

06

Issue No.

# TKP LEGAL NEWSLETTER

*Warsaw/Poland*

*December 2021*

## In this issue:

### WHAT'S NEW? LEGAL NEWS FROM POLAND

#### MORE ABOUT

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

**Truple  
Konarski  
Podrecki  
& Partners**

# TKP



# Merry Christmas

FROM TRAPLE KONARSKI  
PODRECKI & PARTNERS

TKP

## AMENDMENT TO WASTE ACT SIGNED BY PRESIDENT

*Author: Michał Sobolewski, Attorney-at-law*

**On 23 November 2021, the President of Poland signed into law the Act of 17 November 2021 amending the Waste Act and certain other acts (Journal of Laws 2021, item 2151). The act implements the European Parliament and Council waste directives.**

The architects behind the act wish to take the next step in Poland towards further development of the the circular economy in Poland, eventually leading to 65% preparing for reuse and recycling of municipal waste by 2035, in line with the EU joint declarations. The amendment substantially changes the national rules in the Waste Act and other acts on cleanliness and tidiness in municipalities, batteries, chemical substances and chemical mixtures, used electric and electronic equipment, and packaging and waste packaging management.

In line with the waste directives, the act makes a range of changes, including the amendment of definitions currently in use with regard to management of waste, biowaste, or municipal waste, and also adds new definitions of food waste, construction waste, or extended producer responsibility. The act provides for a limit on the volume waste a municipality can deposit at a landfill site and fines for exceeding the limits, and at the same time sets higher volumes for recycling waste packaging. It also provides for a range of awareness-raising measures to promote sustainable production and consumption models and reuse or repair.

As it was emphasized in the reasoning for the project of the amendment, the prospective changes will result in particular in a lower rate of consumption of primary raw materials (leaving them for future generations), a higher rate of use of secondary raw materials in manufacture of goods, less waste processing in general and per inhabitant, and should reduce the harmful effect of waste on the environment.

The act will take effect on 1 January 2022, except for particular provisions on collection of construction waste, which will come into force from 2023.

## NEW ACT ON CONTRACTUAL ADVANTAGE, NEW RISKS FOR BUSINESS

*Author: Krzysztof Witek, Attorney-at-law*

On 23 November, the President signed a new Act on Combating Unfair Use of Contractual Advantage in Trade in Agricultural and Food Products. This a long name, and will mean many changes on the market. These changes will also mean many new dangers.

### **The situation in the past**

The first act regulating this issue in Poland came into force in 2017, and on that basis the President of UOKiK has issued 12 decisions to date.

That act contains a general clause prohibiting unfair use of a contractual advantage, and also lists four examples of violations of this kind. It does not provide detailed guidelines on when a contractual advantage exists. It only contains a vague definition, which says that an advantage exists when there is a significant disproportion between the financial means of the parties. A contractual advantage is used unfairly when the conduct of one of the parties contravenes good customs and poses a threat to a major interest of the other party, or violates such an interest.

### **The cause of the changes**

The new act transposes Directive (EU) 2019/633 of the European Parliament and of the Council on unfair trading practices in business-to-business relationships in the agricultural and food supply chain.

### **The situation in the future**

The new act extends the list of practices that are prohibited, and these include “black list” practices (prohibited in any situation). Examples are excessive deadlines for payment for delivery of agricultural products, unilateral change of contractual terms by buyers, or requiring suppliers to make payments unrelated to sale of agricultural and food products. Six “gray list” practices are also included. These are practices that are permitted on condition that the parties agree them explicitly in consultations before they are applied, such as the buyer requiring the supplier to pay fees for advertising or marketing their products. One practice – where the buyer requires the supplier to cover the cost in whole or in part of decreases in the prices of products on special offer, must be provided for in advance in a contract that lays down the special offer terms and conditions in full.

### **The danger**

Once again, the President of UOKiK will enforce the laws. The new rules on prohibited practices pose new risks of being in breach of the law and incurring severe fines of up to 3% of the turnover of the undertaking in question.

## POLISH PARLIAMENT WORKING ON THE INTRODUCTION OF ELEMENTS OF HOLDING COMPANY LAW

*Author: Maciej Toroń, Attorney-at-law*

**Legislative work is ongoing in the Sejm on a bill amending the Commercial Companies Code[1] to introduce elements of holding company law into the Polish legal system. If the new rules are enacted, this could have a major effect on how companies in international capital grounds operate.**

A government proposal to amend the Commercial Companies Code was submitted to the Sejm in August 2021. The principal aim of the legislation is to regulate in part the rules for operation of *de facto holding companies*, i.e. groups of companies that in fact are linked (for example through capital affiliation), but between which there is no agreement on management or profit-sharing. The scope of the legislation is determined in this way due to the minimal significance of holding company agreements in the true reality of commerce.

The envisaged legislation **creates a formal framework for a coherent policy for managing and coordinating commercial strategy** within a capital group. The main instrument used to achieve this objective is intended to be **binding instructions** that a dominant company can issue to a subsidiary. The proposal also provides for instance for the option for the dominant company to obtain information about the subsidiary's operations and for the dominant company's supervisory board to perform oversight.

Coordination of commercial strategy within a corporate group may not be detrimental to subsidiary minority shareholders, and for this reason lawmakers have also provided for instruments to protect them, such as a request for the accounts of the entire group to be audited by a certified accountant, a right to request redemption of shares, or compensatory liability on the part of the dominant company for a decrease in the value of shares caused by instructions issued by the dominant company.

If passed, the act, which also provides for more effective oversight by supervisory boards, might be **beneficial** with regard to the day-to-day operations of subsidiaries with foreign capital which are part of international capital groups. As there is a six-month *vacatio legis*, the bill will come into force in mid-2022 at the earliest.

---

[1] The government proposal to amend the Commercial Companies Code and certain other acts IX term of the Sejm, docket 1515.

## NEW LEGISLATIVE PROPOSAL TO AMEND THE NATIONAL CYBERSECURITY SYSTEM ACT

*Author: Agnieszka Wachowska, Attorney-at-law, Partner and Aleksander Elmerych, Trainee attorney-at-law*

A government proposal to amend the National Cybersecurity System Act (CSA) has been published after many weeks of public statements. The proposal is somewhat similar to the proposal for an amendment to the act of last year, which was discussed in our previous international newsletter. However, it contains a range of new solutions not announced to the public before. Although a very short timeframe has been set, many comments have been submitted regarding the proposed bill, from business organizations and elsewhere. Government officials have said that the proposal has been submitted to the Government National Security and Defence Committee (KRMBNSO).

There is a major change compared to the previous version of the amendment, which is that telecommunications operators, which to date were completely excluded, will be included in the National Cybersecurity System. Telecommunications operators are only to be subject to the CSA to a certain extent, and the wording in this respect is vague and imprecise. This will apply only where telecommunications operators belong to one of the groups with special obligations under the CSA, for example they are digital service providers or operators of essential services.

As in the previous proposal, the National Cybersecurity System will include new entities such as institutions of higher education, or for example the Polish Financial Supervision Authority. Another change that has been retained is that Security Operations Centers (SOCs) have to be used to comply with obligations of operators of essential services where this relates for instance to management of security of an IT system, or dealing with and reporting incidents. Under the new provisions, agreements for SOC services performed for an operator of essential services must state Polish law as the governing law, and the competent minister will have an obligation to maintain a list of all SOCs in operation.

As in the previous proposal for the amendment, under the current proposal a national system of cybersecurity certification will be created. Under this system, a national cybersecurity certification scheme will be set up, and will have three trust levels (basic, essential, and high) for ICT products, services, and processes. The concept of creating a strategic cybersecurity network has also been retained, and this will be used by a strategic cybersecurity network operator to provide services to the most important state authorities (such as the Chancellery of the President, the Chancellery of the Sejm and Senate, and the National Security Bureau).

Once again, there is strong feeling and controversy surrounding the procedure for classifying a hardware or software supplier as a *high-risk supplier* and the power of the minister competent for computerization to issue instructions for security purposes.

# MORE ABOUT

Under the proposal, if a supplier is designated as high-risk, a significant number of firms operating on the market (such as digital service providers, operators of essential services, and telecommunications operators) may be prohibited from using certain hardware or software supplied by that supplier.

Meanwhile, under the new system for issuing instructions for security purposes, the instructions would take the form of an administrative decision. Security instructions are to be issued in cases of critical incidents, and for example it will be possible, in these instructions, to prohibit entities in the national cybersecurity system (such as operators of essential services and digital service providers) from using particular hardware or software, require them to place limits on traffic from IP or URL addresses of a particular entity joining the infrastructure, or order that distribution of a specific version of software be stopped or installation of that software be prohibited. Under the amendment, the penalty for not complying with instructions for security purposes is an administrative fine as high as 3% of total annual global turnover in the previous financial year in the case of digital service providers.

There is a new development in relation to the previous proposal for the amendment, concerning 5G networks. Under the current proposal, a new capital company will be formed called Polskie 5G, and it will have the goal of establishing the nationwide wholesale 5G network. Principally, the company will be responsible for ensuring that the wholesale 5G network signal covers the entire country and for providing wholesale paid telecommunications services via that network. According to the proposed provisions, the 5G network frequencies would be granted to telecommunications operators in an auction held by the President of the Office of Electronic Communications.

# MORE ABOUT Cybersecurity

## RECOMMENDATIONS OF THE MINISTRY OF CLIMATE AND ENVIRONMENT ON CYBERSECURITY FOR THE ENERGY SECTOR

*Author: Jakub Chlebowski, Attorney-at-law*

On 15 October 2021, the Ministry of Climate and Environment released recommendations on measures to improve cybersecurity in the energy sector and industry guidelines on incident reporting. The recommendations were drawn up on the basis of art. 42(1)(5) of the National Cybersecurity System Act of 5 July 2018, following consultations with CSIRT NASK, CSIRT GOV, and CSIRT MON, and operators of essential services in the energy sector.

The recommendations issued by the Ministry of Climate and Environment list best practices for energy sector undertakings to implement, especially undertakings classified as operators of essential services, to enable comprehensive rules to be formulated concerning many areas of organization, to protect their IT resources.

The recommendations cover areas such as:

- drawing up risk management procedures,
- using suppliers,
- raising personnel awareness,
- conducting security audits,
- ensuring continuity of operations, in particular of essential services,
- physical security, and also network security and IT system security, or for example
- policies concerning dealing with and reporting incidents.

Each of the spheres described in the Ministry's document includes recommendations that account for the specific nature of the energy sector.

For suppliers of IT services to energy sector undertakings, the most important guidelines are those on use of third-party services by energy sector undertakings. The recommendations focus in particular on issues that need to be regulated in agreements with IT suppliers whose assistance should be used in mitigating cybersecurity risk. In addition, the Ministry states that energy sector undertakings have to establish internal policies to improve supervision of tasks performed by IT suppliers.

Importantly, in the recommendations, the Ministry emphasizes the issue of using cloud computing solutions provided by external suppliers. The recommendations state that when selecting cloud computing services, energy sector undertakings need to take special security measures, such as measures to secure data processed in a cloud computing system or risk assessment when making use of solutions of that kind.



## PROCESSING OF PERSONAL DATA ON THE INTERNET – THE POLISH REGULATOR'S PERSPECTIVE

*Authors: Xawery Konarski, Attorney-at-law, Senior Partner*

Over the last few years, the European Court of Justice has issued a number of important judgments relating to the processing of personal data on the Internet (Wirtschaftsakademie, Fashion ID, and Planet49). The European Data Protection Board has also issued a number of guidelines in this area (for example for processing personal data of social network users).

The policy of the Polish Data Protection Authority (Polish DPA) is relevant in this context.

First, the Polish data protection authority is not competent in matters of privacy as defined in Directive 2002/58/EC (e-Privacy Directive). This is important in deciding cases concerning whether it is permitted to install and use different identifiers (e. g. cookies). The competent authority for this is the President of the Office of Electronic Communications, who issues the decision on the basis of telecommunications law. Telecommunications law provisions also specify the penalties for breaching these provisions.

Secondly, it can be seen from the Polish DPA's decisions that where the entity concerned only has a user's Internet identifier (e. g. their IP address), the regulator even considers this processing of personal data within the meaning of the GDPR where. Consequently, the GDPR will apply to *unregistered users*, i. e. users who visit a given website but do not have an account or profile there.

Unlike in the case of the Wirtschaftsakademie or Fashion ID case rulings, the Polish DPA has not yet adopted the concept of co-management of entities cooperating in various types of Internet advertising campaigns, including the collection of personal data for the purpose of such campaigns.

Also, with regard to the processing of personal data on the Internet for the controller's own marketing purposes, the grounds for these activities may be the legitimate interests pursued by the controller (Article 6(1)(f) GDPR). However, a *balance of interest* test is required in this case.

In light of the latest Polish DPA decisions, the right of access to personal data covers not only personal data provided by Internet users (e. g. where an account is created), but also *observed* and *inferred* data.

The highest fine imposed so far by the Polish DPA on an Internet entity was PLN 2,800,000 (EUR 600,000).

Finally, to date, the Polish DPA has not approved a code of conduct for the Internet industry. This code is expected in 2022. A proposal has been drawn up by the Internet Advertising Bureau Poland (IAB Poland).

## CHALLENGES FACING EMPLOYERS IN 2022

*Author: Paweł Krzykowski, Attorney-at-law, Partner BKB and Łukasz Łaguna, Junior Associate - Managing Partner's Assistant BKB*

The coming year will bring a number of new challenges for employers.

### 1. Polish Deal

One of the key changes proposed under the Polish Deal is the increase of the tax-free threshold for income tax to PLN 30 000 for all taxpayers who calculate their tax according to the tax scale. In addition, under the Polish Deal, the second tax threshold will be raised to PLN 120 000, beyond which a 32% tax rate will apply.

The Polish Deal would change the amount of the healthcare contribution paid by businesses. As a rule, the calculation base for this contribution would be the actual income of a person running a business instead of a fixed payment. This will mean that the healthcare contribution will be 4.9% of income. A minimum contribution will also be introduced, of 9% of the minimum wage - next year PLN 270 (the minimum wage in 2022 has been set at PLN 3000). The proposed changes to the tax system also envisage that the health contribution will not be tax-deductible.

Employees will also pay a 9% healthcare contribution calculated on income. Moreover, it will no longer be possible to deduct 7.75% of the healthcare contribution calculation base from tax. In the case of some employees, this effect will be compensated by the increase of the tax scale threshold (from PLN 85,528 to PLN 120,000) and the introduction of the middle-class relief, available to persons with income from an employment relationship up to PLN 133,692 per year. Employees whose income level makes it impossible to take advantage of the middle-class relief will be in a different situation. These are persons earning more than PLN 11,141 gross per month. In their case, the proposed changes will reduce the level of their net salaries. This may cause an increase in labor costs, as these employees may demand pay increases to compensate for the net amount paid to date.

### 2. Whistleblowing

According to the Directive on protection of whistleblowers, Poland has until 17 December 2021 to introduce relevant statutory regulations. Although the legislative proposal has already been published, we can expect it to enter into force next year. Therefore, most probably the beginning of 2022 will be the time for many employers to implement obligations provided for in the Directive and the Act on protection of whistleblowers. One such obligation is the introduction of internal whistleblowing procedures. Under the proposal, failure to establish an internal whistleblowing and follow-up procedure is punishable by imprisonment of up to three years and other sanctions.

# MORE ABOUT

## 3. Remote work

Work on amendments to the Labor Code with respect to remote working is still in progress. In recent weeks, information has emerged according to which the new regulations would be passed as soon as possible, so that they could enter into force as of 1 January 2022. In our opinion, this seems unlikely. This does not change the fact that the legislation on remote work will most likely be enacted in 2022. The specific form still remains unclear due to disputes within the public consultation process.

## 4. Minimum wage

According to the new regulations, the minimum wage in Poland from 1 January 2022 will be PLN 3010 gross. The hourly rate will also increase and will be PLN 19.70, which is PLN 210 more than the currently binding minimum wage (PLN 2800), which means an increase of 7.5 percent compared to last year.

## 5. Changes in allowances

From the new year, a delay in the payment of contributions by a business will no longer be an obstacle to obtaining sickness benefit. Among other things, the amount of benefit for the period of hospitalization will also change.

Also from the new year, this insurance will not cease due to late payment of contributions. This means that businesses will be able to receive sickness insurance benefits even if they pay their contributions after the deadline.

At present, sickness benefit for a period of hospitalization is, as a rule, 70% of the benefit base. From the new year, the monthly sickness benefit will be 80%.

Another change concerns the determination of the benefit calculation base. It will not have to be determined anew if there was no break between the periods of drawing benefits (regardless of their type) or the break was shorter than a calendar month. Currently, the calculation base is determined anew if the break in drawing benefits is three or more calendar months.

In addition, currently, if there are breaks in incapacity to perform work, the previous period of incapacity to perform work is included in the benefit period if it is caused by the same disease and the break does not exceed 60 days. As of the new year, the reason for incapacity to perform work before and after the break will not matter. However, periods of incapacity to perform work prior to a break of up to 60 days will not be included in the benefit period if, after the break, incapacity to perform work occurs during pregnancy.

# MORE ABOUT FinTech

## NEW LEGAL FRAMEWORKS OF CROWDFUNDING SERVICES IN POLAND

*Author: Jan Byrski, PhD, Habil., Cracow University of Economics Professor, Attorney-at-law, Partner and Michał Słuszniak, Trainee attorney-at-law*

The application of Regulation 2020/1503 from November 10, 2021 means that Poland, like other EU countries, will have provisions that regulate online crowdfunding in an almost comprehensive manner. What form will the provisions of crowdfunding services take in Poland? More about it in the article of trainee attorney-at-law, Associate Michał Słuszniak.

On November 10, 2021 the EU Regulation ECSP[1] began to apply. RECPS envisages the creation of a new regulated activity consisting in the provision of crowdfunding services. According to the definition, crowdfunding service regulated by RECPS covers loan and equity crowdfunding up to EUR 5 million which are to be calculated over a period of 12 months. The regulation does not regulate the form of donation (charity) or prize-based crowdfunding. The provision of the crowdfunding service is to take place only through the online platform, and the possibility of performing this activity will be reserved only to entities that obtain the authorisation.

Currently, in Poland, a draft act on crowdfunding for business ventures is being processed in order to harmonize domestic law with the content of RECPS. According to this draft, it is planned to limit the possibility of using crowdfunding services with regard to shares in limited liability companies, and at this stage (this issue may change) it provides for a two-year transition period (from 10 November, 2021) when the admissibility of such action will remain possible.

At the same time, in the period from the entry into force of the provisions of the draft act until November 9, 2023, the maximum threshold of crowdfunding in Poland will amount to EUR 2.5 million, and after that date the threshold specified in art. 1 clause 2 let. c RECPS, i.e. EUR 5 million. It should be mentioned that the proposed act provides a regime for the protection of information related to the provision of crowdfunding services, covering it with professional secrecy, the scope of which is to be equivalent to other professional secrets known from the financial market in Poland, e.g. banking secrecy.

According to art. 49 RECPS after 10 November, 2021 entities providing crowdfunding platforms on the basis of the previous national regulations may continue to operate on the terms set out therein until 10 November, 2021 or until they obtain an authorisation, whichever is sooner. It is important, however, that until the draft regulations enter into force, the Polish Financial Supervision Authority is not a supervisory authority within the meaning of RECPS, therefore the possibility of applying for a permit will open after the draft act enters into force. The moment of entry into force of the draft act is not known yet.

Crowdfunding is a constantly growing industry that offers a promising prospect as an alternative form of obtaining financing for commercial endeavors. On the other hand, taking into account the current lack of regulations in the Polish system regulating this matter, as well as the limitations related to the risk of operating in this area, the new regulations will allow for wider activity in the field of running crowdfunding platforms and faster development of this industry in our country. Importantly, providers of crowdfunding services from other Member States may conduct activities in Poland (and vice versa) with prior notification this intention in competent authority (art. 18 RECPS).

---

[1] Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937

## CURRENT DEVELOPMENTS REGARDING THE COMMON STATE IT INFRASTRUCTURE PROGRAM (WIIP)

*Author: Karolina Grochecka-Goljan, Attorney-at-law*

The WIIP program has been operating since 2019, and to date a number of steps have been completed in the program, including introduction of the Cloud Service Provision System (ZUCH), or for example the drafting of the Cloud Cybersecurity Standards. What are the current developments regarding the program? Is the WIIP program applicable to commercial suppliers?

Working with the COI, NASK, and GovTech Polska as providers assigned Ministry of Digital Affairs tasks, the Ministry of Digital Affairs is working to construct the Common State IT Infrastructure (WIIP).

The WIIP program comprises a range of organizational and investment measures concerning supply of IT infrastructure as cloud computing services. Elements of the program include:

1. **giving public authorities the option of acquiring Public Cloud services (PChO) – public cloud services provided by commercial suppliers** that meet in particular confidentiality, integrity, and accessibility requirements defined in terms of ensuring security for government authorities;
2. construction, development, and maintenance of the Government Cloud (RChO) – common public authority cloud;
3. the Cloud Service Provision System (ZUCH) – in which buyers can review the services provided in a cloud and cloud support services offered by vetted sellers and procure cloud services, of which the scope and parameters are specified in the Public Cloud Service Catalog by the ZUCH Operator (Ministry of Digital Affairs);
4. The Government Cybersecurity Cluster (RKB), which is part of Government Cloud (RChO) security;
5. The Cloud Cybersecurity Standards (SCCO) – a set of legal, organizational, and technical requirements ensuring cybersecurity in cloud computing implementation models.

There are plans to expand the ZUCH platform and ensure that the Public Procurement Law is amended accordingly to make using ZUCH easier. The Cloud Security Standards document is particularly noteworthy (available [here](#)). This document specifies the requirements for:

1. government entities that manage Data Centers (CPD) for them to be connected to the Government Cybersecurity Cluster (RKB) or incorporated into the Government Cloud (RChO) resources, as well as
2. **suppliers of cloud computing services as part of the PChO.**

**More information on how to become a seller in ZUCH can be found [here](#) and [here](#). The second edition of the PChO catalog is expected in Q1 2022. In the second edition, a seller will be able to offer cloud services in ZUCH in two service catalogs: The Polish PChO and EU PChO (PChO service catalog in the Polish jurisdiction and in the EU jurisdiction).**

# MORE ABOUT Intellectual Property



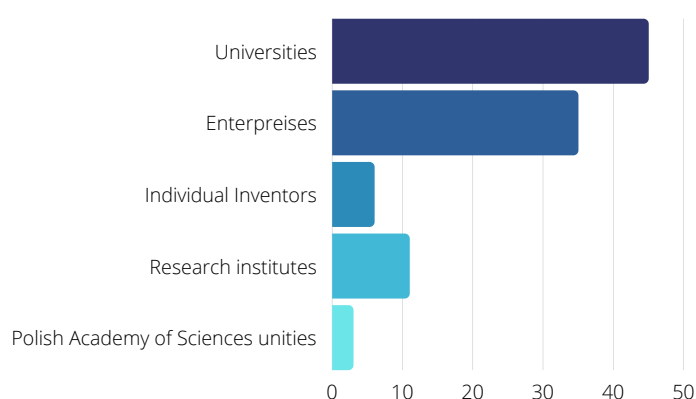
## IS POLAND INNOVATIVE ENOUGH?

*Author: Anna Sokółowska-Lawniczak, PhD, Patent and trademark attorney, Partner and Katarzyna Puchała, Trainee patent and trademark attorney*

European Patent Office (EPO) and Polish Patent Office (PPO) statistics show that the answer to the question *is Poland innovative Enough* should be – “not exactly”. There has been some increase in the number of patent applications from Poland (before the EPO) or in Poland (before the PPO) compared to past years, but we are still a long way behind the major players. Also, as the summary below shows, the most innovative entities in Poland are universities and public research organizations, not private companies.

In 2020, the number of European patents applied for by Polish companies was 483 (4.3% increase compared to 2019). The EPO granted 278 patents, which indicates an increase of 20.3% compared to 2019. This ranks Poland 35th in European patent applications per million inhabitants and 27th in patent applications.

### Granted patents (national procedure)



In 2020, in the Polish procedure, the Polish Patent Office granted 2260 patents and 533 protection rights for utility models to Polish applicants, while the respective figures for foreign entities were 48 and 19. This represents a slight downward trend compared to 2019, when 2947 patents and 603 protection rights for utility models were granted to Polish applicants.

EPO statistics show that nearly 74% of patent applications were filed by large enterprises, and 21% by SMEs and individual inventors. Meanwhile, only 5% were filed by universities and public research organizations. In Poland, the structure of patent applicants is significantly different – nearly 60% of patent applications are filed by universities and public research organizations, while only 6% are filed by individual inventors.

The principal technical fields in Polish applications have remained the same for several years: thermal processes and mechanical engineering apparatus (9.5% of all applications/ 46 applications); medical technology (instruments) - 38 applications; Pharmaceuticals (8% of applications/38 applications) and transport (31 applications). There was a noticeable increase in applications for furniture, games (+700%) and biotechnology (+200%).

More data here:

- In 2020, the number of patents and protection rights for utility models granted to research organizations was 244 and 19 respectively (in 2019 259 patents and 12 utility models)
- In 2020, the number of patents and protection rights for utility models granted to Polish Academy of Sciences organizations was 72 and 4 respectively (in 2019 91 patents and 1 utility model)
- In 2020, the number of patents and protection rights for utility models granted to individuals was 137 and 67 respectively (in 2019 207 patents and 54 utility models)
- In 2020, the number of patents and protection rights for utility models granted to businesses was 797 and 381 respectively, and in 2019 1150 patents and 473 utility models
- In 2020, the number of patents and protection rights for utility models granted to institutions of higher education was 1010 and 62 respectively, and in 2019 1240 patents and 63 utility models.



## INFLUENCERS UNDER SCRUTINY BY THE OFFICE OF COMPETITION AND CONSUMER PROTECTION

*Author: Agnieszka Karcz, Lawyer*

On 28 September, 2021, the President of Office of Competition and Consumer Protection (“**UOKiK**”) launched a preliminary inquiry into market influencer activities. UOKiK intends to determine whether activities of entities that post advertising content on social networking sites such as Instagram, Facebook, and TikTok might be misleading for consumers with regard to the way in which advertising content is presented on those sites. Among the reasons why influencers and the advertising agencies representing them have come under scrutiny is complaints by consumers regarding *scams*. This is a term used for a dishonest way of publicly praising products of doubtful quality or of an exorbitant price. Measures taken by regulators in other European countries such as the UK or France are also a factor in the launching of the inquiry. The measures in those countries are intended to regulate or issue guidelines for standards for activities of influencers with regard to identifying advertising, intended to mitigate the risk of consumers being misled.

For many people in the influencer’s audience, the influencer’s activity is associated with fun that is provided free of charge. A favorite content creator can be followed on their channel and it is possible to communicate with them, and listen to their recommendations or tips in the same way as a good friend. According to the first Marketing Influencer Handbook on the Polish market[1] - published at the end of October this year by the working group IAB Polska - influencers should be defined simply as people who ‘exert an influence’ on the community around them due to and by way of content posted on their social media profiles. Meanwhile, so that the work of such influencers is not merely a hobby and can be done on a professional level, they frequently seek sponsors for their activities. Due to support obtained in this way, the produced content can continue to be free of charge for society, and the influencer can devote more time to producing that content and not worry too much about the cost.

It needs to be borne in mind, however, that the activity, and essentially the influencer’s existence, is founded on the trust placed in them by their target audience. For this reason, cryptoadvertising in this sector involves great risk, as this risk is twofold. It can result not only in a severe fine being imposed on the undertaking of that kind by the President of UOKiK, but also a loss of target audience. This can happen when it is not expressly stated in published material that the viewer – consumer is dealing with promotion of a product or service for which the influencer received payment[2]. In turn, under art. 16(1)(4) of the Act on combating unfair competition[3], making a statement of encouragement to purchase goods or services while creating the impression of neutral information is an act of unfair competition with respect to advertising. This is also why the inquiry instigated by UOKiK is intended to focus on examining whether influencers identify advertising or sponsored content in their posts. In this context, agreements between influencers and advertisers or advertising agencies are being examined carefully as to whether they provide for restrictions of guidelines of any kind concerning the way in which advertising or sponsored content is identified.

# MORE ABOUT



There is no doubt that influencers need to start being mindful today of the responsibility they have for the message they convey to their audience, who are often fascinated by their activities. A publication must state clearly and unequivocally which material on a profile is advertising, and which material is their individual and independent opinion. Although they have been on the influencer marketing market for a number of years, content creators still do not identify advertising in their posts, or do not do so properly. This situation is probably principally due to lack of awareness, both of the obligations they have and of how to translate general guidelines in the law into specific measures.

Since UOKiK launched the inquiry, significantly more content identified as sponsored has appeared on social media. This can be seen at the first results of UOKiK's measures even at the outset. It may however be too early for rejoicing, because in addition to the fear of penalties there is a new problem of how to identify content without undermining the quality and reach of posted content. The tools provided by the main social media platforms consider content identified in this way to be less attractive, and this has a direct effect on content creators.

UOKiK and the advertising industry do not have an easy task – to devise systems that protect consumer interests on one hand and limit the chances of them being misled, but which on the other hand are not too onerous for the audience or render content less attractive due to advertising identification standards being too rigorous. In view of the rapid rate of development and the increasingly important role of influencer marketing, mechanisms for ongoing revision of markings that exist and are used in trade, and for a rapid response to new problems on the market, also need to be provided for.

---

[1] [https://www.iab.org.pl/wp-content/uploads/2021/10/INFLUENCER-MARKETING\\_poradnik-IAB-Polska-2021.pdf](https://www.iab.org.pl/wp-content/uploads/2021/10/INFLUENCER-MARKETING_poradnik-IAB-Polska-2021.pdf)

[2] Art. 7(11) of the Act of 23 August 2007 on combating unfair commercial practices (consolidated text, Journal of Laws of 2017, item 2070)

[3] Act of 16 April 1993 on combating unfair competition (consolidated text, Journal of Laws of 2020, item 1913)



## ADVERTISING OF DIETARY SUPPLEMENTS - TRENDS IN RECENT CASE-LAW IN POLAND

*Author: Zaneta Zemla-Pacud, PhD, Attorney-at-law*

*Administrative authorities and courts are clarifying the scope of health claims considered unacceptable.*

Health claims are claims that state, suggest or imply that a relationship exists between a food category, a food or one of its constituents, and health. They are used in the labelling, presentation and advertising of dietary supplements. Under EU law (Regulation (EC) No 1924/2006 of the European Parliament and of the Council of 20 December 2006 on nutrition and health claims made on foods), health claims made about food are prohibited unless they have been authorized by the Commission and included in a list of permitted claims. They are also subject to general rules on health claims set out in the Regulation (for instance medicinal properties cannot be attributed to dietary supplements).

However, the status of some categories of health claims remains uncertain. A list of over 2,000 health claims for botanical substances remains on hold (on a *pending list*), awaiting EFSA evaluation. Other claims, attributing properties such as *probiotic*, *prebiotic* and *psychobiotic* are said to imply that the product contains a substance that may be beneficial for health.

Judgments issued by Polish administrative courts continue to clarify EU rules on health claims. The Supreme Administrative Court has recently stated that “the presentation and advertising of dietary supplements cannot suggest to the consumer that supplementation of foodstuffs will prevent health problems or even have curative properties”, rendering the health claim “x is an invaluable aid in supporting the treatment of phobias or depression” unacceptable (II GSK 919/21, 23.09.2021). The Voivodeship Administrative Court in Warsaw pointed out that the wording of claims must have the same meaning for consumers as that of a permitted health claim (VII SA/Wa 2243/20, 7.04.2021) and that claims cannot exploit fear in the consumer (VII SA/Wa 2223/20, 16.03.2021, where the claim indicated that synthetic vitamin K2 could be “poisonous” or “dangerous”, in contrast to the vitamin K2 offered by the applicant).

### **Commentary**

The Polish dietary supplement market value continues to grow. Its rapid growth is built on increasing demand from consumers, which is why the current state of play with regard to the uncertain future of the *pending list*, and the lack of clear regulations concerning the terms *probiotic*, *prebiotic* and *psychobiotic* is not only creating a difficult situation for entities who wish to place dietary supplements on the Polish market, but also potentially poses a threat to both public health in Poland and the reputation of the dietary supplements industry. For now, subsequent judgments provide the only authoritative guideline as to borderline cases.

## PROTECTIVE LETTERS IN PATENT LITIGATION CASES

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

In July 2020, specialist IP courts began operating in Poland, and there are now five specialist IP courts operating in Poland. Only one, the Warsaw Regional Court, is competent to hear patent disputes (patent infringement, finding no patent infringement, proceedings in which an injunction is sought for the duration of patent infringement litigation). In light of this development, there is more and more discussion about whether legislation is needed in Poland to introduce protective letter, an important tool in injunction proceedings in IP, primarily patent, litigation cases.

This will be a protective letter that can be filed with a court when there is a strong possibility of IP disputes being initiated, primarily concerning patents, by the prospective adverse parties/defendants in such cases, before a statement of claim or motion for an injunction is filed with the court. The main purpose of this instrument is to present the court with which a filing for an injunction might be made with the prospective defendant's counterarguments. The protective letter is thus intended as a means of preventing a court from granting preliminary injunction, for instance prohibiting a certain activity (production, or even seizure of products manufactured by a potential party in breach) for the duration of the case. It is common for crucial court decisions and action to occur at this stage that determine the ultimate outcome of the patent dispute.

The creation of a single court in Poland to deal with patent litigation cases makes the practice of filing protective letters more important, and in particular increases the effect they might have on the range of arguments considered by the court when ruling on an injunction in a patent case. Protective letters are a well-known and regulated instrument in Western European countries, and this includes rules on court procedures concerning protective letters of this kind when they are filed, such as whether protective letters of this kind are served to patent owners who file a motion for an injunction. In Poland, there are no procedural rules governing protective letters; they are merely an instrument known and formed in practice, to which courts' approaches have been highly inconsistent to date. Some courts do not even take these protective letters into account when issuing an injunction, some return them, and some place them in the case files and review them. Now that a single court has been created to deal with patent cases, this has revived the debate on whether legislation on protective letters is necessary in litigation law, for instance with respect to intellectual property. As a minimum, this is also an opportunity to establish uniform practice of that court as regards this instrument. Enacting legislation, or at least formulating uniform practice of courts regarding this issue, will be especially important for entities that decide to enforce a patent in Poland, as well as for entities that decide to introduce a temporary solution or a product, where this could result in claims for patent infringement. If this happens, the latter in particular will have a more predictable legal instrument to mitigate the risk of their activities being stopped due to a court granting an injunction while not having the opportunity to consider their arguments.

## CYBERSECURITY AND PUBLIC PROCUREMENT IN POLAND. LEGISLATIVE PROPOSAL TO AMEND THE NATIONAL CYBERSECURITY SYSTEM ACT

*Author: Tomasz Krzyżanowski, Attorney-at-law*

The National Cybersecurity System Act of 5 July 2018 forms the legal and institutional bases for cybersecurity in Poland. On 12 October 2021, a controversial proposal to amend the act was submitted for consultations. This could have major implications, including for the public procurement market in Poland. The proposal allows a business undertaking to be classified as a *high-risk supplier*, and this may result in a bid being rejected.

The proposal has been commented upon as possibly aimed at certain manufacturers based in non-EU and non-NATO countries. For this and other reasons, work on the bill is beginning to become protracted. On 12 October 2021, a version was published that is theoretically close to the final version.

The amendment provides for proceedings to classify a hardware or software supplier as *high-risk*. This is to be decided by the minister responsible for computerization, if they consider the supplier to pose a serious risk to defense, state security, public safety or order, or human life and health. The Cybersecurity College will issue an opinion on this subject. According to the statement of reasons for the amendment, the College's opinion may be based on substantive criteria, but other aspects which are "non-technical" may be considered as well. This gives rise to a risk that the minister's decisions might be arbitrary, and concerns that decisions may be politically motivated in some cases.

In cases of public procurement proceedings conducted by entities listed in the proposal for art. 66a(1)(1) – (4) which at the same time are contracting authorities bound by the Public Procurement Law of 11 September 2019 (for example national cybersecurity system entities, which include many state entities), a decision naming a supplier as *high-risk* will have serious consequences for that supplier. Contracting authorities in the public sector will not be permitted to purchase hardware and software, or services, specified in the decision. This means that a bid submitted by a high-risk supplier would have to be rejected. As a result, the entity concerned would be eliminated from the market in the case of public tenders subject to the National Cybersecurity System Act with respect to the products named in the decision.

TKP is monitoring work on the amendment and we will provide updates on progress on the bill in future newsletters.

**More can be found on the subject discussed above on our Polish blog**

[READ MORE](#)



# KEY CONTACTS

## International Committee

If you have any questions, please do not hesitate to contact us by e-mail at: [international@trapple.pl](mailto:international@trapple.pl)



**Xawery Konarski**  
Attorney-at-law, Senior Partner



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



## Climate





 **Wojciech Kulis**  
Attorney-at-law, Partner  
 [wojciech.kulis@trapple.pl](mailto:wojciech.kulis@trapple.pl)

## Competition & Antitrust



 **Paweł Podrecki, PhD, Habil.**  
Attorney-at-law, Senior Partner  
 [pawel.podrecki@trapple.pl](mailto:pawel.podrecki@trapple.pl)



 **Tomasz Targosz, PhD**  
Attorney-at-law, Partner  
 [tomasz.targosz@trapple.pl](mailto:tomasz.targosz@trapple.pl)



## Corporate



 **Wojciech Kulis**  
Attorney-at-law, Partner  
 [wojciech.kulis@trapple.pl](mailto:wojciech.kulis@trapple.pl)



## Cybersecurity





 **Agnieszka Wachowska**  
Attorney-at-law, Partner  
 [agnieszka.wachowska@trapple.pl](mailto:agnieszka.wachowska@trapple.pl)

## Data protection



 **Xawery Konarski**  
Attorney-at-law, Senior Partner  
 [xawery.konarski@trapple.pl](mailto:xawery.konarski@trapple.pl)



 **Grzegorz Sibiga, PhD, Habil**  
Attorney-at-law, Partner  
 [grzegorz.sibiga@trapple.pl](mailto:grzegorz.sibiga@trapple.pl)

# KEY CONTACTS

## Employment



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



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

## FinTech



**in** **Jan Byrski, PhD, Habil.**  
Attorney-at-law, Partner  
jan.byrski@trapple.pl

## Internet & Media



**in** **Xawery Konarski**  
Attorney-at-law, Senior Partner  
xawery.konarski@trapple.pl



**in** **Piotr Wasilewski, PhD**  
Attorney-at-law, Partner  
piotr.wasilewski@trapple.pl

## Intellectual Property



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



**in** **Beata Matusiewicz-Kulig**  
Attorney-at-law, Partner  
beata.matusiewicz@trapple.pl



**in** **Tomasz Targosz, PhD**  
Attorney-at-law, Partner  
tomasz.targosz@trapple.pl



**in** **Agnieszka Schoen**  
Attorney-at-law, Partner  
agnieszka.schoen@trapple.pl





**in** **Anna Sokołowska-Ławniczak, PhD**  
Patent and trademark attorney, Partner  
anna.sokolowska@trapple.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





 **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

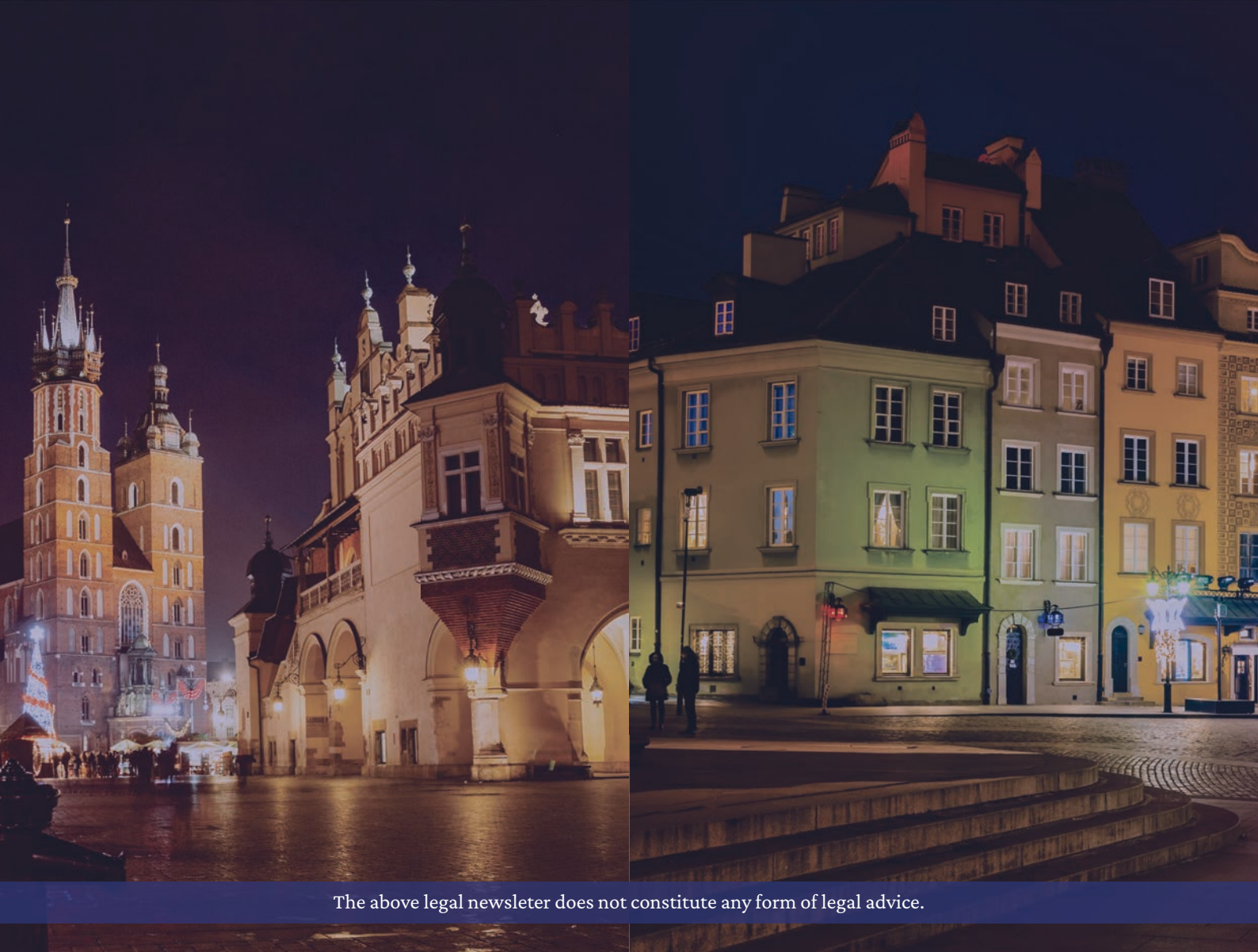


 **Agnieszka Wachowska**  
Attorney-at-law, Partner  
 agnieszka.wachowska@traple.pl

## TAX



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



The above legal newsletter does not constitute any form of legal advice.

**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](mailto:office@traple.pl)  
[www.traple.pl](http://www.traple.pl)**

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



**Traple Konarski  
Podrecki & Partners**