POLAND

Trends and Developments

Contributed by:
Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk
Sołtysiński Kawecki & Szlęzak

Sołtysiński Kawecki & Szlęzak is one of Poland's leading full-service law firms. With more than 180 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 joined SK&S in 1998 and has been a partner since 2009. She specialises in new technologies and personal data protection, and in state aid and public procurement. Agata has advised on cloud computing for many years, especially on its deployment in the financial sector. She also advises on AI and the sharing of data generated by devices or applications, and helps in reviewing IT solutions from the privacy perspective, handling sensitive data protection requests, and complaints. Agata is a member of the European Commission's Expert Group on B2B data sharing and cloud computing contracts.

Sylwia Macura-Targosz is a senior associate at SK&S, specialising in IT, new technologies and e-commerce law. She is experienced in the field of IT system implementation projects and licensing issues, and also has expertise in personal data protection and privacy matters. Sylwia has advised in a number of IT and employment projects in which personal data was of importance. She also acts as a Data Protection Officer for certain SK&S clients, and supports entrepreneurs in proceedings conducted by the President of the Personal Data Protection Office. She is a member of the Polish New Technologies Law Association.

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk,
Sołtysiński Kawecki & Szlęzak

Aleksandra Krześniak-Sałajczyk is an associate at SK&S, and an advocate at the Warsaw Bar Association. She specialises in intellectual property cases (copyright, industrial property, combating unfair competition, IT system implementation contracts) and regulatory issues in telecommunications law and broadcasting law. Aleksandra supports entrepreneurs in proceedings conducted by Polish regulatory authorities (President of the Office of Electronic Communications, National Broadcasting Council).

Sołtysiński Kawecki & Szlęzak

Jasna 26
00-054 Warsaw
Poland

Tel: +48 22 608 70 00
Fax: +48 22 608 70 01
Email: office@skslegal.pl
Web: www.skslegal.pl

SOŁTYSIŃSKI KAWECKI SZLĘZAK

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk,
Sołtysiński Kawecki & Szlęzak

TMT in Poland: An Introduction

One of the most important events in Poland in 2023 was the parliamentary elections in October, which established a new parliament and with it new authorities in the various ministries. 2024 will see significant legislative changes in Poland, which will likely cover, in part, those bills that had not been successfully adopted in the previous year. Such projects include the draft Electronic Communications Law (implementing the European Electronic Communications Code), amendments to the Copyright and Related Rights Act (implementing the Copyright Directive) and an act implementing the Digital Services Act. Telecommunications entrepreneurs and email providers will also face new obligations to combat abuse of electronic communications under the new regulations. 2024 will also be a crucial year for cybersecurity and for further empowering consumers in their e-commerce and media activities.

Priorities of the New Minister of Digitisation

A new Minister of Digitisation and deputy ministers were appointed in December 2023, following Poland's parliamentary elections. At a press conference, the new minister presented the priorities of the Ministry of Digitisation for the coming months.

It plans to prepare a strategy for the digital development of the country, which is expected to indicate directions for further development. Legislative activities include the amendment of the law on the National Cyber Security System, which has been discussed for a long time. The last bill, prepared by the previous government, introduced additional obligations for electronic communication entrepreneurs (a new category of entities) regarding the handling of telecommunications incidents, among other changes.

The second legislative project indicated by the new minister is the adoption of the Electronic Communications Law – ie, a law implementing the European Electronic Communications Code. In other areas, the minister mentioned that programmes for the development of digital competencies for schoolchildren are to be continued.

Appointment of New Data Protection Authority

The newly appointed President of the Polish Data Protection Office (*Prezes Urzędu Ochrony Danych Osobowych*) took office on 26 January 2024. The leaving President was often criticised for limited involvement in data protection matters. The Committee of the Lower Chamber of the Polish Parliament met on 15 January 2024 to evaluate four remaining candidates to this post and provide recommendations.

In a unique development, the selection process included a public debate with the candidates for the post, which was held in mid-December 2023. Everyone agreed that the new President has to rebuild public trust in the office. The candidates also stressed that the Data Protection Office should be reorganised and that some procedural changes are needed, particularly to speed up the review of complaints, improve competences in new technologies and enhance open co-operation with other stakeholders. It also follows from the debate that there is a lack of independent supervision over the processing of personal data by the law enforcement agencies, and that this issue should be resolved urgently.

Finally, the Parliament appointed Mr Mirosław Wróblewski, a lawyer and author of many publications, who recently worked for the Polish Ombudsman, as the new President at the end of January 2024.

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk,
Sołtysiński Kawecki & Szlęzak

Cybersecurity Remains Crucial

2023 saw a continued increase in the scale of cyber-attacks. At the same time, however, the level of awareness and the effectiveness of security measures among companies and other organisations were also increasing. Subsidy programmes for public organisations that raise the level of digital protection provided additional resources to increase resilience against cyber-attacks.

In 2024, further digital development will be enhanced by the obligations imposed on public and private entities by the EU NIS 2 Directive and the EU CER Directive, which should be implemented into Polish national law by 17 October 2024.

NIS 2 Directive and CER Directive

The EU NIS 2 Directive and the EU CER Directive create a harmonised legal framework for ensuring the continuity of state-critical services and the resilience (both physical and in cyberspace) of the entities providing them. These directives will stimulate additional digital development and increase the level of security in Polish (and European) companies.

The NIS 2 Directive introduces, among other things, obligations to report incidents and to train employees in cybersecurity. One of the key challenges of the NIS 2 Directive will be to ensure that incidents are handled and reported appropriately, and that plans and procedures are in place to restore business operations and to restore data and infrastructure.

The CER Directive establishes a framework for the resilience of critical entities, including resilience strategies, risk assessments by EU member states or mechanisms for identifying critical entities.

National Cybersecurity System

Work on the National Cybersecurity System Act ("Polish Cyber Act") – aimed at ensuring cybersecurity at the national level, particularly the uninterrupted provision of essential services and digital services, and the achievement of a sufficiently high level of security among the ICT systems used to provide these services – was not completed in 2023, due to the parliamentary elections and the principle of the discontinuity of parliamentary work (when a parliament ends its mandate, it closes all the projects it has worked on and does not pass them on to the new parliament).

At the beginning of January 2024, the Ministry of Digitalisation announced the commencement of work on the Polish Cyber Act and its completion during 2024. The content of the new draft of the Polish Cyber Act is not yet known – ie, whether it will be broader than the current one and include the implementation of the NIS 2 Directive (and the CER Directive) or whether a new law (or laws) will be passed to implement these directives.

Cyber-resistance of the internet of things (IoT)

Complementary to the EU cybersecurity framework referred to above, the Cyber Resilience Act (CRA) regulation is intended to cover the security of internet-connected devices (especially IoT). The CRA will apply to all products that are directly or indirectly connected to another device or network. Exceptions apply to products for which cybersecurity requirements have already been introduced in EU legislation, such as medical devices, aircraft or vehicles.

In addition, the proposed regulation allows consumers to take cybersecurity into account when selecting and using products with digital elements – users will be able to make a conscious

choice of equipment and software with appropriate cybersecurity features.

The CRA is expected to come into force in early 2024, and manufacturers will have to apply the regulations 36 months after they come into force.

Empowering Consumers in E-Commerce and Media Activities

Additional obligations for Polish entrepreneurs when trading with consumers

The Omnibus Directive was implemented into the Polish legal system in 2023, imposing new obligations on entrepreneurs entering into contracts with consumers and aiming to increase the protection of consumers, primarily those operating in the digital world, from unfair marketing practices of entrepreneurs.

In order to facilitate the interpretation of the new rules, in May 2023 the Polish President of the Office of Competition and Consumer Protection (*Prezes Urzędu Ochrony Konkurencji i Konsumentów* – OCCP) published extensive explanations on the rules for the presentation of price reductions ("Explanations"). These Explanations provide guidance on the interpretation of the rules regarding the presentation of discounts by, inter alia, shopping platforms and price comparison sites, when using discount codes, and for participants in loyalty programmes.

However, the Explanations appear to go beyond the mere interpretation of the rules and impose new obligations on entrepreneurs that do not stem from the Omnibus Directive. However, the Explanations do not constitute a source of law and entrepreneurs are not obliged to comply with them, according to the OCCP representatives' declarations.

Prior consent for changing the terms of service subscription

The President of the OCCP recently examined the subscription terms and conditions of various services, looking first at the subscription terms and conditions of the services available as part of the Amazon Prime and Amazon Prime Video packages. In their contracts, Amazon EU and Amazon Digital UK used, among other things, procedures that allowed unilateral price changes from the new subscription period. This type of condition is particularly detrimental to customers in a situation where a payment card (debit or credit) has been assigned to the account and the operator grants itself the right to automatically charge the new amount for the next subscription period.

The President of the OCCP opined that, in such cases, material terms and conditions – including above all the changed price of the service – should not bind consumers if they do not give their informed consent to extend the subscription on new terms, and that the new price or other new material terms of the contract may be introduced from the next subscription period only with the consumer's prior consent. Amazon EU and Amazon Digital UK have complied with the OCCP's position and amended their contractual terms.

The OCCP is currently investigating subscription services offered by Apple, Disney+, Google (with YouTube Premium), HBO Max, Microsoft (with GamePass), Netflix and Sony (with PlayStation Plus), and any price changes made by them.

Increased regulatory control over dark patterns

The President of the OCCP began to combat the use of "dark patterns" (ie, the practice of taking unfair advantage of knowledge about

consumers' online behaviour to influence their purchasing decisions) by entrepreneurs, and has imposed financial penalties on entrepreneurs who engage in such prohibited market practices. The President of the OCCP recognised, inter alia, the following practices as examples of dark patterns:

- the automatic addition of a product to the shopping cart without the consumer's knowledge so that, when placing an order, the consumer may overlook excess items and make unplanned purchases;
- inducing customers to subscribe for a paid subscription without their knowledge through appropriate use of the website interface (the button for online ordering was improperly labelled); and
- use (next to the offer) of a countdown timer that counts down the hours until the end of the discount; each day the countdown resumes for the next alleged promotion. The countdown timer encouraged quick purchases, which persuaded consumers to take advantage of the same offers each day.

Further action by the President of the OCCP in this area can be expected in 2024.

Influencer marketing – Polish regulator says "check"

Since the end of 2021, the OCCP has been drawing attention to the need to strengthen social media control in the area of advertising content presented by influencers, particularly in the area of medical products, dietary supplements, medicines, gambling or alcohol, the advertising and promotion of which is restricted by law or completely prohibited in Poland. The "Recommendations pertaining to the tagging of advertising content by influencers in social media" announced at the end of 2022 by the President of the OCCP, indicating good practices in this area, and the large-scale educational campaigns carried out by the OCCP have contributed to raising awareness of influencers and consumers in this area.

However, the scale of influencer marketing and the mislabelling of advertising collaborations by influencers in social media is still very high. Consequently, after two years of informing and building awareness about the rules of advertising co-operation between entrepreneurs and influencers, the President of the OCCP is moving to enforcement, imposing fines of more than PLN5 million in 2023 on a dietary supplement manufacturer and three influencers co-operating with it for using improperly labelled influencer advertising in social media. On behalf of the manufacturer and in accordance with its instructions, the influencers were to post on their profiles posts and accounts in which, under the guise of neutral information, they recommended certain products without sufficiently disclosing that it was an advertisement – such crypto-advertising became the reason for the OCCP's intervention.

Proceedings have also been initiated against three well-known celebrity influencers, and there have been several procedural penalties (for the lack of co-operation with the authority during the proceedings). However, the President of the OCCP has not yet had the last word, and further actions against mislabelled influencer advertising on social media can be expected in 2024.

A further step towards cleaning up the social media advertising market is the so-called round table meeting initiated by the OCCP, which brought together representatives of social media platforms (Meta, Google and TikTok), the advertising industry and universities to discuss faster and more effective elimination of unlawful adver-

tising and improved procedures for the supervision of advertising content that may infringe the law.

Development of e-services in public administration

The field of electronic administrative services will clearly develop in 2024. At the end of the year, Poland will face the launch of the e-Delivery system, which will make it easier for citizens to contact the administration. The National e-Invoice System, which was also due to be launched this year, will probably not be launched until 2025.

With the development of e-government, investments in cloud solutions in public administration are also likely to increase.

New Electronic Communications Law

The long-awaited implementation into the Polish legal system of the European Electronic Communications Code (Directive (EU) 2018/1972 of 11 December 2018) was not completed in 2023. The proposed Electronic Communications Law and the Law Introducing the Electronic Communications Law have passed the stage of government work and have been referred to the *Sejm* (lower house of parliament) for further proceedings. However, due to a number of controversies and reported amendments, both bills were withdrawn from the *Sejm* in April 2023.

Critical comments included provisions on "Must carry must offer" (MCMO) regulations (MCMO is the obligation put on certain broadcasters to make their channels available (must offer) to operators that distribute TV channels; the operators, in turn, are obliged (must carry) to distribute these channels or pay a fine) and the obligation of instant messaging providers to store their users' data (Messenger, WhatsApp) to the same extent as telecommunications entrepreneurs do.

Since the withdrawal of the bills from the *Sejm*, no new projects have been published.

According to announcements made by the new Minister of Digitisation in January 2024, a draft bill – the Electronic Communications Law – will be prepared by the Ministry of Digitisation in the first quarter of 2024. No information is yet available on the extent to which the new bill will coincide with the previous version from last year.

Implementation of the Copyright Directive

The implementation of the Copyright Directive (Directive (EU) 2017/790 of 17 April 2019 on copyright and related rights in the Digital Single Market) was also not completed in 2023. Due to the principle of the discontinuation of parliamentary work when a parliament ends its term of office, the bill implementing the Copyright Directive, which was to significantly amend the Act of 4 February 1994 on Copyright and Related Rights, is unlikely to be further processed following the election of the new parliament in Q4 2023.

No information has yet been provided on when the new draft law implementing the Copyright Directive will be published, nor on the extent to which the draft will differ from the most recent version from last year. An issue that continues to stir up a lot of controversy in the Polish market is the planned regulation of the payment of royalties to creators from online streaming.

The DSA and Changes in the Provision of Electronic Services

In January 2024, the Minister of Digitisation published an invitation to participate in consultations on the assumptions of the bill amending the law on the provision of electronic services and some other laws that implement the DSA – ie, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Sin-

gle Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). The bill itself has not yet been published; only the scope of issues that the bill is expected to regulate has been announced. The co-ordinator for digital services in Poland is to be the President of the Office of Electronic Communications (President of the OEC), and part of the duties related to the enforcement of the DSA will be carried out by the competent authorities – namely, the President of the OCCP.

The bill is to address issues delegated to member states for regulation at the national level, including:

- defining the scope of competence of the President of the OEC and the President of the OCCP in connection with the performance of their tasks;
- the conduct of investigations, inspections and proceedings before the competent authorities related to the violation by providers of intermediary services of their obligations under the DSA;
- the procedural aspects of imposing penalties on providers of intermediary services (with the maximum amount of the penalties themselves resulting directly from Article 52 of the DSA);
- the procedural aspects of filing complaints against providers of intermediary services, referred to in Article 53 of the DSA;
- the granting of "vetted researcher" status as referred to in Article 40(8) of the DSA;
- the granting of trusted whistle-blower status ("trusted flaggers") as referred to in Article 22 of the DSA;
- the certification of out-of-court dispute resolution bodies;
- the adaptation of the requirements for orders to take action against illegal content and orders to provide information; and
- rules on civil liability and proceedings before the courts, in the event of a claim for damages for violation of the DSA.

A number of entities (including chambers of commerce, NGOs and regulatory authorities) participated in the consultations. The Ministry of Digitisation has not yet indicated specifically when the bill will be drafted and published.

New Law: Combatting Abuse in Electronic Communications

Most of the provisions of the Act of 28 July 2023 on Combating Abuse in Electronic Communications came into force in September 2023. The law implements Article 97 (2) of the EUropean Electronic Communications Code into the national legal order, according to which member states should ensure that national regulatory authorities may, in justified cases, require providers of public electronic communications networks or publicly available electronic communications services to block access to numbers or services on a case-by-case basis. The purpose of the new legislation is to increase user protection against harmful activities carried out through communication technologies, including phishing, smishing distribution, email spoofing or CLI spoofing (caller ID spoofing). The law imposes new obligations on telecommunications entrepreneurs and email service providers, and also on CSIRT NASK (the Computer Security Incident Response Team at National Research Institute) and public entities.

New definition: abuse in electronic communications

According to the Act, abuse in electronic communication is the provision or use of a telecommunications service or the use of telecommunications devices contrary to their purpose or the law. The purpose or effect of such action is to

cause harm to the telecommunications entrepreneur or end user, or to achieve undue benefits for the abuser of electronic communications or another person/entity. Examples of such abuses (phishing, etc) are indicated above, with this being an open catalogue.

New obligations fortelecommunications entrepreneurs and email service providers

Telecommunications entrepreneurs are obliged to block SMS messages containing content with a message pattern that CSIRT NASK deems to be smishing. They may also block SMS or MMS messages other than those matching the template developed by CSIRT NASK, using a system that allows the automatic identification of such messages for smishing. When it comes to combating CLI spoofing, the President of the Office of Electronic Communications will publish a list of numbers of institutions (eg, banks, insurance companies) that are used exclusively to receive calls. The numbers concerned are hotline numbers from which the institutions themselves generally do not make calls, but at the same time these numbers are easy to find online and are often used by fraudsters to impersonate these institutions. Telecommunications entrepreneurs are required to either conceal number identification or block voice calls that are intended to impersonate another person or institution. In terms of protection against fraudulent websites, CSIRT NASK is to maintain a list of warnings against fraudulent websites. The telecommunications entrepreneur will be able to block users from accessing websites that are included on the warning list.

Email service providers that provide services to at least 500,000 users or public entities are required to use the following mechanisms, which are designed to prevent the use of a domain to impersonate its owner or modify messages sent from it:

- SPF (Sender Policy Framework);
- DMARC (Domain-based Message Authentication Reporting and Conformance); and
- DKIM (DomainKeys Identified Mail).

Implementation of the Data Act

EU Regulation 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) was finally published on 22 December 2023 and entered into force on 11 January 2024. It will become applicable from 12 September 2025.

The Data Act will include rules on:

- the mandatory sharing to users or third parties of non-personal data generated by products connected to the internet and related services;
- facilitating switching between cloud service providers;
- data holders making data available to public sector bodies, the Commission, the European Central Bank and Union bodies where such data is needed in exceptional cases for the performance of a specific task carried out in the public interest; and
- introducing safeguards against unlawful third-party access to non-personal data and the development of interoperability standards.

Before the Data Act starts to apply, the European Commission and member states should implement certain steps. For member states, these steps include the following:

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk,
Sołtysiński Kawecki & Szlęzak

- Designating competent authorities to be responsible for the application and enforcement of the Data Act. In Poland, this authority is most likely to be the current telecommunication and postal regulator (*Prezes Urzędu Komunikacji Elektronicznej*), provided that the monitoring of the application of the Data Act with respect to personal data will be performed by the current personal data regulator (*Prezes Urzędu Ochrony Danych Osobowych*).
- Ensuring that the competent authorities have the appropriate tasks and powers listed in Article 37 Section 5 of the Data Act. Therefore, as in the case of the GDPR or the Data Services Act, the Polish authorities would adopt the local implementing legislation. The draft of such legislation has not yet been proposed.