur under a written agreement satisfying conditions such as business-continuity planning or adequate safeguards for confidential information, and for outsourcing with non-EEA entity or if services are provided outside of EEA – non-objected notification to the Financial Supervision Authority (the 'KNF'). Outsourcing may not cover bank management or internal audit. As for liability – see sec. 6. KNF recommendations on IT and outsourcing risk reflect equivalent, non-binding supervisory expectations. Specific outsourcing rules apply also to other financial sector entities, including insurance companies, investment funds or brokerage houses.

IT outsourcing by financial entities also falls within the scope of the ICT third-party risk management requirements under Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (the 'DORA'), which impose due diligence obligations, mandatory contractual content requirements, and the maintenance of a register of ICT third-party arrangements. In cloud services, the EU Data Act will apply, particularly for switching and exit. Where personal data is involved, GDPR processor/controller obligations are also triggered. In addition, where the outsourced function falls within critical infrastructure or covers certain digital service providers, the NCS may impose supply-chain security obligations on the outsourcing entity.

10. IT Outsourcing – Please summarise the

 © 2026 Legalease Ltd

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.

The principal protection is Article 23¹ of the Polish Labour Code, interpreted in line with EU Directive 2001/23/EC on safeguarding employees' rights on transfers of undertakings. Whether Article 23¹ applies to a given IT outsourcing project depends on the specific circumstances: Polish courts examine whether the outsourced activity constitutes an identifiable economic entity, or an organised part of the undertaking, that retains its identity after the transfer. As a result, some IT outsourcing arrangements can trigger the transfer rules, while others are treated merely as service contracts with no accompanying employee transfer.

Where it applies, Article 23¹ principal safeguards are: automatic transfer of employment by operation of law, on existing terms, without new contracts or consent; a prohibition on dismissal by either employer on grounds of the transfer; joint liability of both employers for pre-transfer employment obligations; a duty to inform staff in writing at least 30 days before the transfer of its date, reasons and consequences (this direct information duty applies only where no trade union operates at the employers concerned); a right for the employee to resign within two months of the transfer on seven days' notice, treated as employer-initiated termination. The law applies to staff engaged based on employment contract and is not applicable to B2B contractors.

The purpose of the law is to protect the employees against redundancy if the entire employment establishment or organized part thereof is transferred to another employer with keeping its earlier identity, structure, etc.

11. 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.

Electronic Communications Law ('PKE'), which entered into force in November 2024 is the principal statute governing the provision of telecommunications networks and services in Poland. It transposes the European Electronic Communications Code, together with the ePrivacy Directive and related EU instruments. The PKE regulates: the conditions for pursuing electronic communications activity (networks, telecommunications services and number-independent interpersonal communications services); the rights and obligations of electronic communications undertakings and end users; spectrum, orbital resource and numbering management; telecommunications access and market regulation; universal service; data processing and confidentiality of electronic communications; and the powers of the President of the Office of Electronic Communications ('UKE') and the minister for digitalisation.

A further principal statute is the Act of 28 July 2023 on Combating Abuse in Electronic Communications ("CAEC"), which also implements part of the EECC. It sets out telecommunications undertakings' rights and obligations, and the President of UKE's powers, in preventing and combating abuse in electronic communications, including CLI spoofing, smishing and misuse of SMS sender IDs. It also establishes a public warning list of fraudulent internet domains.

12. 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.

Under the PKE, telecommunications activity constituted as business activity is a 'regulated activity' and is subject to entry in the register maintained by UKE. An applicant submits a written application containing prescribed particulars; UKE must register the applicant within 3 working days, and the applicant may commence activity once that period has lapsed without a response. No prior individual authorisation or licence is required to provide publicly available telecommunications services or to deploy telecommunications networks; separate rights of use are required only for the use of scarce resources such as frequencies and numbering.

13. 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.,

 © 2026 Legalease Ltd

whether requests are confidential, subject to challenge, etc.), and any legal or procedural safeguards that apply.

Access to communications data by law enforcement and other authorised bodies is governed principally by the PKE, read together with the sectoral statutes governing each requesting authority (e.g. the Police Act). Telecommunications operators and service providers must retain, at their own cost and within Poland, data enabling identification of the parties, timing, type and location of a communication (including failed call attempts) for 12 months, after which the data must be destroyed unless secured under separate rules. Retained data must be made available, on request and free of charge, to the authorised entities, as well as to courts and prosecutors. Operators must provide the technical and organisational means (such as interfaces) enabling access without the involvement of their staff. Such requests are, in practice, confidential; procedural or legal safeguards are very limited in practice.

14. Telecommunications – Please summarise the principal laws (present or impending) that impose cyber security and/or operational resiliency obligations applicable to the operation of telecommunications infrastructure and/or provision of telecommunications services.

Cybersecurity and operational resiliency obligations applicable to telecommunications infrastructure and services arise from two regimes. First, Chapter VIIA of the telecom law requires telecommunications undertakings to take technical and organisational measures proportionate to risk to ensure the security and integrity of networks, services and the transmission of communications, to notify UKE without delay of any breach of security or integrity with a significant impact on network or service functioning, and to take measures such as blocking harmful traffic. Second, the NCS as described in sec. 20 below.

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?

Poland does not have a distinct national standard-setting body for mobile communications.

16. Mobile communications and connected technologies – How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

Same as above.

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.

The principal law governing data protection in Poland is the GDPR, which is directly applicable in Poland. The GDPR is supplemented at national level by the Act of 10 May 2018 on the Protection of Personal Data (the 'Personal Data Protection Act'), which establishes the national institutional and procedural framework by determining: the competent data protection authority (the President of the Personal Data Protection Office, the 'PUODO'). In addition to the GDPR and the Personal Data Protection Act, data protection is also regulated by a range of sector-specific acts, such as the Polish Labour Code (which contains specific rules on the processing of job candidates' and employees' personal data) and other sectoral laws (e.g. in banking, insurance, healthcare and telecommunications) that impose additional or more specific data processing requirements applicable to their respective sectors. In particular, the PKE has its own regime governing the confidentiality of telecommunications (electronic communications secrecy), the notification of personal data breaches, and marketing consents and cookies.

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?

In Poland, sanctions for breach of personal data protection law derive from Article 83 of the GDPR, which sets two tiers of maximum administrative fine depending on the type of infringement. For the less serious category of infringements, the PUODO may impose a fine of up to EUR 10,000,000 or, in the case of an undertaking, up to 2% of its total worldwide annual turnover for the preceding financial year, whichever is higher. For the more serious category of infringements, the maximum fine is up to EUR

 © 2026 Legalease Ltd

20,000,000 or, in the case of an undertaking, up to 4% of its total worldwide annual turnover for the preceding financial year, whichever is higher. For a violation of the obligation to maintain the secrecy of electronic communications, and for processing data covered by the secrecy of electronic communications or user data without a legal basis, the President of UKE imposes a fine of up to 3% of the penalized entity's revenue earned in the preceding calendar year.

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

Because the GDPR applies directly, technology contracts in Poland expressly reference the GDPR even where the contract has no international element. References to other regimes, such as the US CCPA, are rare and appear only where the transaction has a genuine connection to that market.

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.

The principal law governing cybersecurity in Poland is the Act of 5 July 2018 on the National Cybersecurity System ('KSC'), amended with effect from 3 April 2026 to implement Directive (EU) 2022/2555 ('NIS2"). It sets the horizontal framework for essential and important entities, covering cybersecurity risk management, supply-chain security, incident reporting and regulatory supervision.

The KSC operates alongside DORA, which directly regulates ICT risk management, incident reporting, resilience testing and third-party provider risk for financial entities, supplemented by national banking, payment services, insurance and capital-markets legislation.

Cybersecurity certification is governed by Regulation (EU) 2019/881 (the Cybersecurity Act, 'CA") and the Act of 25 June 2025 on the National Cybersecurity Certification System. Regulation (EU) 2024/2847 (the Cyber Resilience Act, 'CRA") imposes security-by-design, vulnerability-management and reporting obligations on products with digital elements placed on the EU market, with reporting duties applying from 11 September 2026 and most provisions from 11 December 2027.

Further sector-specific requirements arise from PKE and the CAEC which govern the security and confidentiality of electronic communications and address abuses such as smishing and caller-line identification spoofing.

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?

There is no single maximum sanction; the ceiling depends on the entity and obligation infringed. Under the KSC, an essential entity may be fined up to the higher of EUR 10 million or 2% of its preceding financial -year revenue, and an important entity up to EUR 7 million or 1.4% of revenue. A separate fine of up to PLN 100 million applies where an infringement creates serious cyber threats or risks. Ordinary KSC fines may first be imposed after 3 April 2028; the PLN 100 million fine is not expressly subject to that deferral. Under KSC, a manager of an essential or important entity may be personally fined for failing to perform specified cybersecurity obligations, up to 300% of their remuneration, or 100% for most public-sector entities; such fines may first be imposed after 3 April 2028.

For financial entities, DORA and Polish financial supervision legislation allow the KNF to fine a legal person up to PLN 20,869,500 or 10% of total annual revenue, or twice the benefit obtained or loss avoided if determinable. From 11 December 2027, the highest CRA fine will be the higher of EUR 15 million or 2.5% of an undertaking's total worldwide annual turnover.

Where a cyber incident also constitutes a personal-data breach, parallel liability may arise under the GDPR or, in the electronic communications sector, the PKE– as indicated in the paragraph 18 above.

22. Cybersecurity – Are there any cybersecurity regulatory frameworks in your jurisdiction which require registration for certain sectors or services?

The principal registration requirements arise under the KSC. Under the KSC, essential and important entities must be entered in the national register of essential and important entities. Most private-sector entities register themselves, while public bodies, telecommunications

 © 2026 Legalease Ltd

undertakings and trust service providers are entered ex officio.

DORA does not require financial entities to register with an external cybersecurity register.

23. Cybersecurity – Please summarise the regulatory framework for the reporting of cybersecurity incidents.

The principal incident-reporting regimes are the KSC, DORA, the CRA and the transitional regime under former Article 175a of the Telecommunications Law ('TL'). The GDPR or the PKE may apply separately where A cyber incident may also constitute a personal-data breach at once; such a personal-data breach is to be notified to PUODO under PKE, in accordance with the data protection regime

Under the KSC, essential and important entities must generally submit an early warning within 24 hours, an incident notification within 72 hours and a final report within one month. Under DORA, financial entities report major ICT-related incidents to the KNF through initial, intermediate and final reports on broadly equivalent deadlines.

From 11 September 2026, the CRA requires manufacturers to report actively exploited vulnerabilities and severe incidents affecting products with digital elements to the coordinating CSIRT and ENISA. Telecommunications undertakings previously subject to former Article 175a TL (transitional regime, as pointed out above) must keep reporting significant security or integrity breaches to the President of UKE until they move to the KSC regime, no later than 3 April 2027 if they met the relevant criteria on 3 April 2026.

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

The Commission for the Development and Safety of Artificial Intelligence

The Commission for the Development and Safety of Artificial Intelligence (Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji) (the 'Commission') is the central market surveillance authority (Article 70(1) AI Act) and single point of contact (Article 70(2)). Its responsibilities include: (i) supervising compliance with the AI Act and the Polish Act on AI; (ii) issuing infringement decisions; (iii) establishing regulatory sandboxes; (iv) imposing administrative fines; (v) issuing opinions and guidance; (vi) maintaining registers of complaints and penalised AI systems; and (vii) cooperating with the European Commission, the European Artificial Intelligence Board, the scientific panel, and other Member States' authorities.

The Minister responsible for digital affairs

The Minister responsible for digital affairs (minister właściwy do spraw informatyzacji) serves as the notifying authority (Chapter III, Section 4 of the AI Act), responsible for accreditation and notification of conformity assessment bodies. The Minister also supports innovation, including by issuing best-practice recommendations for AI use and providing conditions for regulatory sandboxes.

The Social Council for Artificial Intelligence

The Social Council for Artificial Intelligence (Społeczna Rada do spraw Sztucznej Inteligencji) (the 'Council') is an advisory body composed of nine to fifteen members appointed by the Commission for a two-year term. Its tasks include issuing opinions on matters referred by the Commission, forwarding requests for infringement proceedings, and overseeing compliance by the Commission's Chairperson and Deputy Chairpersons with conflict-of-interest provisions.

Cooperation with other public authorities

The Commission cooperates with the KNF, the PUODO, the National Broadcasting Council, the Government Plenipotentiary for Cybersecurity, the President of the Office for Registration of Medicinal Products, Medical Devices and Biocidal Products, the Chief Pharmaceutical Inspector, the Digital Services Coordinator, the Patent Office, and the Prosecutor General. Supervision over the intelligence services' use of AI is exercised by the Prime Minister or the Minister-Coordinator of the Intelligence Services.

25. 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 deployment and use of artificial intelligence in Poland is governed principally by the AI Act and the Polish Act on AI. The AI Act, as a directly applicable EU regulation, establishes a risk-based classification of AI systems, sets out requirements for providers and deployers, prohibits certain AI practices, and provides for conformity

 © 2026 Legalease Ltd

assessment, market surveillance and enforcement.

The Polish Act on AI does not introduce substantive requirements beyond the AI Act but establishes the domestic regulatory architecture necessary for its enforcement, including the organisation of the Commission, the procedure for investigating infringements, accreditation of conformity assessment bodies, regulatory sandboxes, and administrative fines.

On 21 November 2025 the Polish Parliament adopted the Act Amending the Road Traffic Act and Certain Other Acts, which defines 'automated vehicle' and 'fully automated vehicle' (aligned with EU Regulation 2019/2144) and establishes six levels of automation corresponding to the SAE classification. The holder of an automated or fully automated vehicle is subject to strict (risk-based) liability for damage caused by its movement and must maintain valid mandatory third-party motor insurance.

Poland has not yet transposed Directive (EU) 2024/2853 on liability for defective products, the implementation deadline for which is 9 December 2026. The Directive extends the product definition to cover software, including in relation to compensation for destruction or corruption of data. It simplifies the burden of proof for claimants and permits recovery of both material damage and medically certified non-material damage. However, the practical significance of the Directive in the AI context may be limited by the liability exemptions provided therein.

26. 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)?

There are currently no specific legal provisions, whether in force or impending, governing the deployment and use of Large Language Models or generative AI (including agentic AI) as distinct categories. The laws mentioned above apply.

27. 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?

There are no mandatory provisions required in such contracts, although market practice increasingly addresses AI risk.

Given that unrestricted use of AI systems may entails processing of internal data (potentially confidential or personal), contractual provisions addressing AI-related data risks are now standard in AI supply agreements. In particular, prohibitions on training AI models using the customer's input or output data are routinely included in enterprise type licenses.

The AI Act will most likely further influence the wording of agreements, especially for high-risk systems.

28. 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?

Yes, there is a growing market practice of incorporating AI-specific provisions in technology contracts and in contracts with creative personnel. AI-generated content created without meaningful human intervention is considered not to be protected under copyright law, on the basis that it lacks the requisite element of human creative input. Nevertheless, the prevailing market standard in enterprise transactions is that any output is treated as the client's data (although certain providers restrict the use of output generated under free or basic-tier subscriptions), and indemnification clauses addressing the lawfulness of, and freedom to use, such output are common. A notable example is Microsoft's Customer Copyright Commitment, under which Microsoft undertakes to defend the customer against third-party intellectual property claims, subject to the customer's compliance with specified usage requirements.

With respect to creative personnel, contracts typically require the use of only internally authorised AI tools and, given that AI-generated output cannot be the subject of a transfer of copyrights, include provisions permitting the employer to use such output on exclusive basis and requiring the personnel to undertake not to raise any claims in respect thereof.

29. Blockchain – What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital

 © 2026 Legalease Ltd

assets, including a brief explanation of the general purpose of those laws?

There is no separate, dedicated regulation of blockchain technology in Poland. The law regulates the digital assets (crypto-assets) based on that technology and the services related to them. The currently applicable national law comprises the AML Act, which since 2021 has regulated 'virtual currency activity' as a regulated activity subject to entry in a register, for anti-money laundering purposes; the transitional period allowing entities on that register to continue operating under the previous rules expired on 1 July 2026. Since that date, directly applicable EU Regulation (EU) 2023/1114 on markets in crypto-assets ('MiCA') apply in Poland. Although MiCA applies directly and does not require transposition, Poland has not yet adopted the accompanying national act on the crypto-asset market that would designate the KNF as the supervisory authority, introduce a licensing regime for crypto-asset service providers and issuers, and set out administrative and criminal sanctions and civil liability rules. A government bill was vetoed by the President on 11 June 2026; revised draft legislation remains subject to ongoing legislative proceedings. As a result, Poland currently has no operational domestic licensing regime for crypto-asset service providers under MiCA.

30. 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.

The regulation of online search engines and marketplaces in Poland is principally governed by directly applicable EU legislation, supplemented by Polish implementing measures.

EU Digital Markets Act (Regulation (EU) 2022/1925)

The DMA, directly applicable in Poland, targets 'gatekeepers' providing core platform services (including online search engines and marketplaces) that meet quantitative thresholds of market power. Its purpose is to prevent unfair practices that undermine contestability of digital markets, including self-preferencing in ranking and indexing.

EU Digital Services Act (Regulation (EU) 2022/2065)

The DSA, also directly applicable, establishes a harmonised framework of due diligence obligations for intermediary services, including online search engines and marketplaces, covering notice-and-action mechanisms for illegal content, transparency, and, for marketplaces specifically, traceability of traders. Very large online platforms and search engines (45 million+ monthly EU users) are subject to additional risk-assessment and auditing obligations.

Poland has not yet enacted the domestic legislation required to designate a national Digital Services Coordinator and lay down enforcement procedures for the DSA. A government bill was vetoed by the President on 9 January 2026; revised draft legislation remains subject to ongoing legislative proceedings.

EU General Product Safety Regulation and Polish implementation

The General Product Safety Regulation (the 'GPSR'), directly applicable since 13 December 2024, is relevant to online marketplaces, requiring providers to designate contact points for authorities and consumers, register with the Safety Gate Portal, and maintain product safety compliance processes. Poland has given domestic effect to GPSR through the Act of 7 November 2025 on Supervision of General Product Safety.

Other relevant regulations

The EU Platform-to-Business Regulation (Regulation (EU) 2019/1150) promotes fairness and transparency for business users of online intermediation services and search engines, requiring clear terms and advance disclosure of ranking parameters, and access to internal complaint-handling and mediation mechanisms. The Polish Consumer Rights Act imposes specific pre-contractual information duties on marketplace providers, implementing EU Directive (EU) 2019/2161 (the 'Omnibus Directive'). These sit alongside general Polish competition and consumer protection law enforced by the PCA. The EU Accessibility Act and the Polish implementing legislation impose accessibility requirements on operators of e-commerce services, including online marketplaces.

31. 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?

EU Digital Markets Act (Regulation (EU) 2022/1925)

See more about DMA in response to Question 26.

 © 2026 Legalease Ltd

EU Digital Services Act (Regulation (EU) 2022/2065)

See more about DSA and Polish Act in response to Question 26.

Platform-to-Business Regulation (Regulation (EU) 2019/1150)

See our response in Question 26.

Act on Providing Services by Electronic Means of 2002

The Act sets out the obligations of electronic service providers, the principles for excluding their liability, and the rules on protection of users' personal data. Providers must adopt terms of service specifying, in particular, the types and scope of services offered, conditions of provision (including a prohibition on unlawful content), conclusion and termination of service agreements, and the complaints procedure.

Copyright Act of 1994 (implementing DSM Directive)

The Polish Copyright Act, implementing Article 17 of the EU Copyright in the Digital Single Market Directive, establishes a specific liability regime for online platforms that store and provide public access to user-uploaded copyrighted content, balancing the protection of rightholders' rights with users' rights to make lawful use of works.

Act on Consumers Rights of 2014

The Polish Act on Consumer Rights governs distance contracts with consumers, requiring entrepreneurs to provide clear pre-contractual information (including price, duration, essential terms, and consumer rights), regulating the statutory fourteen (14) day withdrawal right, and addressing the consumer's remedies in the event of non-conformity of goods or services with the contract. The Act implements, inter alia, Directive 2019/770.

The significance of this framework has increased considerably due to the highly active enforcement approach of the PCA, which applies a broad and formalistic interpretation of consumer protection provisions to ensure that entrepreneurs do not exploit the weaker position of consumers.

The PCA's enforcement activities focus on combating abusive clauses, i.e. non-individually negotiated provisions that shape consumer rights contrary to good practice and to the gross detriment of consumer interests, as well as practices infringing collective consumer interests, particularly misleading advertising and improper price presentation (implementing Directive 2019/2161).

The PCA has issued detailed recommendations on price presentation (80 pages) and on the labelling of advertising content by influencers (30 pages), and conducts regular inspections with substantial financial penalties in both areas.

32. 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?

Under the DSA, national Digital Services Coordinators may impose fines of up to 6% of global annual turnover (or 1% for providing incorrect, incomplete or misleading information), and periodic penalty payments of up to 5% of average daily worldwide turnover per day of non-compliance.

Under the DMA, the European Commission may impose fines of up to 10% of worldwide turnover (20% for repeat offences) and, for systematic non-compliance, structural remedies including divestiture.

The PCA may impose fines of up to 10% of worldwide turnover per infringement and up to PLN 2 million (EUR 500,000) on managers who intentionally permitted the infringement, declare abusive clauses non-binding on consumers, order publication of its decision, and require consumer compensation (e.g. refunds or discounts).

33. 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?

Poland has no dedicated statute for spatial computing. The relevant legal framework is EU-derived and directly applicable, supplemented by general Polish civil and consumer law. The principal instruments include:

- **the EU AI Act**, which may apply e.g. to spatial computing use cases involving biometric categorisation, emotion recognition, eye-tracking and gesture recognition – systems performing such functions may fall within the prohibited or high-risk categories under the Act, triggering conformity assessment, documentation and transparency obligations;
- **the GDPR**, which governs the processing of

 © 2026 Legalease Ltd

personal data (including biometric and other special-category data) by spatial computing devices, with particular compliance challenges arising from the capture of third parties in public spaces by always-on sensors, where the household exemption does not apply and transparency obligations toward incidentally recorded bystanders are difficult to satisfy;
- **the revised EU Product Liability Directive and its Polish implementation** , which extends strict manufacturer liability to software, including software controlling AR/VR hardware, once transposed into Polish law;
- **for consumers: general Polish consumer protection legislation and the Act on Providing Services by Electronic Means**, which apply to spatial computing platforms offering digital content, virtual goods or in-world transactions.

34. 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?

There is currently no single, dedicated statute in Poland regulating quantum computing or quantum cryptography as such. The subject is instead addressed indirectly, through general cybersecurity, classified-information and dual-use export control legislation, supplemented by strategic policy instruments that set out the direction of future regulatory and legislative work.

- **NCS.** While the NCS does not mention quantum technology expressly, it is the general vehicle through which resilience requirements – including cryptographic requirements – for key sectors are imposed.
- **National Cybersecurity Strategy (Resolution No. 92 of the Council of Ministers of 10 March 2026).** The Strategy contains a dedicated objective on 'development of national cryptology, including migration to post-quantum cryptography and development of quantum technologies,' under which Poland commits to developing national cryptographic capacity that takes into account the challenges of post-quantum cryptography, including the ability to design and produce cryptography-based solutions independently of foreign organisations and institutions.

The Strategy further provides for the assessment and implementation of new international cryptographic standards, the establishment of R&D programmes covering post-quantum cryptography and quantum key distribution, and the strengthening of NCS entities' operational capabilities through new technologies. While not binding legislation, it signals forthcoming legislative and regulatory initiatives in this space.

- **National Digital Decade Action Plan.** This non-binding policy instrument addresses quantum technology from an infrastructure and industrial-policy perspective. The Action Plan records that Poland does not yet operate its own quantum computer and sets a national target of two operational quantum computers by the end of the decade, committing public funding to that end. It further identifies the development of dedicated policy on quantum technologies and the work of an inter-ministerial working group on breakthrough technologies as planned measures intended to shape future legislative and regulatory initiatives in this space.

- **Classified Information Protection Act.** Existing rules on IT security under the Act on the Protection of Classified Information require cryptographic devices and tools used to protect classified information to undergo security certification by the Internal Security Agency or Military Counterintelligence Service, and empower the Prime Minister to set baseline security requirements for ICT systems. These certification requirements will, over time, need to accommodate post-quantum cryptographic modules as they are adopted.

- **Dual-use export controls.** Poland applies the directly applicable EU Dual-Use Regulation. Quantum computers and related components were formally added to the EU's control list under new classification 4A506 by a Commission Delegated Regulation effective 15 November 2025, meaning exports of qualifying quantum hardware and related electronic assemblies' and components therefor from Poland outside the EU now require prior authorisation.

35. Datacentres – Does your jurisdiction have any specific regulations that apply to data

 © 2026 Legalease Ltd

centres?

Poland does not have a separate, dedicated statute regulating data centers exclusively.

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

First, the AI Act supervisory regime will move from legislation to live operation. The Polish Act on AI has already entered into force, but the Commission has not yet been established.

Second, NIS2 implementation will shift from legislative transposition to practical compliance Entities generally have 12 months to implement the new requirements, they need to register until 3 October 2026.

Third, digital sovereignty will become an increasingly prominent driver of policy and regulation, with growing focus on cyber security amid the security situation created by Russia.

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

Sustainability, net-zero, or similar environmental commitment provisions are not yet a common feature of technology contracts in Poland. Where such clauses do appear, it is almost exclusively in contracts involving subsidiaries of international corporate groups, which import their parent group's global ESG standards or supplier codes of conduct into the local contract. Outside these international-group cases, such clauses remain rare in standard Polish contracting practice.

Contributors

Agata Szeliga
Partner
agata.szeliga@skslegal.pl



Marta Kupczak-Strzelecka
Senior Counsel
marta.kupczak-strzelecka@skslegal.pl



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



Maciej Gil
Senior Associate
maciej.gil@skslegal.pl



Michał Kalinowski
Associate
michal.kalinowski@skslegal.pl



Alicja Maciążka
Associate
alicja.maciazka@skslegal.pl

 © 2026 Legalease Ltd