03

Issue No.

TKP LEGAL NEWSLETTER

Warsaw/Poland

April 2021

In this issue:

WHAT'S NEW?
LEGAL NEWS FROM POLAND

MORE ABOUT

- Competition & Antitrust
- Cybersecurity
- Data protection
- Employment
- Fintech
- Intelectual Property
- Internet & Media
- Information Technology
- Life Science
- Litigation
- Public Procurement

Traple
Konarski
Podrecki
& Partners

TKP

LEGAL NEWS
Poland

LEGISLATIVE DEVELOPMENTS

POLISH OFFSHORE WIND ACT NOW IN FORCE

On February 18, 2021, the Act on Promoting Electricity Generation in Offshore Wind Farms, (the Offshore Wind Act) came into force.

The purpose of the act is to realize the potential of offshore wind energy in the Baltic Sea and to create a legal framework that will support all entities interested in the development of the offshore wind energy sector in Poland.

The main elements of the act include a two-phase support system, streamlining of administrative procedures, rules for the connection of generators to the power grid, the regulation of power output from offshore wind farms, and the development of a local supply chain.

The Act of 17 December 2020 on the Promotion of Electricity Generation in Offshore Wind Farms
(Journal of Laws. 2021 item 234)

READ MORE

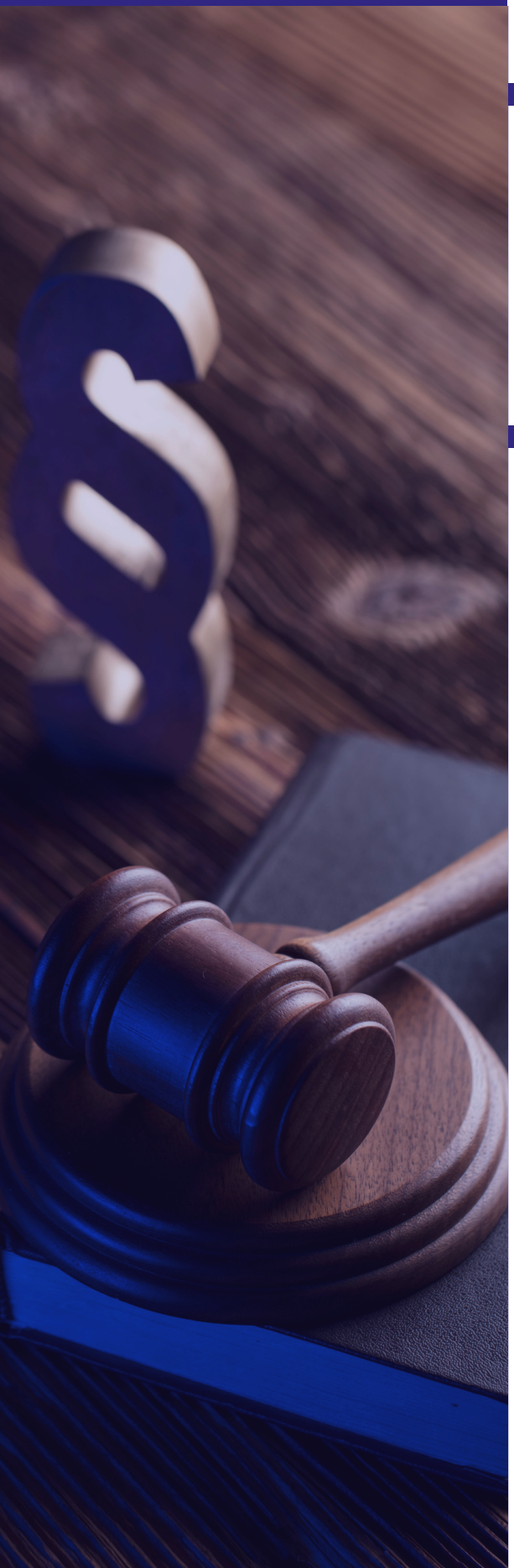
ACT EXPANDING THE USE OF LAND FOR HOUSING DEVELOPMENT

As of April 1, the requirements for acquiring communal properties for investment purposes will change.
The act defines the rules on sale of communal real estate, and incorporation of the price of premises or buildings into the price when selling communal real estate.

The Act of 16 December 2020 on the Inclusion of the Price of Premises or Buildings in the Price when Selling Communal Real Estate.
(Journal of Laws. 2021 item 223)

READ MORE

LEGAL NEWS
Poland



PLANS FOR AMENDMENTS TO THE LAW

LEGAL CHANGES REGARDING E-SCOOTERS

An amendment to the Road Traffic Law has been passed, regulating the status of e-scooters and personal transport devices, such as e-skateboards. Users of these devices will have to give way to pedestrians on sidewalks, and will not be allowed to ride on a road where the speed limit is higher than 30 km/h. There will also be restrictions for children.

READ MORE

CHANGES IN ENERGY INVESTMENT REGULATIONS

Amendments to the laws regulating and streamlining investments in undertakings necessary to ensure national energy security have been adopted by the Sejm. The amendment is designed to ensure stability and reliability of power consumption by electricity consumers and the supply of gaseous and liquid fuels. The bill provides among other things for the participation of transmission system operators in the planning process for the enactment of local spatial development plans and decisions on the location of public purpose investments.

Government bill to amend the laws regulating the preparation and implementation of key investments in strategic energy infrastructure

READ MORE

LEGAL NEWS
Poland

CASES AND JUDGEMENTS

PUBLICATION AND DISTRIBUTION OF ENTIRE BOOK PROHIBITED IN UNPRECEDENTED JUDGMENT

In a judgment dated January 29, 2021, the District Court in Warsaw ruled that the author of a book entitled "The Secret Life of Butterflies" presented false information about a mountaineering expedition and about the moral and professional qualifications of the expedition's participants.

This is an unprecedented judgement in Poland as it prohibits the publication and distribution of an entire book.

The judgment is not final and the statement of reasons for the judgment has not yet been published.

READ MORE

DISPUTE OVER COPYRIGHT TO A CARTOON DEPICTING THE ADVENTURES OF REKSIO

The District Court in Bielsko-Biała ruled on February 11, 2021 that the sole owner of copyright to the cult Polish animated character of Reksio the dog is the cartoon production studio Studio Filmów Rysunkowych, based in Bielsko-Biała.

The judgment is not final and the statement of reasons for the judgment has not yet been published.

READ MORE

RIGHT OF ACCESS AND AN URBAN COMPLEX REGISTERED AS AN HISTORIC MONUMENT

In a resolution dated February 26, 2021 (case III CZP 21/20), the Supreme Court held that establishment of right of access on real property listed as an historical urban layout does not require a permit from the conservator.

READ MORE

IMPLEMENTATION OF THE ECN+ DIRECTIVE: THE POLISH WAY

Author: Katarzyna Menszig-Wiese, PhD, LL.M, Attorney-at-law

Shortly before the deadline for the implementation of EU Directive 2019/1, aimed at empowering competition authorities to be more effective enforcers, the Polish legislator took formal steps to amend national legislation accordingly. It comes as little surprise that the competition authority, which is responsible for the proposal for the amendment, grabbed the opportunity to make some changes which go beyond the requirements under the EU act.

National competition authorities are required to apply art. 101 and 102 of the Treaty on the Functioning of the EU, where an anticompetitive practice might have an effect on trade between member states. A few years ago, it was rightly observed that significant differences between enforcement toolkits might impede proper enforcement of EU competition law. In order to address the issue, the "ECN+ directive" was adopted with a view to achieving an EU-wide standard.

The recently released proposal for amendment of the Polish Act on Competition and Consumer Protection goes further than proscribed in the directive. The provisions based on the directive are namely to be applied not only to cases of application of the Treaty by the Polish competition authority, but also to infringement of Polish law. This begs the question if, at times, severe responsibility rules that ensue from the directive are proportionate in cases where the proper functioning of the internal market is not at risk. The best example is probably the way fines are to be calculated. The directive says that the maximum level of fines for infringement of competition law shall be determined in proportion to the total worldwide turnover of an undertaking. This might be appropriate where the infringement has a vast negative impact on competition throughout the EU, but less so in exclusively local cases. The Polish legislator also plans to extend the individual liability of managers of undertakings – a topic not covered by the ECN+ directive. Where an undertaking commits an infringement of competition law and is subject to the decisive influence of another undertaking, a manager of the undertaking which exerts the influence shall also face fines.

The legislative process is still in progress. However, as the deadline for implementation has now expired, it could be concluded pretty quickly.

CLOUD PROCESSING SERVICES PROVIDERS UNDER POLISH LAW – CAUSE FOR MAJOR CONCERN REGARDING REGULATION?

Author: Agnieszka Wachowska attorney-at-law, Joanna Jastrząb, attorney at law

There is some concern among Polish businesses regarding the Act on the National Cybersecurity System, which transposes the Directive on Security of Network and Information Systems (NIS Directive). Doubts arise in particular regarding the group of entities that are subject to the act, above all cloud processing services providers. It is unclear under the act whether it applies to every firm providing services of that kind, even if the services it provides are solely for internal purposes, including for its own capital group.

This is due to the wording of the definition of *cloud processing* services in the Act on the National Cybersecurity System, which is *a service through which a scalable and flexible pool of shareable computing resources by multiple users can be accessed*. This is aligned with the NIS Directive, although the directive does not mention multiple users in the definition. This phrase is used in indent 17.

This wording may cause interpretation complications due to the provisions not specifying what is meant by *multiple* (the specific number denoted by the word *multiple*) or *users* (does this mean customers of digital service providers, or perhaps end users that use the cloud directly, such as a customer's employees or customer's business counterpart?). In addition, there are no guidelines of any kind from the authority competent for cybersecurity issues with regard to these issues.

These concerns mean that it is difficult to determine in advance whether a company provides cloud processing services as defined in the Act on the National Cybersecurity System. This applies in particular to those entities that provide services solely within their capital group or for a small number of customers. In these cases, it cannot be ruled out that they will have an obligation to comply with requirements under the Act on the National Cybersecurity System, if they have their registered office in Poland and are not micro- or small enterprises. These cases need to be evaluated on a case-by-case basis according to the pertinent facts.

NOTIFYING A SUPERVISORY AUTHORITY OF A DATA BREACH – DECISION OF THE POLISH DPA

Authors: Katarzyna Syska, Attorney-at-law and Iga Małobęcka-Szwast, PhD, LL.M.

A recent decision of the Polish data protection authority (DPA) shows that failure to report a data breach to the DPA could result in an administrative fine.

Facts of the case

In the case in question, an e-mail with an unencrypted attachment containing personal data of several hundred people was sent to an unauthorized recipient. The recipient reported this confidentiality breach to the DPA. The DPA investigated, and asked the company (being the controller in this case) to clarify the circumstances of the incident, provide an analysis of the incident, and assess whether there was a requirement to report the breach under art. 33 GDPR.The company explained that it had conducted an assessment of the risk to the rights and freedoms of natural persons, which led it to the conclusion that a breach was unlikely to result in such a risk, and therefore it was not required to notify the DPA of the breach.It also argued that due to prompt action, and a declaration by the unauthorized recipient that he had permanently destroyed the data he was not authorized to receive, the risk of adverse effects of this event for data subjects had been eliminated.The DPA disagreed and found that the company was required to report the breach in line with art. 33 GDPR. Despite the fact that the DPA informed the company of its standpoint during the proceedings, the company did not perform the notification until the date of the DPA's decision.
The DPA fined the company PLN 136,000 (around EUR 29,500). When determining the amount of the administrative fine, the DPA took into account mitigating circumstances, i.e. actions taken by the controller to minimize the harm suffered by data subjects.

Key takeaways

Recent decisions by the Polish DPA show quite a stringent approach towards the obligation to report a data breach to the DPA. We therefore have the following recommendations:

- to notify the DPA, unless it is clear that the data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
- to document data breaches, including the circumstances of the breach, the effects (in particular with regard to the level of the risk involved for data subjects) and the remedial action taken;
- to comprehensively clarify the reasons for the delay if the notification is submitted 72 hours after the breach is discovered;
- to cooperate with the DPA during the investigation and respond to the DPA's questions without undue delay;
- to take immediate action to minimize the damage suffered by data subjects.

MORE ABOUT Employment

EU - EQUAL PAY FOR EQUAL WORK?

Author: Paweł Krzykowski, Attorney-at-law, Partner BKB and Łukasz Łaguna, Trainee attorney-at-law

On March 4, 2021, the European Commission presented a proposal on pay transparency, with the aim of ensuring equal pay for men and women for equal work across the EU. The proposal aims to increase transparency in the pay structure and reduce the pay gap between men and women.

It sets out pay transparency measures, such as informing job applicants about pay, the right to information about the level of pay of employees doing the same job, and requiring large companies to report on the gender pay gap.

Employers will not be able to ask job applicants for information about their past salaries, and will have to make anonymized salary data available to employees upon request. Employees will be entitled to compensation for pay discrimination.

In addition, employers with 250 or more employees will have to publish information on the pay gap between female and male employees in their companies. For internal purposes, they should also make available information on the pay gap between female and male employees by categories of employees who perform the same work or work of equal value.

Consequently, if reports reveal a gender pay gap of 5 percent or more and the employer cannot cite gender-neutral factors justifying the difference , the employer will have to conduct a pay assessment in cooperation with employee representatives.

From a practical point of view, the question of the burden of proof under the proposed directive is very important. In the case of pay discrimination on the basis of gender, if the employer has not fulfilled its obligations to ensure pay transparency, the burden is on the employer to prove that there has been no discrimination, and the employee does not even have to provide evidence of discrimination.

As announced, Member States will be required to set the penalties applicable in the event of a breach of the principle of equal pay for men and women for equal work. While Member States are free to set specific amounts, the proposal for the Directive requires the penalties to be effective, proportionate and dissuasive.

The proposal will be submitted to the European Parliament and the Council for approval. Once it has been approved, Member States will have two years to transpose the Directive into national law.

The UK has already introduced gender pay gap regulations. In the UK, the gender pay gap among full-time employees in April 2020 was 7.4%, down from 9.0% in April 2019 (data from the ASHE and LFS). In the UK, the gender pay gap among all employees was 15.5% in 2020, down from 17.4% in 2019.

The new European regulations may force many employers in the Member States to review their salary and remuneration schemes in the context of transparency and equal treatment. New rules would also significantly change recruitment processes (disclosure of salary to applicants, a rule that it is not permitted to ask about previous remuneration).

BKB | BARAN KSIĄŻEK BIGAJ

PROPOSAL FOR AMENDMENTS TO LAW REGARDING SMALL PAYMENT INSTITUTIONS

Author: Jan Byrski, PhD, Habil., Cracow University of Economics Professor, Attorney-at-law, Partner and Karol Juraszczyk, Attoreny-at-law

The Polish Ministry of Finance has produced a proposal for an amendment to the Act on Payment Services, which is now being submitted for consultations. One of the proposed amendments concerns the activities of small payment institutions (SPI) with regard to AML compliance and notification obligations towards the Polish Financial Supervision Authority.

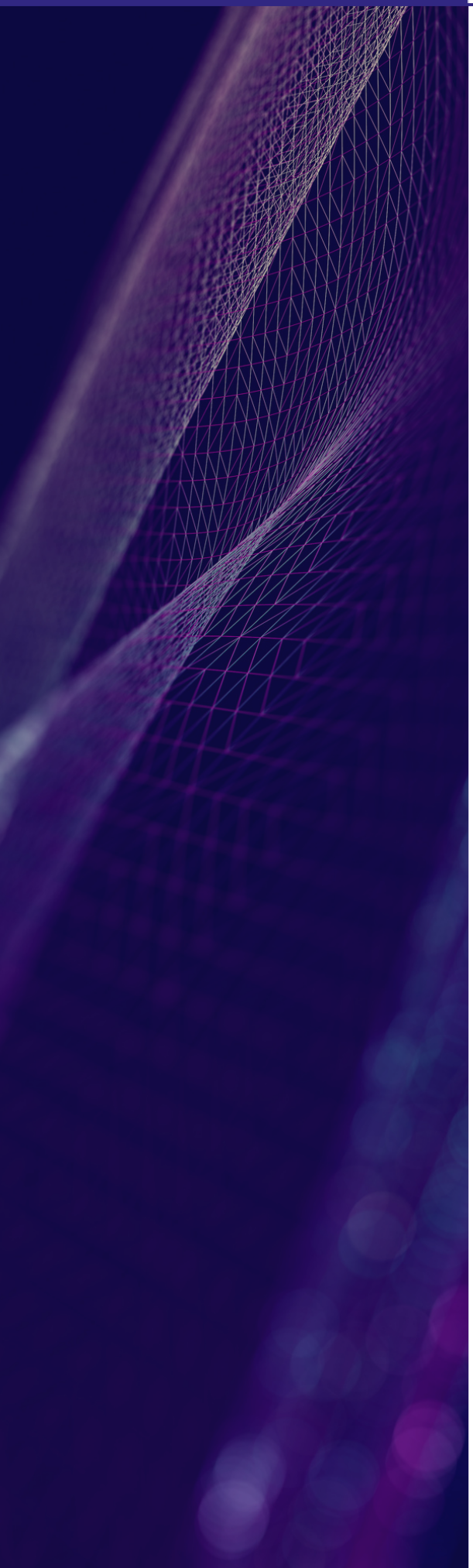
Under the current Act on Payment Services in Poland, payment services may be provided in the form of an SPI, due to an exemption that member states can apply in their national laws under article 32 of Directive (EU) 2015/2366 of the European Parliament and of the Council (PSD2). Under article 32, member states may introduce, in their national legal systems, an additional type of payment service provider that is less stringently regulated, while certain restrictions will continue to apply to business operations of that kind, for instance:

- the payment services provided by the SPI do not include payment initiation services (PIS) and account information services (AIS);
- the monthly average value of transactions executed in the preceding 12 months may not exceed EUR 1.5 m (under PSD2 this limit can be set at EUR 3 m);
- small payment institutions may only operate within Poland.

An SPI has become a popular form of activity among firms in the FinTech sector that launch payment services. To date, more than 90 firms of this kind have been registered with the Polish Financial Supervision Authority. When the thresholds described above are exceeded, an SPI may apply for a license to provide services as a payment institution. An SPI may continue to operate until the application is reviewed, and is not required to observe the thresholds described above.

Under the legislative proposal of 11 January 2021, SPIs will be subject to the requirement to submit to the Polish Financial Supervision Authority, when applying to be registered as a SPI, information regarding the AML compliance procedures and information concerning any other activity (hybrid small payment institution). The amendments described above are aligned with a certain shift in the approach taken by the Polish Financial Supervision Authority to entities of this kind, and with a policy of more extensive financial regulation of these entities, even during the registration proceedings.

The changes envisaged in the proposal also include further limits on transactions effected by payment service offices (firms only authorized to provide money transfer services), while for these entities, the requirements and regulatory obligations will be eased.



WILL POLISH COPYRIGHT CHANGE DIRECTION? WARSAW APPEAL COURT DECISION

Author: Anna Sokołowska-Ławniczak, PhD, Patent and trademark attorney, Partner

Polskie Koleje Państwowe (PKP S.A.) conducted an advertising campaign to promote its services on various posters, leaflets, banners, and billboards, using a slogan taken from Polish song.

The plaintiff, author of the lyrics of the well-known song *Remedium*, claimed that PKP had used part of the song in question, and that the defendant was in breach of the author's right to decide how the work was used and disposed of. The plaintiff also stated that the modification of the words were detrimental to the form and content of the artistic work.

The regional court dismissed the lawsuit, finding that a single phrase in the lyrics of a song is not protected under copyright law, remarking, among other things, that the phrase in question did not have any original features and thus was not subject to protection.

On the other hand, the court of second instance – the Warsaw Appeal Court, found in favor of the plaintiff in a judgment of 17 July 2020 (case VI ACa 666/18). The Appeal Court stated in the statement of reasons for the judgment that use of even a short segment of the lyrics of a word and musical work might be an infringement of copyright. The court stated that when reviewing the issue of infringement, the focus should always be not whether a particular phrase which is part of a larger work exists separately as an artistic work in the meaning of copyright law, but whether that phrase is an essential element of the whole work from which it is taken, and whether it reflects its original and unique nature and demonstrates to the listener those elements that express the intellectual creativity of the author of the entire work.

The court found that the borrowing and modifying by the defendant of the phrase for advertising purposes was a reference to the song *Remedium*, and that the reference was immediate and evident to any listener. In this case, therefore, the issue was not description in an advertisement of the quite mundane action of getting on a train to with no particular destination, but intentional reference to the popularity of the song and the pleasant associations and memories it evokes for listeners.

PROPOSAL FOR LEGISLATION IMPLEMENTING THE AUDIOVISUAL MEDIA SERVICES DIRECTIVE

Author: Michał Matysiak, Associate

The Polish government is finalising work on a proposal to amend the Broadcasting Act and the Cinematography Act, implementing the Audiovisual Media Services Directive (Directive 2010/13/EU - AVMSD). The new regulations will apply to "providers of video-entertainment platforms established in the territory of the Republic of Poland" (article 1a(1) of the bill).

Under the proposal, video platform providers would be required to provide basic information about their operations (e.g. name, registered office, or contact details) and to specify the National Broadcasting Council (KRRiT) as the competent authority in matters related to video platform providers. Under article 47o(1) of the bill, before a video platform service can be provided, it must be registered with the KRRiT.

Under article 28 of the AVMSD, video platform providers are required to take measures to protect viewers from harmful content by creating and operating effective technical safeguards (implemented in article 47p of the bill).

A video-sharing platform provider is required to comply with the obligations set out in the Act on Provision of Electronic Services, including drawing up terms of service (article 8 of the Act on Provision of Electronic Services). Article 47s of the bill requires the terms of service to provide for an additional obligation, which is to specify rules for qualifying and labelling programmes (videos) that pose a risk to minors and for placing commercial messages in programmes (videos).

In comparison with the amendment of the AVMSD, the bill goes further to regulate the issue of removal of harmful content (article 47l). According to article 47t(11), the provider of a video-sharing platform is required to provide its users with transparent and user-friendly mechanisms for reporting content placed on the video-sharing platform that contravenes the harmful content requirements under the new legislation. The activities of the platform provider will be monitored by the KRRiT - in particular, a user whose content has been blocked will be able to submit a complaint to the KRRiT (article 47u(4)).

IS DECOMPILATION PERMITTED WHEN NECESSARY TO CORRECT ERRORS, AND IN WHAT CIRCUMSTANCES? FINDINGS IN THE ADVOCATE GENERAL'S OPINION IN CASE C 13/20 TOP SYSTEM S.A. OF 10 MARCH 2021.

Author: Agnieszka Wachowska, Attorney-at-law, Partner

The Advocate General's opinion

On 10 March 2021, the Advocate General issued an opinion in a case of major significance for the IT world, Top System SA. v. État belge (C 13/20).

The main legal issues

The main legal dispute referred to the Advocate General concerned Council Directive 91/250/EEC, namely article 5(1) of that directive, and whether, as that article permits activities described in article 4(a) and (b) of the directive, it also permits software decompilation, meaning transformation of the software from the form of binary code into source code, given that decompilation is regulated separately under article 6 of Council Directive 91/250/EEC. This identified legal issue has practical implications – **is decompilation of software permitted in order for an authorized purchaser to use the software for the purpose for which it is intended, including correction of errors?**

Another question is whether, if decompilation in this way is ruled permissible for the purpose of correcting errors, the restrictions under article 6 of Council Directive 91/250/EEC apply, and subject to what requirements.

Arguments and findings in the Advocate General's opinion

The key findings in the Advocate General's opinion are as follows:

1. Software decompilation to correct software errors can be prohibited effectively in a licensing agreement;
2. Unless prohibited in the agreement, software decompilation is possible under article 5(1) of Directive 91/250 (transposed into Polish law in article 75(1) of the Copyright Law) for the purpose of correcting software errors, provided that decompilation is necessary in order to use the software in a normal way;
3. Decompilation to correct errors is possible, subject to the following premises:

    - decompilation is performed by an authorized purchaser;
    - decompilation is performed solely to correct errors that cause faulty operation and prevent the program being used for the intended purpose, while the term 'error' should be interpreted in a narrow sense;
    - no modification or upgrade of the program constitutes correction of errors, and no modification or upgrade can be performed under article 5(1) of Directive 91/250 (article 75(1) of the Copyright Act). This means that the term 'correction of errors' is understood in a narrow sense;

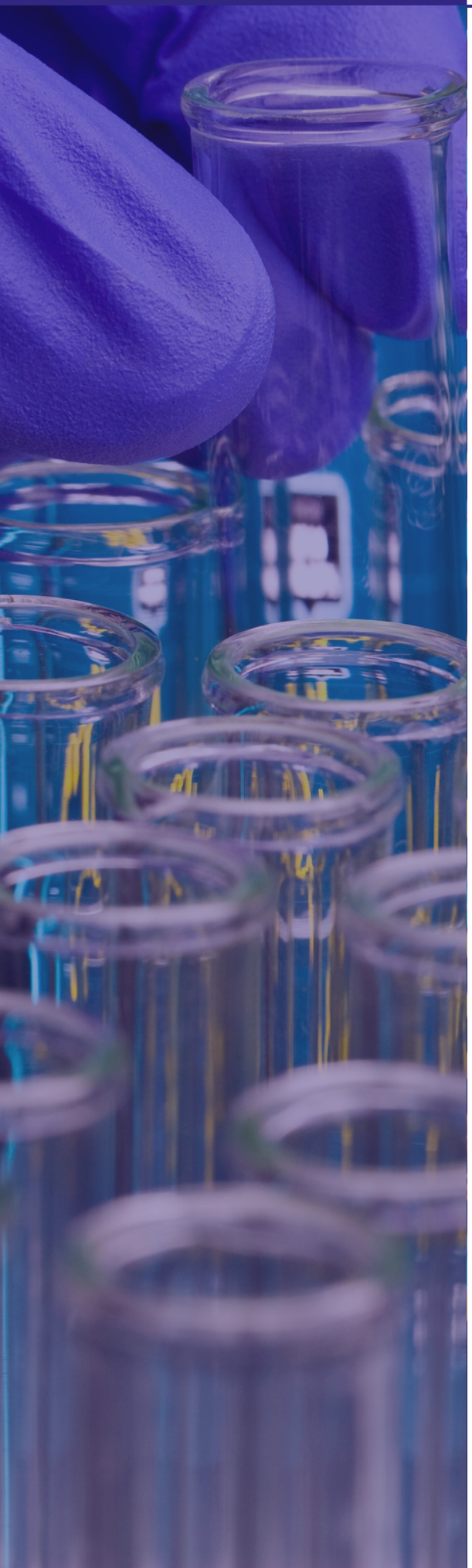
- decompilation is performed to the extent necessary to correct an error in the strict meaning of that term, but also to locate the error, and may include parts of the program that need to be modified due to the error, but may not in fact contain an error;

- when performing decompilation lawfully, the program purchaser does not have an obligation to request that the rightholder correct errors, to request access to the program's source code, or to file a lawsuit seeking a ruling ordering the rightholder to perform that or any other action.

Importantly, although this question was not expressly raised in the requests for a preliminary ruling, the Advocate General stated that correction of errors by the purchaser and software decompilation for this purpose can be prohibited in a licensing agreement.

The opinion issued by the Advocate General is not a final adjudication and is not binding for the CJEU. The final ruling will be given by the CJEU. As it concurs with the main arguments presented in the Advocate General's opinion, and in view of the authority enjoyed by the Advocate General, the CJEU can be expected to find that under article 5(1) of Directive 91/250 (transposed into Polish law in article 75(1) of the Copyright Law), it is permitted to perform decompilation of software to correct errors in software.

At the same time, the most interesting issue, with the greatest implications for IT-related transactions, is whether, in its judgment, the CJEU will address the issue of whether this right can be completely excluded contractually, and whether it concurs with the definitive and slightly more controversial standpoint of the Advocate General, that software decompilation to correct software errors can be prohibited effectively contractually.



BETWEEN PROTECTION OF CONFIDENTIAL INFORMATION AND TRANSPARENCY OF REGULATORY PHARMACEUTICAL DATA

Author: Żaneta Zemła-Pacud, PhD

In a judgment of 18 December 2020 (I OSK 2377/19), the Supreme Administrative Court of Poland (NSA) revised the rules of access to pharmaceutical data submitted in the authorization procedure.

The NSA ruled that information contained in documents submitted in the medicinal product authorization procedure constitutes public information, and as such must be accessible to all, and a legal interest in obtaining such access does not have to be demonstrated. Art. 34 of the Polish Pharmaceutical Law, being the legal basis for such a request, must be interpreted broadly.

Moreover, the Supreme Administrative Court referred to the long-established CJEU case law, denying a general presumption of confidentiality of information enclosed in pharmaceutical registration documents. The court also cited soft law documents: the European Ombudsman's decision of 19 May 2010 and the EMA's CCI Guidelines that followed the decision. Finally, the court referred to art. 37(4) of Regulation 536/2014 on clinical trials, not in force yet, and to the Proactive Publication Policy implemented by the EMA. According to these documents, reports from clinical trials are to be publicly available once the medicinal product is authorized. Thus, essential parts of the registration dossier are to be proactively made public and they cannot as a whole be deemed trade secrets.

The court mentioned the CJEU judgments relevant for the issue in question: T-235/15 Pari Pharma, T-718/15 PTC Therapeutics International Ltd, and T-729/15 MSD Animal Health Innovation. The NSA did not however consider whether any information requested in the case at hand could be protected as a trade secret. The case has been returned to the court of first instance for reexamination according to the newly interpreted rules.

The judgment clearly leans towards the principle of transparency of pharmaceutical documentation submitted to the Polish medicinal agency. This approach, being in conformity with values and objectives proclaimed in the pending regulation on clinical trials, is also of great importance in the context of the Covid19 pandemic and an urgent need to enforce open science mechanisms on an international scale.

HOW TO PROTECT TRADE SECRETS DURING LITIGATION IN POLAND

Author: Beata Matusiewicz-Kulig, Attorney-at-law, Partner

Trade secrets often determine the true value of a business and its position on the market. In litigation cases before common courts in Poland in which trade secrets might be disclosed, it is important to be informed about the laws in effect in Poland in this regard. This is because businesses often consider trade secrets to be an asset that takes priority over claims, and will not risk disclosure of trade secrets in the course of litigation. The general solutions in effect in civil procedure in Poland, that might relate or directly apply to aspects of disclosure of trade secrets during litigation, are discussed below.

In this regard, the general laws on civil procedure in Poland are discussed that are applicable in any court litigation case, including a commercial case (between business undertakings), as well as the specific solutions for separate proceedings in intellectual property cases, concerning for instance disputes over protection of trade secrets. Separate provisions on protection of trade secrets in court proceedings also apply in Poland with regard to competition and consumer protection and unfair practices that exploit contractual advantage (article 479(28) et seq. of the Civil Procedure Code - CPC) They also apply in cases concerning redress for damage caused due to violation of competition laws (the Act on Remedy of Damage due to Breach of Competition Law). These separate areas of regulation are not dealt with below in this article.

Trade secrets during a trial – general regulation

Non-public hearings

In civil cases in Poland, a party that believes that a trade secret might be disclosed during court hearings has a right to request that the court review the case *in camera*, so that the public are not admitted (article 153 (1)§ 1 of the Civil Procedure Code). The hearing is thus of course not held publicly, and therefore the parties' confidential information is protected from third parties. Due to the principle that court proceedings are held publicly in Poland, people who are not party to the dispute would be able to attend a hearing as they would be among the public. Meanwhile, this does not solve the problem of disclosure of the other party's confidential information.

When a court requires a document containing trade secrets

During a court litigation case, including in separate proceedings for commercial cases (between business undertakings), a court may require documents to be submitted that are material evidence in the case (article 248 of the CPC). A court may require this of the parties to the proceedings, or even third parties unrelated to the ongoing litigation. The issue of protecting trade secrets arises when a document required by the court contains trade secrets. The fact that those documents constitute or contain confidential commercial information is not grounds for refusing to submit the documents when required by the court. At the same time, there is currently no general regulation in civil procedure in Poland on the procedure to be followed when submitting a document required by a courtinvolves a risk of disclosure of trade secrets. One solution might be for a party or third party to refuse to submit evidence on the grounds that

disclosure of documents containing trade secrets will cause a severe and direct damage . Ultimately, a third party that is concerned about disclosure of their trade secrets in court can weigh the risks and consequences of complying or not complying with a court's requirements, as the court's penalty for compliance by a third party when a court requires disclosure is a single fine of PLN 3 000. Often, the potential losses, and other adverse market consequences for third parties of submission of a document containing trade secrets when required by a court may outweigh this. In the case of the parties, however, the only potential penalty in this situation is that this would undermine the overall assessment of the evidence in the case (article 479 of the CPC).

Trade secrets in IP litigation cases

In fact, prevention of disclosure of trade secrets during a litigation case is regulated in most detail in provisions on separate IP proceedings that came into force in Poland in July 2020. These regulations apply for instance to disputes concerning protection or breach of trade secrets, and other acts of unfair competition.

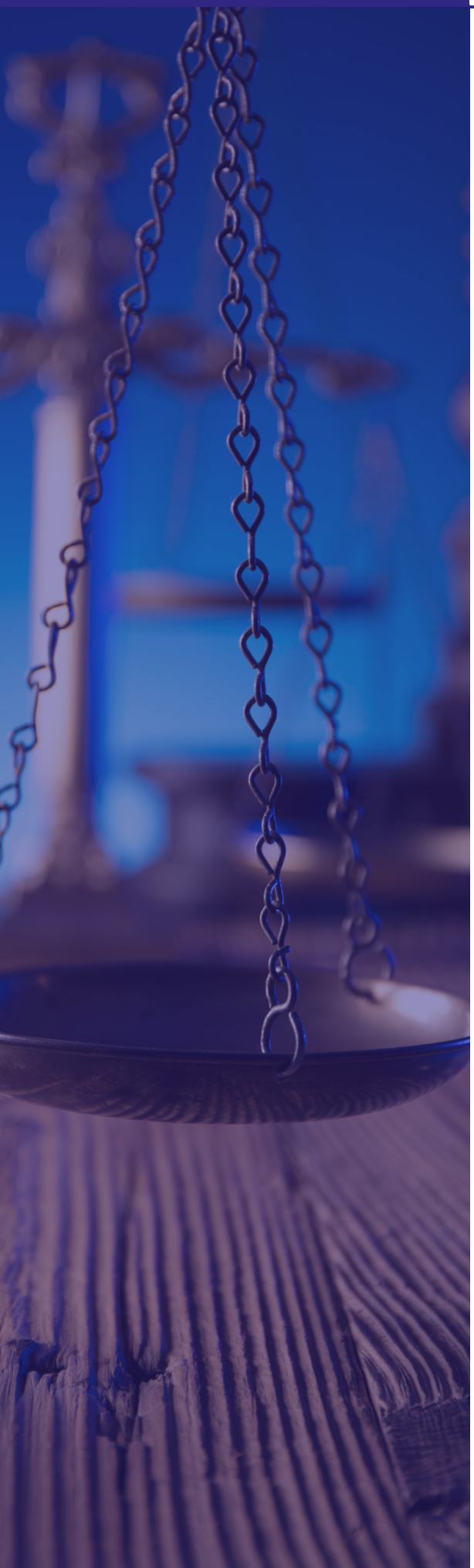
In separate proceedings in IP cases, a party wishing to defend its intellectual property rights may request that the other party be ordered to disclose specific information (article 479(112) CPC), secure evidence (article 479(96) CPC), and hand over or disclose evidence (article 479 (106) CPC) that is important to demonstrate raised claims and the scope and value of those claims. In strictly defined circumstances, a third party can be ordered to do this as well. Evidence or information that is to be submitted when these procedural tools are employed often include confidential information that is a trade secret for the disclosing party. For this reason, when ordering that specific information be submitted or when securing evidence, or ordering a party to surrender the evidence, a court must take trade secrets into consideration and apply the mechanisms that protect the disclosing party's confidential information. At the same time, a party that has been ordered to disclose information or surrender or disclose evidence may contest that court decision, citing the need to protect its trade secrets.

When employing one of the remedies described above for evidence in IP cases, on one hand the court is required to take into consideration the need to protect trade secrets, while on the other it has broad discretion as to the means of securing trade secrets. In particular, a court can apply specific rules on evidence use and examination, enforce additional restrictions on evidence examination, render the submitted documents anonymous, or reveal only parts of documents. This is a new development in the Polish legal system, and therefore time will tell whether it is applied consistently and uniformly, and above all effectively.

In addition, a court might not allow refusal to provide information or submit evidence on the grounds of risk of disclosure of trade secrets, in which case non-compliance when a court requires information could lead to a fine or a financial penalty in separate proceedings. In turn, a refusal to surrender evidence when a court requires evidence to be secured or submitted could result in the materials being retrieved by a court enforcement officer under a court enforcement procedure.

In IP litigation cases, there is also an option for an entity that suffers damage due to disclosure of trade secrets in an IP case to claim compensation. This applies when the damage is due to use by the other party of information disclosed in the dispute for purposes other than defending claims (article 479(113) § 5 CPC). However, this is a new development and it is difficult to judge whether and to what extent it will be effective in the future. In particular, it is anticipated that problems may arise with demonstrating the damage caused in this way.

[1] art. 248 § 1 and 2 of the CPC in conjunction with art. 261 § 2 of the CPC.



CONTRACTOR COMPENSATION CLAIMS IN POLAND AGAINST CONTRACTING AUTHORITIES NOW MORE REALISTIC

Author: Tomasz Krzyżanowski, Attorney-at-law

On 25 February 2021, the Supreme Court in Poland adopted a resolution in case III CZP 16/20 stating that a contractor may seek compensation from a public contracting authority if the authority breaches the Public Procurement Law (PZP), and that the contractor is not required to first exhaust all other legal remedies envisaged under the PZP.Prawo zamówień publicznych.

There are various factors that make it difficult to claim compensation from public contracting authorities that are in breach of the PZP. One major obstacle is that to date the prevailing view in case law and legal literature was that a contractor must exhaust all legal remedies under the PZP, namely appeal to the National Appeals Chamber (KIO) and then to the regional court if unsuccessful, before even thinking about compensation.

On 25 February 2021, the Supreme Court adopted a resolution in case III CZP 16/20 that fundamentally changes this situation. One of the points made in the resolution is that:

A contractor whose bid is rejected in a manner that is a breach by the contracting authority of the Public Procurement Law of 29 January 2004 (consolidated text, Journal of Laws of 2019, item 1843) may seek compensation without the breach of the Public Procurement Law being confirmed beforehand in a final and binding ruling given by the National Appeals Chamber or by a court following review of an appeal against a National Appeals Chamber ruling.

The resolution makes it significantly easier to seek compensation from a Polish contracting authority if, as the contractor, we consider the contracting authority to have breached the PZP. Most importantly, contractors can forego expensive and protracted appeal procedures provided for in the PZP. In addition, despite this unequivocal standpoint taken by the Supreme Court, it would not be advisable to neglect to file an appeal with the KIO. In practice, it will certainly be more difficult to pursue claims if the relatively inexpensive and quick legal remedy of an appeal is not used. This would not be a sensible course of action.

KEY CONTACTS

International Committee

If you have any questions, please do not hesitate to contact us by e-mail at: **international@traple.pl**

Xawery Konarski
Attorney-at-law, Senior Partner

Anna Sokołowska-Ławniczak, PhD
Patent and trademark attorney, Partner

Competition & Antitrust

Paweł Podrecki, Habil.
Attorney-at-law, Senior Partner
pawel.podrecki@traple.pl

Tomasz Targosz, PhD
Attorney-at-law, Partner
tomasz.targosz@traple.pl

Corporate

Wojciech Kulis
Attorney-at-law, Partner
wojciech.kulis@traple.pl

Covid-19

Wojciech Kulis
Attorney-at-law, Partner
wojciech.kulis@traple.pl

Cybersecurity

Agnieszka Wachowska
Attorney-at-law, Partner
agnieszka.wachowska@traple.pl

Data protection

Xawery Konarski
Attorney-at-law, Senior Partner
xawery.konarski@traple.pl

Gzegorz Sibiga, PhD, Habil
Attorney-at-law, Partner
grzegorz.sibiga@traple.pl

KEY CONTACTS

Employment

Paweł Krzykowski
Attorney-at-law, Partner BKB
pawel.krzykowski@ksiazeklegal.pl

Daniel Książek, PhD
Attorney-at-law, Partner BKB
daniel.ksiazek@ksiazeklegal.pl

FinTech

Jan Byrski, PhD, Habil.
Attorney-at-law, Partner
jan.byrski@traple.pl

Internet & Media

Xawery Konarski
Attorney-at-law, Senior Partner
xawery.konarski@traple.pl

Piotr Wasilewski, PhD
Attorney-at-law, Partner
piotr.wasilewski@traple.pl

Intellectual Property

Prof. Elżbieta Traple, PhD, Habil.
Attorney-at-law, Senior Partner
elżbieta.traple@traple.pl

Paweł Podrecki, PhD, Habil.
Attorney-at-law, Senior Partner
pawel.podrecki@traple.pl

Beata Matusiewicz-Kulig
Attorney-at-law, Partner
beata.matusiewicz@traple.pl

Tomasz Targosz, PhD
Attorney-at-law, Partner
tomasz.targosz@traple.pl

Anna Sokołowska-Ławniczak, PhD
Patent and trademark attorney, Partner
anna.sokolowska@traple.pl

Agnieszka Schoen
Attorney-at-law, Partner
agnieszka.schoen@traple.pl

KEY CONTACTS

InfoTechnology

Xawery Konarski
Attorney-at-law, Senior Partner
xawery.konarski@traple.pl

Agnieszka Wachowska
Attorney-at-law, Partner
agnieszka.wachowska@traple.pl

Life Science

Prof. Elżbieta Traple, PhD, Habil.
Attorney-at-law, Senior Partner
elżbieta.traple@traple.pl

Paweł Podrecki, PhD, Habil.
Attorney-at-law, Senior Partner
pawel.podrecki@traple.pl

Tomasz Targosz, PhD
Attorney-at-law, Partner
tomasz.targosz@traple.pl

Litigation

Paweł Podrecki, PhD, Habil.
Attorney-at-law, Senior Partner
pawel.podrecki@traple.pl

Beata Matusiewicz-Kulig
Attorney-at-law, Partner
beata.matusiewicz@traple.pl

Public Procurement

Agnieszka Wachowska
Attorney-at-law, Partner
agnieszka.wachowska@traple.pl

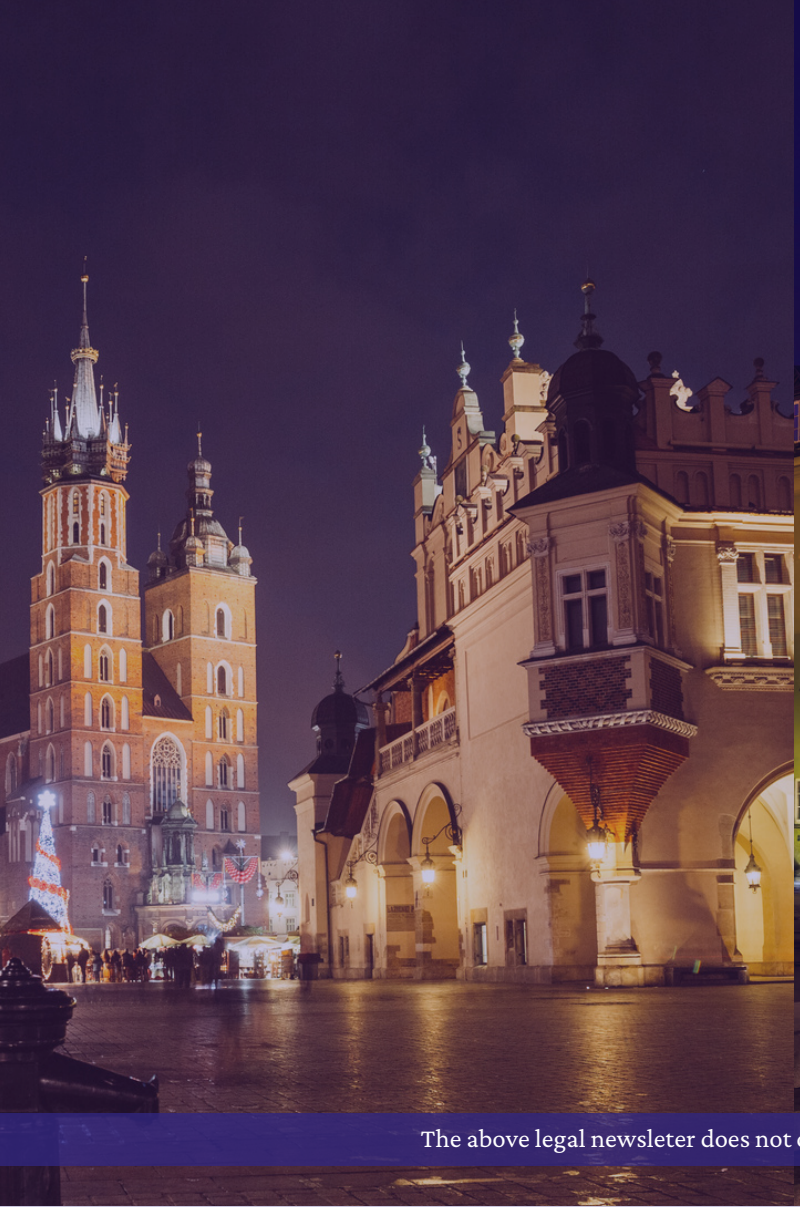
Telecommunication

Xawery Konarski
Attorney-at-law, Senior Partner
xawery.konarski@traple.pl

Agnieszka Wachowska
Attorney-at-law, Partner
agnieszka.wachowska@traple.pl

TAX

Wojciech Kulis
Attorney-at-law, Partner
wojciech.kulis@traple.pl



Traple Konarski Podrecki i Wspólnicy Sp.j.

Biuro w Krakowie:
ul. Królowej Jadwigi 170
30-212 Kraków
tel.: +48 12 426 05 30

e-mail: office@traple.pl
www.traple.pl

Biuro w Warszawie:
ul. Twarda 4
00-105 Warszawa
tel.: +48 22 850 10 10

Traple Konarski Podrecki & Partners