Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2026

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

Poland: Trends & Developments

Agata Szeliga, Marta Kupczak-Strzelecka and Sylwia Macura-Targosz
Sołtysiński Kawecki & Szlęzak

POLAND

Trends and Developments

Contributed by:
Agata Szeliga, Marta Kupczak-Strzelecka and Sylwia Macura-Targosz
Sołtysiński Kawecki & Szlęzak

Sołtysiński Kawecki & Szlęzak (SK&S) is one of Poland's leading full-service law firms. With more than 200 attorneys, the firm provides the highest standard of legal services in all areas of business activity, and is well reputed for the quality of its work and for its innovative approach to complex legal problems. Since the 1990s, SK&S has been closely associated with the ever-changing technology sector, especially the dynamically developing IT industry. The firm provides high-quality legal services to both individuals and companies, covering the full scope of TMT issues. The team works alongside the firm's fintech, IP/IT, privacy and tax teams to provide an innovative interdisciplinary service, and to help businesses use state-of-the-art technologies in a safe, cost- and time-effective manner. SK&S was the founding member of the New Technologies Association.

Authors

Agata Szeliga is a partner at SK&S and specialises in new technologies and personal data protection, as well as state aid and public procurement laws. She advises on cloud computing and on software and IT services, including negotiations on the implementation of IT systems. Agata helps in reviewing IT solutions from the privacy perspective, and in handling sensitive data protection requests or complaints. She also advises on AI and the sharing of data generated by devices, especially in the automotive sector. She represents clients before Polish authorities and regulators and the European Commission, and is a member of the Commission's Expert Group on B2B data sharing and cloud computing contracts.

Marta Kupczak-Strzelecka specialises in media and telecommunications regulation, advising media companies, mobile operators and e-commerce clients on complex regulatory matters. She represents clients before Polish media and telecoms regulators and courts, including in freedom of speech disputes, licensing proceedings, spectrum refarming, digitalisation of broadcasting and 5G auctions. Marta supports major international and Polish clients in the application of EU and national regulations (EMFA, EECC, EAA, NIS2, DSA). She is a certified expert to the Polish Chamber of Commerce for Electronics and Telecommunications, a member of the New Technologies Law Association, and an author of numerous publications on media, telecoms and technology law.

Sylwia Macura-Targosz is a senior associate at SK&S, specialising in IT, new technologies and e-commerce law. She has advised on numerous IT projects, and also supports clients on the legal side of projects relating to the use of AI and the sharing of device-generated data. Sylwia excels in the field of personal data protection and privacy. She acts as Data Protection Officer for clients, and supports entrepreneurs in proceedings conducted by the President of the Personal Data Protection Office. Sylwia assists local and global companies with data protection issues, helping them to comply with the Polish law. She is a member of the Polish New Technologies Law Association.

Contributed by: Agata Szeliga, Marta Kupczak-Strzelecka and Sylwia Macura-Targosz, **Sołtysiński Kawecki & Szlęzak**

Sołtysiński Kawecki & Szlęzak

Jasna 26
00-054 Warsaw
Poland

Tel: 0048 22 608 70 00
Fax: 0048 22 608 70 01
Email: office@skslegal.pl
Web: www.skslegal.pl

TMT in Poland: An Introduction

2025: a brief summary

2025 was driven by lengthy legislative procedures that aimed to implement the Digital Services Act (DSA), the European Media Freedom Act (EMFA) and NIS2 Directives into Polish national legislation. Unfortunately, none were completed (see below for more details).

The President of the Office of Competition and Consumer Protection (OCCP) continued the actions undertaken in 2023 towards strengthening consumer protection on the internet. The President of the OCCP's actions are directed against entrepreneurs who infringe consumers' rights by failing to provide them with the information required by law or by using "dark patterns" through improperly presenting prices, not revealing who the seller is, using false counters, and providing misleading statements. The President of the OCCP also challenged the practices of platforms operating on a subscription model that allowed the platform to unilaterally change prices and other material terms of the contract without obtaining the user's active consent.

In September 2025, Przemysław Kuna was appointed as the new President of the Office of Electronic Communications (UKE). For over 20 years, he held managerial positions in the telecommunications sector, and he recently held the position of Deputy Director of the National Research Institute (NASK). In December 2025, Piotr Kuriata (a former member of the management board of the Play mobile network operator) became an adviser to the President of UKE. His role is to support the President of UKE in building a strategy for the telecommunications market in Poland.

2026: trends and developments

Polish implementation of the Digital Services Act

In Poland, the legislative process aimed at implementing the DSA is still ongoing. This is to be achieved by amending the Polish Act on the Provision of Electronic Services, which was finally passed by the Sejm after considering the Senate's amendments on 18 December 2025. The Polish implementation of the DSA is attracting a lot of public interest, mainly due to its provisions on blocking illegal content and unblocking content that has been wrongly blocked.

Orders to block or unblock content on the internet

The draft law provides for the possibility to issue two types of orders:

- an order to take action against illegal content – ie, to block access to it; and
- an order to remove restrictions (moderation) imposed by the hosting provider on the user – ie, to unblock access to the content.

During the Sejm's deliberations, Polish lawmakers clarified that the country-of-origin principle set out in Article 3a of the Act on the Provision of Electronic Services will not apply to these orders. This is important in the case of cross-border situations, as it means that Polish blocking and unblocking orders may be addressed to foreign internet platforms, particularly social media platforms used by Polish internet users.

The orders will be issued by the President of UKE or the Chair of the National Broadcasting Council (KRRiT); the latter will only supervise video sharing platforms. The user who posted the questionable content will also be able to participate in the proceedings before the competent authority. An objection to an order to block illegal content may be lodged with a common court within 14 days of its delivery. The blocking order will not be enforceable immediately. After the ruling of the courts of first and second instance, it will be possible to lodge a cassation appeal with the Supreme Court.

Blocking illegal content on the internet

Orders to take action against illegal content may be addressed to all types of internet intermediaries – ie, not only to internet platforms and hosting providers, but also to telecommunications operators.

A request for an order to block illegal content may be submitted by a user of a given online service, a prosecutor, the police, an authority of the National Revenue Administration, a copyright or related rights-holder or, in cases involving human trafficking, the Border Guard. At the stage of parliamentary work, the legislator excluded trusted flaggers, who will be appointed by the President of UKE from the group of applicants.

The Polish legislator has decided to introduce significant restrictions for the purposes of issuing orders to block content on the internet. First, it has significantly limited the scope of illegal content that may be subject to a blocking order. Second, it has explicitly indicated the content, data and infringements to which blocking orders will not apply (statutory exclusions).

The Polish DSA implementation draft limits the scope of illegal content that can be blocked by an order to enumerated violations of:

- the Polish Criminal Code;
- the Polish Act on Copyright;
- the Polish Act on the Protection of Health against the Consequences of Tobacco and Tobacco Products Use;
- the Polish Industrial Property Law; and
- the Polish Fiscal Penal Code.

Poland also intends to block internet domains with illegal content. An internet domain used by a website subject to an order to block illegal content will be subject to entry in the register kept by UKE, but only in the absence of effective measures that could lead to the enforcement of a blocking order.

Information from the register will automatically be forwarded to internet providers, which will be required to:

- block access to websites using the internet domain name entered in the register, free of charge, no later than 48 hours after entry into the register; and
- redirect connections, free of charge, to a website operated by UKE containing a message about the entry of the searched internet domain name into the register.

Internet providers will also restore access to websites using an internet domain name deleted from the register no later than 48 hours after the internet domain name has been deleted from the register. The new register is a solution introduced in the Polish implementation of the DSA and is an additional regulation not provided for in the DSA itself.

The Polish DSA implementation draft limits the application of blocking orders to:

- terrorist content;
- IT data and ICT services related to terrorism or espionage;
- violations of consumer rights; and
- broadcasts, videos or other transmissions regulated by the Act of 29 December 1992 on Radio and Television Broadcasting.

Removal of the block

The Polish implementation of the DSA provides that an order to remove a block may be issued by UKE or the KRRIT only at the user's request. The order will be addressed to the hosting provider, including the online platform that has determined that the user has provided information that constitutes illegal content or is inconsistent with the platform's terms and conditions.

The order to unblock the content should be issued within 14 days of receiving the user's request, and will not be enforceable if an objection is lodged with the court. It will also not be possible to make it immediately enforceable.

It is important to note, however, that the Polish legislator has not decided to limit the definition of illegal content regarding orders to unblock content that is wrongly considered illegal.

Conclusions
The legislative process in Poland has not yet been completed. On 19 December 2025, the Polish implementation of the DSA was submitted to the President. It is not known whether the President will approve the bill.

Amendment to the Polish Broadcasting Act
In December 2025, the government published a long-awaited draft amendment to the Polish Broadcasting Act. Its main purpose is to regulate the status of state-owned broadcasters and ensure stable financial resources for them (PLN2.5 billion per year), and to implement the European Media Freedom Act.

The draft bill also contains regulations affecting the operations of commercial media. The existing satellite and cable broadcasting licences are to be replaced by permits that will be more flexible for broadcasters. Furthermore, media concentrations will be subject to additional scrutiny by the media regulator – ie, the National Broadcasting Council.

The draft bill is currently at the public consultation stage. It is difficult to foresee whether the Polish President will sign the bill.

National Cybersecurity System
An important legislative change in 2026 will be the adoption of a long-awaited amendment to the Act of 5 July 2018 on the National Cybersecurity System, implementing the NIS2 Directive (Directive 2022/2555). In December 2025, the government draft bill was submitted to the lower house of the Polish parliament. The draft introduces a new division of entities governed by the Act's provisions. Instead of the existing key service operators and digital providers, the legislator introduces a division between essential and important entities.

In addition, the catalogue of economic sectors covered by the bill's provisions has been significantly expanded. The essential sectors also now include collective sewage disposal, the management of ICT services, outer space and public administrations (including units of the public finance sector, research institutes or bodies such as the National Bank of Poland or the National Health Fund). The following are also essential entities:

- electronic communications entrepreneurs that are at least medium-sized businesses;
- cybersecurity-managed services providers that are at least medium-sized businesses; and
- domain name registration service providers.

In turn, the catalogue of important sectors has been expanded to include:

- postal services;
- nuclear power investments;
- waste management;
- the chemicals sector (production, manufacturing and distribution);
- the food sector (production, processing and distribution);
- the production of other goods and equipment (medical products, computers, electronic devices, optical devices, machinery, motor vehicles and transportation equipment); and
- scientific research.

The draft also provides for the establishment of a central register of essential and important entities, which will be maintained by the competent authority for cybersecurity in the supervised sector.

Each essential and important entity will be required to implement an information security management system (ISMS) covering risk assessment and a catalogue of technical and organisational measures, including those relating to supply chain, business continuity, continuous monitoring, cryptography and multi-factor authentication. The draft also introduces a precise system for reporting serious incidents – ie, an obligation to issue an early warning within 24 hours and to submit a notification within 72 hours of detecting an incident. The draft also provides for additional information obligations towards users in the event of serious cyber threats and incidents.

Changes are also planned to the personal liability of managers of essential and important entities – eg, for failing to fulfil the obligations relating to the ISMS, training, designating contact persons, incident reporting and conducting audits. The draft expands the possibility of imposing an administrative penalty on managers of essential and important entities, and increases the maximum penalty by up to 300% of a manager's monthly salary, and up to 100% of a manager's monthly salary for public entities. The entity's manager may be a member of the board of directors, a partner in charge of the company's affairs, or an individual conducting a business activity.

An extension of the deadline for essential and important entities to implement the obligations arising from the amendment to the Act has been announced during work in parliament, as has the issuance of a Q&A intended to clarify numerous doubts regarding the understanding and application of the Act.

At the present time, it is difficult to accurately predict when parliament will adopt the new legislation. However, rapid proceedings to adopt this draft are expected, so it is likely that the adoption of the law will take place in the first or second quarter of 2026.

Consumer protection measures

The President of the OCCP continues to verify how entrepreneurs have adapted to the requirements regarding the presentation of prices on discounts (an obligation imposed by the EU Omnibus Directive). At the end of 2025, the President of the OCCP was conducting seven proceedings in which charges were brought against companies such as Temu.

Furthermore, in connection with the incorrect presentation of information about discounts, the President of the OCCP issued more than 70 soft interventions in 2025, and seven investigative proceedings are ongoing regarding bricks-and-mortar stores, including against grocery chains. According to the position of the President of the OCCP (also adopted in the judgment of the Court of Justice of the EU in the *ALDI SÜD* case (C- 330/23)), price reductions must be calculated in relation to the "prior price" – ie, the lowest price applied during at least 30 days before the reduction. A discount "in the plus", where the sale price is higher than the lowest price from those 30 days, is not a discount, and an entrepreneur who uses such communication violates the law.

The President of the OCCP draws attention to other practices that mislead consumers, such as misleading consumers about the existence of a special price benefit ("eternal promotions", constantly renewed discount codes, and countdown timers for promotions that keep resetting). Such practices are an example of so-called dark patterns – ie, the unfair use of knowledge about online buyers' behaviour to influence their choices. For misleading consumers about the existence of a special price benefit, the President of the OCCP imposed a fine of nearly PLN15 million on the owner of online stores.

The President of the OCCP also challenges the practices of platforms operating on a subscription model that allowed the platform to unilaterally change prices and other material terms of the contract without obtaining the user's active consent. If a platform operates on a subscription model in which the fee for the next period is automatically charged from the consumer's payment card linked to the account, any change in price, tariff plan or material elements of the contract must be made with the consumer's informed consent. Without such acceptance, the contract should not be renewed with changed terms. In the opinion of the President of the OCCP, such practices may lead to a violation of consumers' material interests. Currently, in investigative proceedings, the President of the OCCP is verifying the terms and conditions and practices applied by Disney+, Google (with YouTube Premium) and Adobe, for example.

The President of the OCCP increasingly resorts to allowing financial compensation for consumers; instead of merely enforcing discounts or issuing vouchers, direct refunds to those harmed are ordered. For example, the President of the OCCP has applied such measures in decisions that imposed fines for additional costs incurred by consumers related to service operations, for exceeding statutory deadlines for processing complaints, or for cancelling orders after their confirmation and delays in shipping and delivery, despite messages such as "shipping within 24 hours".

Implementation of EU Data Act

The EU Data Act regulates the sharing of data generated by connected products and related services, and the switching and exiting from data processing services, which encompasses most cloud computing services. It became fully applicable on 12 September 2025. Even though it is an EU regulation that is directly applicable in EU member states, there are some areas that require local implementation, including the level of penalties or the authorities responsible for implementing and enforcing this law. The Polish implementation is delayed; the first draft of the implementing law was published on 5 November 2025 and, as of the end of 2025, is still being processed within government.

The draft act indicates that, with respect to the product or related service data being personal data, the competent authority will be the President of the Office of Protection of Personal Data (PUODO). With respect to other product or related service data and switching and exit, the authority competent for implementation and enforcement, as well as the data co-ordinator under Article 37 of the Data Act, will be the President of the UKE; this role has previously been played by telecommunication and postal regulators.

The allocation to PUODO of the powers related to personal data does not raise concerns and follows the approach adopted in many EU countries. However, there may be doubts as to whether UKE will be able to perform its new tasks, due to its limited experience in the matter and potential conflicts of interest between the telecommunication operators and providers of data processing services, especially cloud services, which are often accused of benefitting disproportionately from telecommunication infrastructure.

The proceedings under the Data Act should, in principle, be conducted under the Polish Administrative Procedure Code. This has been seen positively as the authorities often created many exceptions from general administrative rules in particular areas of law, increasing the costs of compliance for public and private authorities and often making the enforcement of rights more complicated.

Regarding penalties, the draft law provides that, except for business entities, the maximum penalty is 4% of the turnover in the financial year preceding the year in which the penalty is imposed. However, for violations of the processing of personal data, GDPR penalties apply. With respect to the other entities (eg, public authorities), the maximum penalty is PLN100,000. An appeal of the decision to award penalties to the Administrative Court suspends the enforcement of the decision.

The draft law does not currently envisage special rules for gatekeepers, nor sanctions other than financial penalties, such as warnings. In general, the proposal may be found beneficial for business entities, especially the largest; as an example, it limits the base of calculation of penalties falling outside of the GDPR to the turnover in Poland only, while in some other jurisdictions it extends to global turnover.

The adoption of the new law is expected in 2026, but it is not a priority for the authorities.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com