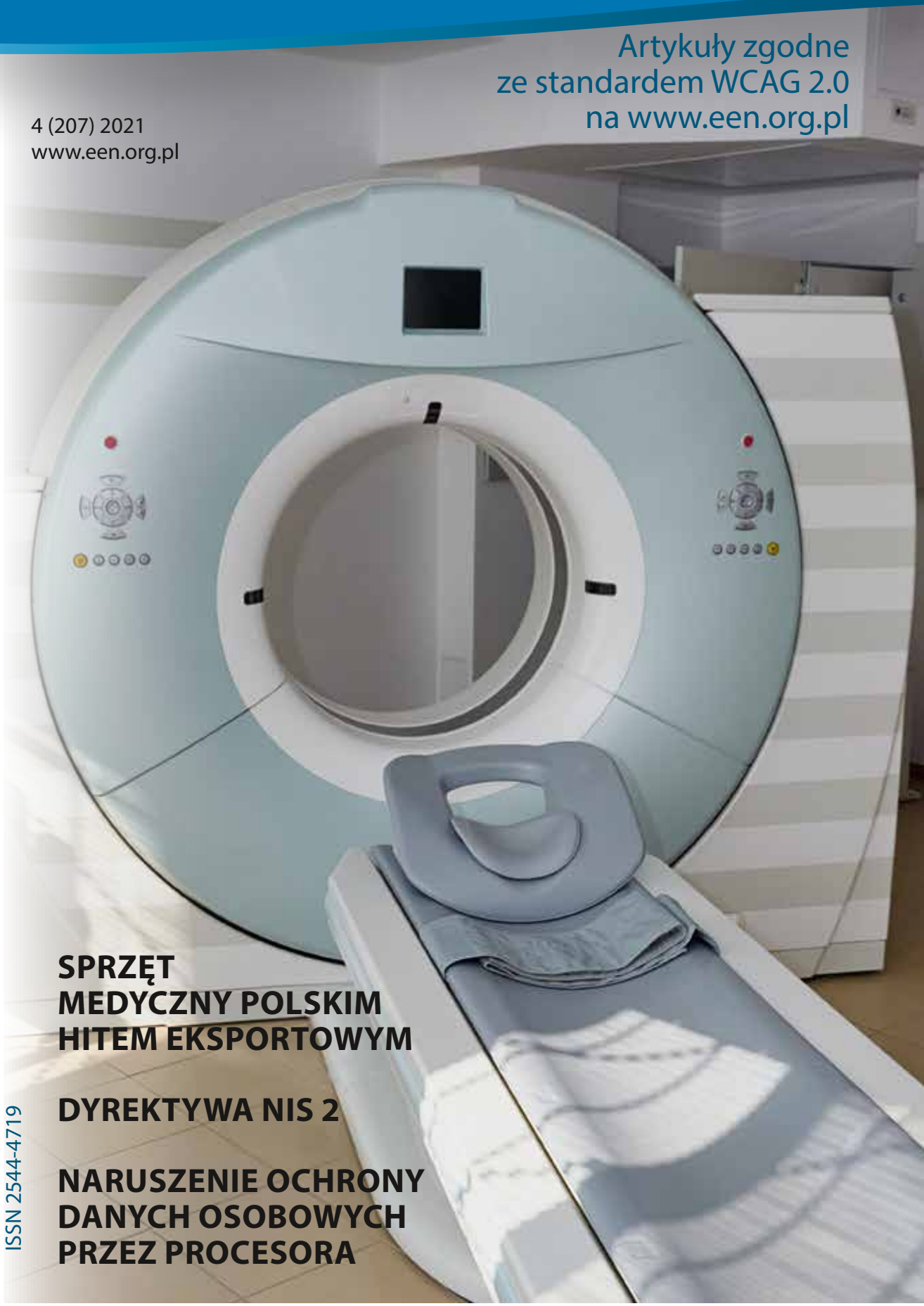
enterprise
europe
network

POLSKA

BIULETYN EURO INFO

4 (207) 2021
www.een.org.pl

Artykuły zgodne
ze standardem WCAG 2.0
na www.een.org.pl



SPRZĘT MEDYCZNY POLSKIM HITEM EKSPORTOWYM

DYREKTYWA NIS 2

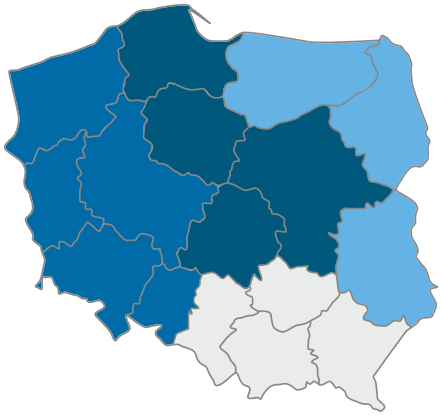
NARUSZENIE OCHRONY DANYCH OSOBOWYCH PRZEZ PROCESORA

ISSN 2544-4719

PARP Grupa PFR / Centrum Rozwoju MŚP

enterprise europe network
Wsparcie dla biznesu w zasięgu ręki

Konsorcja realizujące projekt Enterprise Europe Network w Polsce



Enterprise Europe Network – Central Poland

Enterprise Europe Network – East Poland

Enterprise Europe Network – West Poland

Enterprise Europe Network – South Poland

Konsorcjum: Enterprise Europe Network-Central Poland

Polska Agencja Rozwoju Przedsiębiorczości
ul. Pańska 81/83, 00-834 Warszawa
tel. (22) 432 71 02
www.een.org.pl

Instytut Mechanizacji Budownictwa i Górnictwa Skalnego
ul. Racjonalizacji 6/8, 02-673 Warszawa
tel. (22) 847 53 68
www.een-centralpoland.eu

Fundacja Rozwoju Przedsiębiorczości
ul. Piotrkowska 86, 90-103 Łódź
tel. (42) 630 36 67
www.frp.lodz.pl

Stowarzyszenie „Wolna Przedsiębiorczość"
ul. Piekarnicza 12A
80-126 Gdańsk
tel. 58 350 51 40
www.een.pomorskie.pl

Toruńska Agencja Rozwoju Regionalnego SA
ul. Włocławska 167, 87-100 Toruń
tel. (56) 699 54 80-83
www.een.tarr.org.pl

Uniwersytet Warszawski DELab
ul. Dobra 56/66, 00-312 Warszawa
tel. (22) 55 27 606
www.delab.uw.edu.pl/pl/een/

Konsorcjum: Enterprise Europe Network-East Poland

Podlaska Fundacja Rozwoju Regionalnego
ul. Starobojarska 15, 15-073 Białystok
tel. (85) 740 86 83
www.pfrr.pl, www.een-polskawschodnia.pl,
www.een.pfrr.pl

Centrum Innowacji i Transferu Technologii, Uniwersytet Warmińsko-Mazurski w Olsztynie
ul. Prawocheńskiego 9, 10-720 Olsztyn
tel. (89) 523 39 00
www.uwm.edu.pl, www.een-polskawschodnia.pl,
www.uwm.edu.pl/een

Warmińsko-Mazurska Agencja Rozwoju Regionalnego SA w Olsztynie
ul. Jagiellońska 91a, 10-356 Olsztyn
tel. (89) 512 24 05
www.een.wmarr.olsztyn.pl,
www.een-polskawschodnia.pl

Centrum Innowacji i Transferu Technologii Politechniki Lubelskiej
ul. Nadbystrzycka 38H, 20-618 Lublin
tel. (81) 538 42 70
http://lctt.pollub.pl,
www.een-polskawschodnia.pl,
www.citt.pollub.pl

Lubelska Fundacja Rozwoju
Rynek 7, 20-111 Lublin
tel. (81) 528 53 11-12-31
www.lfr.lublin.pl,
www.een-polskawschodnia.pl

Park Naukowo-Technologiczny Polska Wschód w Suwałkach Sp. z o.o.
ul. Innowacyjna 1, 16-400 Suwałki
tel. (87) 564 22 24-25
www.park.suwalki.pl,
www.een-polskawschodnia.pl

Konsorcjum: Enterprise Europe Network-South Poland

Centrum Transferu Technologii, Politechnika Krakowska
ul. Warszawska 24, 31-155 Kraków
tel. (12) 628 28 45
www.transfer.edu.pl

Izba Przemysłowo-Handlowa w Krakowie
ul. Floriańska 3, 31-019 Kraków
(12) 428 92 55
www.iph.krakow.pl

Górnośląska Agencja Przedsiębiorczości i Rozwoju sp. z o.o.
ul. Wincentego Pola 16, 44-100 Gliwice
tel. (32) 339 31 10
www.gapr.pl

Fundusz Górnośląski SA Oddział w Katowicach
ul. Powstańców 17, 40-039 Katowice
tel. 32 72 85 828
www.enterprise.fgsa.pl

Świętokrzyskie Centrum Innowacji i Transferu Technologii Sp. z o.o.
ul. Studencka 1, 25-323 Kielce
tel. (41) 343 29 10
www.it.kielce.pl

Staropolska Izba Przemysłowo-Handlowa
ul. Sienkiewicza 53, 25-002 Kielce
tel. (41) 368 02 78
www.siph.com.pl

Rzeszowska Agencja Rozwoju Regionalnego SA
ul. Szopena 51, 35-959 Rzeszów
tel. (17) 867 62 34
www.rarr.rzeszow.pl

Stowarzyszenie Grupy Przedsiębiorców Przemysłu Lotniczego Dolina Lotnicza
ul. Szopena 51, 35-959 Rzeszów
tel. (17) 850 19 35
www.dolinalotnicza.pl

Wyższa Szkoła Informatyki i Zarządzania
ul. mjr. H. Sucharskiego 2, 35-225 Rzeszów
tel. (17) 852 49 75
www.een.wsiz.pl

Konsorcjum: Enterprise Europe Network-West Poland

Wrocławskie Centrum Transferu Technologii, Politechnika Wrocławska
ul. Smoluchowskiego 48, 50-372 Wrocław
tel. (71) 320 33 18
www.wctt.pwr.edu.pl

Poznański Park Naukowo-Technologiczny Fundacji Uniwersytetu im. Adama Mickiewicza
ul. Rubież 46, 61-612 Poznań
tel. (+48) 61 827 97 46
www.ppnt.poznan.pl

Agencja Rozwoju Regionalnego SA w Koninie
ul. Zakładowa 4, 62-510 Konin
tel. (+48) 63 245 30 95
www.arrkonin.org.pl

Centrum Przedsiębiorczości i Transferu Technologii Uniwersytetu Zielonogórskiego
ul. Syrkiewicza 6, 66-002 Nowy Kisielin
tel. (+48) 504 070 281
www.cptt.uz.zgora.pl

Fundacja Kaliski Inkubator Przedsiębiorczości
ul. Częstochowska 25, 62-800 Kalisz
tel. (+48) 62 765 60 58
www.kip.kalisz.pl

Dolnośląska Agencja Rozwoju Regionalnego SA
ul. Szczawieńska 2, 58-310 Szczawno-Zdrój
tel. (+48) 74 648 04 50
www.darr.pl

Stowarzyszenie „Promocja Przedsiębiorczości" w Opolu
ul. Damrota 4, 45-064 Opole
tel. (+48) 77 456 56 00
www.een.opole.pl

Regionalne Centrum Innowacji i Transferu Technologii
ul. Jagiellońska 20-21, 70-363 Szczecin
tel. (+48) 91 449 41 09
www.innowacje.zut.edu.pl

Zachodniopomorskie Stowarzyszenie Rozwoju Gospodarczego – Szczecińskie Centrum Przedsiębiorczości
ul. Kolumba 86, 70-035 Szczecin
tel. (+48) 91 433 02 20
www.zsrg.szczecin.pl/een/

Drodzy Czytelnicy,

jeszcze przed końcem tego roku w Polsce powinny zacząć obowiązywać przepisy, na podstawie których średni i więksi przedsiębiorcy będą zobowiązani wprowadzić rozwiązania umożliwiające dokonywanie zgłoszeń nadużyć w firmach oraz zabezpieczające tych, którzy o takich nieprawidłowościach poinformowali. Inaczej mówiąc – należy implementować unijną dyrektywę dotyczącą ochrony sygnalistów. Powiedzmy wprost – wspomniany akt prawny zawiera wiele problematycznych kwestii, z którymi przedsiębiorcy już niedługo będą musieli się zmierzyć. Dlatego już dzisiaj warto zastanowić się nad tym, w jaki sposób należy opracować i wdrożyć stosowne procedury w tym zakresie. Mamy nadzieję, że pomoże w tym lektura artykułu pt. „Dyrektywa o ochronie praw sygnalistów".

W tym numerze Biuletynu poruszamy także kwestie związane z uzyskaniem ochrony imienia i nazwiska jako znaku towarowego w świetle polskich i unijnych przepisów prawa. Jakie są przesłanki uzyskania takiej ochrony, co może stanąć na przeszkodzie przed rejestracją, jakie są przykłady tego typu sytuacji? Na te i inne pytania należy poszukać odpowiedzi w tekście pt. „Imię i nazwisko jako znak towarowy".

Zapraszamy także do zapoznania się z najnowszymi ofertami współpracy zagranicznej pochodzącymi z bazy POD (*Partnership Opportunities Database*), prowadzonej przez Komisję Europejską i udostępnianej ośrodkom Enterprise Europe Network.

Z wyrazami szacunku
zespół redakcyjny
Biuletynu Euro Info

Spis treści

Biuletyn Euro Info, wydawany przez ośrodek Enterprise Europe Network przy Polskiej Agencji Rozwoju Przedsiębiorczości, jest współfinansowany przez Komisję Europejską ze środków pochodzących z programu COSME na lata 2014–2020 oraz przez Ministerstwo Rozwoju, Pracy i Technologii w ramach programu pn. „Udział Polski w programie na rzecz konkurencyjności przedsiębiorstw oraz małych i średnich przedsiębiorstw (COSME) oraz w instrumentach finansowych programów UE wspierających konkurencyjność przedsiębiorstw w latach 2015–2021".

Redaktor naczelny: Paweł Sikorski
Zespół: Aleksandra Wolska, Agata Kudelska, Eryk Rutkowski
Korekta: Pracownia C&C Sp. z o.o.
Adres redakcji: Enterprise Europe Network przy PARP
ul. Pańska 81/83, 00-834 Warszawa
Telefon: 22 432 71 02

Skład, druk i dystrybucja: Pracownia C&C Sp. z o.o.
www.ccpg.com.pl
Zdjęcia: AdobeStock
Nakład: 1400 egz.

Sprzęt medyczny polskim hitem eksportowym

Urządzenia warte miliardy

Eryk Rutkowski

Według danych Głównego Urzędu Statystycznego w 2019 roku polscy producenci sprzętu medycznego wyeksportowali wyroby o wartości ponad 2,4 mld euro. To kolejny rekord na przestrzeni ostatniej dekady. A jeśli cofniemy się w czasie do początku przemian ustrojowych, wartość eksportu dla tej branży wzrosła już ponad stukrotnie – z poziomu zaledwie 20 mln dolarów w 1992 roku. Rosnące znaczenie branży dla eksportu widać też w jej udziale w eksporcie z Polski ogółem. W ciągu dziesięciu lat wzrósł on z 0,37% do nieco ponad 1%, czyniąc z urządzeń i sprzętu medycznego jedną z polskich specjalności eksportowych.

Paradoksalnie, sukces eksportowy jest odwrotnie proporcjonalny do tego, co dzieje się na rynku krajowym, w którym polscy producenci mają stosunkowo niewielki udział – według szacunków wynosi on kilkanaście procent. Szansą na rozwój dla branży okazała się ekspansja zagraniczna, którą znacząco ułatwiło przystąpienie Polski do Unii Europejskiej i możliwość konkurowania na rynku wspólnotowym.

– Rynek wyrobów medycznych w Polsce opiera się wciąż w większości na imporcie, ale eksport rzeczywiście wzrasta w ogromnym tempie. Jest to zasługa polskich przedsiębiorców i ich dynamicznego działania – mówi Arkadiusz Grądkowski, dyrektor generalny Izby POLMED zrzeszającej polskich producentów sprzętu medycznego. Polskie produkty są coraz bardziej zaawansowane pod względem technologicznym i muszą spełniać te same wymogi jakościowe określane przez regulacje unijne, co np. produkty niemieckie czy francuskie.

Do zalet polskich produktów niewątpliwie można zaliczyć wysoką jakość w połączeniu z przystępną ceną, niezawodność, kompatybilność z wyrobami innych producentów oraz elastyczność w podejściu do wymagań klienta. Główne kategorie produktów obejmują m.in. sprzęt ortopedyczny i rehabilitacyjny, narzędzia medyczne i weterynaryjne, meble szpitalne, wyposażenie sal operacyjnych i oddziałów intensywnej terapii, a także urządzenia diagnostyczne (aparaty rentgenowskie i skanery ultradźwiękowe), sprzęt jednorazowego użytku, a ostatnimi czasy – również urządzenia i usługi telemedyczne.

Rynek wart setki miliardów dolarów

Według Fortune Business Insights, globalny rynek urządzeń medycznych w 2018 roku był wart 425 mld dolarów. Także prognozy tej instytucji wskazują, że do 2025 roku powiększy się on o kolejne 190 mld, rosnąc w tym czasie nieco ponad 5% rok do roku. Wzrost ten napędzany jest zarówno zmianami demograficznymi oraz stylem życia i wynikającymi z nich konsekwencjami zdrowotnymi, jak i starzejącą się infrastrukturą szpitalną.

Już wkrótce jedną piątą ogółu społeczeństwa w Unii Europejskiej będą stanowili seniorzy, w Japonii zaś – aż jedną trzecią. Starzejące się społeczeństwo oraz rosnąca globalna populacja – Organizacja Narodów Zjednoczonych przewiduje, że w ciągu następnej dekady urośnie o kolejny miliard, do 8,6 mld ludzi, by w 2050 roku dobić do blisko 10 mld – to nie jedyne wyzwania, z którymi będą musiały się zmierzyć systemy opieki zdrowotnej.

Mało higieniczny tryb życia, brak sportu i śmieciowe jedzenie sprzyjają otyłości, cukrzycy oraz chorobom serca i nowotworom. W samych Chinach i Indiach liczba diabetyków szacowana jest na 200 mln. Na świecie jest ich już ponad 400 mln, a w ciągu kolejnych kilkunastu lat liczba ta wzrośnie o połowę. Jak podaje WHO (Światowa Organizacja Zdrowia), w 2018 roku było 466 mln osób głuchych oraz niedosłyszących, co stanowi solidny rynek dla aparatów słuchowych i urządzeń wspomagających słyszenie. Co trzy sekundy ktoś na świecie zapada na demencję.

Problemy zdrowotne to jedno, a starzejąca się infrastruktura szpitalna – to drugie. W Europie i Stanach Zjednoczonych głównym wyzwaniem w tym obszarze jest wykorzystanie technologii (w tym również informatycznych) do tego, by zmniejszyć koszty, przy jednoczesnym zwiększeniu dostępności i jakości opieki zdrowotnej. Podczas gdy w krajach rozwiniętych starzejąca się infrastruktura czeka na modernizację, w państwach rozwijających się musi być ona w wielu przypadkach zbudowana od podstaw.

Pomimo tych różnic można jednak zauważyć wspólny dla wszystkich trend. Zarówno państwa rozwijające się, jak i coraz częściej rozwinięte, poszukują wysokiej jakości wyrobów za niższą cenę, co pozwoliłoby zredukować koszty, zachowując przy tym wysoki poziom świadczenia usług.

Eksport do krajów spoza Unii rośnie szybciej

Nic więc dziwnego, że producenci sprzętu medycznego szukają nowych kontaktów biznesowych na zagranicznych rynkach. Według danych Narodowego Banku Polskiego, ponad 60% firm z tej branży w większym lub mniejszym stopniu sprzedaje swoje wyroby za granicę. Jeszcze w 2018 roku dwie trzecie wartości całego eksportu przypadało na kraje unijne, jednak ostatnimi czasy proporcja ta mocno się zmieniła. Za sprawą dynamicznie rosnącego eksportu do Stanów Zjednoczonych, w 2019 roku sprzedaż do krajów UE stanowiła już „tylko" 53% wartości całego eksportu branży.

Niemcy, które od dawna były odbiorcą numer jeden sprzętu medycznego z Polski, zostały zdetronizowane przez Stany Zjednoczone, do których sprzedaż wzrosła dwukrotnie w porównaniu do roku poprzedniego i osiągnęła wartość 530 mln euro. Kwota ta robi ogromne wrażenie, zwłaszcza że na przestrzeni ostatniej dekady średnia wartość eksportu z Polski do USA jest trzykrotnie niższa (170 mln euro – przyp. red). Czy ten trend będzie stały? Trudno stwierdzić. Z podobnym zjawiskiem mieliśmy do czynienia kilka lat wstecz, kiedy to wystrzelił eksport do Danii i stała się ona drugim największym importerem sprzętu z Polski zaraz po Niemczech. Jednak już rok później Duńczycy zrobili dużo mniejsze zakupy…

W latach 2015–2019 eksport z Polski najszybciej rósł właśnie do państw spoza Unii – z 410 mln do 1134 mln euro, a głównymi odbiorcami były Stany Zjednoczone (584 mln euro), Rosja (71,5 mln euro), Ukraina (62,3 mln euro), Kanada (58,8 mln euro) oraz Chiny (51 mln euro). Natomiast eksport do UE nadal stanowi większość – w 2019 roku osiągnął wartość 1286 mln euro, a piątkę największych odbiorców tworzyły Niemcy (530 mln euro), Dania (180 mln euro), Francja (143 mln euro), Wielka Brytania (104 mln euro) oraz Holandia (54,5 mln euro).

Warto też zwrócić uwagę na rosnący eksport (choć z niskiej kwoty bazowej) do bardziej „egzotycznych" państw, takich jak Meksyk, Japonia, RPA czy Australia. Jego wartość nie jest być może wysoka (odpowiednio 19,7 mln euro, 15,3 mln euro, 7,7 mln euro oraz 13,5 mln euro), za to jest o wiele wyższa od średniej 10-letniej i pokazuje, że polscy przedsiębiorcy cały czas szukają nowych rynków zbytu.

– Od lat głównym towarem eksportowym branży są meble medyczne (np. stoły operacyjne itp.) czy też wyroby do indywidualnego zaopatrzenia pacjenta (takie jak ortezy, wózki czy peruki), które zdołały już sobie wyrobić renomę. Jednak portfolio polskich producentów wciąż się rozszerza – wskazuje Grądkowski.

Według wolumenu, dwie największe kategorie eksportowe polskiej branży to sprzęt ortopedyczny, protezy i aparaty słuchowe, których wartość sprzedaży za granicę wyniosła ponad 1,2 mld euro (52% całości eksportu branży), oraz narzędzia medyczne i weterynaryjne – ich eksport wyniósł 962 mln euro (37% eksportu).

Kolejne kategorie eksportowe, jednak już o znacznie mniejszym wolumenie sprzedaży, stanowią sprzęt do mechanoterapii i aparaty do masażu (2,7% – 70 mln euro), respiratory i maski gazowe (2,8% – 67,8 mln euro) oraz aparaty rentgenowskie (2,2% – 49 mln euro).

Wyzwania związane z zagraniczną ekspansją

– Rynek polskich producentów wyrobów medycznych składa się głównie z małych i średnich firm, które są elastyczne i szybko przystosowują się do zmieniających potrzeb rynku czy też wymagań i oczekiwań pacjentów. Nie należy jednak zapominać, że mamy też firmy z globalnym doświadczeniem, które osiągnęły już ogromne sukcesy

międzynarodowe i od lat eksportują swoje produkty do ponad 90 krajów na całym świecie – wyjaśnia dyrektor Grądkowski.

Do takich firm o globalnym zasięgu można zaliczyć między innymi specjalizujący się w produkcji stentów Balton, HTL-strefę, czyli największego na świecie producenta tzw. lancetów bezpiecznych, a także zajmującą się produkcją ultrasonografów firmę Echo-Son, której urządzenia znajdziemy w ponad 50 krajach. Echo-Son działa wyłącznie w modelu b2b z lokalnymi dealerami – jest to bardzo mocno rozdrobniona sieć i żaden z dystrybutorów nie ma dla spółki znaczenia strategicznego. Jednym z nich jest międzynarodowy koncern Abbot, wymagający partner, który oferuje na norweskim rynku skanery pęcherza PINIT marki Echo-Son. Jak mówi Zbigniew Woźniak, prezes zarządu puławskiej spółki, był to nasz ogromny sukces, że sprostaliśmy ich wymaganiom i oczekiwaniom. Ta współpraca trwa już kilka lat. Ostatnim hitem firmy z Puław jest skaner oftalmologiczny PIROP, którego zasięg sprzedaży obejmuje obszar od Wenezueli po Indonezję.

– Wejście na dany rynek zależy od wielu czynników. Przede wszystkim od determinacji producenta. Jednak mogą pojawić się trudności, które, mimo największej chęci, są ciężkie do pokonania – np. sytuacja polityczna w danym kraju, duża biurokracja, bariery prawne, różnice kulturowe, czy wymóg złożenia kosztowej dokumentacji niezbędnej do wprowadzenia wyrobu na rynek. Takie kwestie często zniechęcają do podjęcia decyzji o wejściu na nowe rynki – wskazuje dyrektor Izby POLMED.

Na pewno przyda się bardzo wnikliwe rozeznanie rynku, zwłaszcza w tych regionach, które na pierwszy rzut oka mogą wydawać się bardzo atrakcyjne ze względu na tkwiący w nich potencjał wzrostu i zapotrzebowanie na sprzęt i usługi medyczne. Dla przykładu, obszar Azji i Pacyfiku zamieszkuje już ponad połowa globalnej populacji, a dostęp do nowoczesnej opieki zdrowotnej dla większości pacjentów jest bardzo ograniczony. Zapotrzebowanie ciągle rośnie, a jak wskazują analizy McKinseya, podaż przestaje już nadążać za popytem. Jest to jednak rynek bardzo wymagający i trudny, przede wszystkim zaś ogromnie zróżnicowany – pod względem politycznym, kulturowym, prawnym czy też rozwoju ekonomicznego, a nawet zachorowalności na określone jednostki chorobowe.

Dla przedsiębiorstw, które dopiero rozpoczynają zagraniczną ekspansję, dobrym punktem wyjścia jest uczestnictwo w targach branżowych oraz konsekwentne budowanie świadomości marki podczas tego typu wydarzeń. Taką strategię przyjęła firma Alvo Medical ze Śmigla, która od kilkunastu lat cieszy się statusem przedsiębiorstwa o międzynarodowym zasięgu i dostarcza najwyższej jakości wyposażenie dla sal operacyjnych – jej *showroomy* są zlokalizowane na kilku kontynentach, m.in. w Europie, Afryce oraz w Azji.

Początki ekspansji nie były jednak łatwe. Pomimo tego, że firma od 1998 roku brała udział w międzynarodowych targach medycznych, przez pierwsze lata nie udało się jej pozyskać zagranicznych klientów. Jednak konsekwentna obecność na takich targach jak MEDICA w Düsseldorfie czy Arab Health w Dubaju opłaciła się – kontakty nawiązane podczas wcześniejszych edycji w końcu zostały przekute w kontrakty.

Pierwszym klientem Alvo był dystrybutor sprzętu medycznego w Kairze. Kontakt z nim udało się nawiązać podczas 5. edycji targów medycznych w regionie. – To budowanie świadomości marki. Klient wiedział, że jesteśmy na targach co roku, że się rozwijamy i co jakiś czas pokazujemy coś nowego. W końcu zdecydował się nawiązać z nami współpracę – mówi Tadeusz Olszewski, założyciel Alvo. W Egipcie spółka wyposażyła już kilkaset sal operacyjnych.

Kolejny kluczowy klient Alvo, dystrybutor z Arabii Saudyjskiej, przez cztery lata odwiedzał stoisko polskiej firmy na prestiżowych targach Arab Health – wymieniał uwagi, komentował, ale nie decydował się na złożenie zamówienia. – W końcu przyszedł raz jeszcze obejrzeć nasze stoisko i powiedział do mnie: „Widzę, że poprawiłeś parę rzeczy, na które zwracałem uwagę w poprzednich latach. Myślę, że powinniśmy nawiązać współpracę" – wspomina Olszewski. Arabia Saudyjska to drugi pod względem wielkości sprzedaży rynek dla spółki ze Śmigla. Firma jest tam już dobrze znana, a sale operacyjne wykonane przez polskie przedsiębiorstwo nierzadko wizytuje sam minister zdrowia.

Branżowy program promocji – szansa na nawiązanie kontaktów biznesowych

Firmy, których nie stać na wynajęcie własnego stoiska na targach lub chcą zwiększyć jeszcze bardziej zasięg, mogą skorzystać z gościny polskich stoisk informacyjno-promocyjnych, które są organizowane m.in. podczas dwóch największych imprez branżowych na świecie – MEDICA i Arab Health. Największą wartością dla przedsiębiorców jest możliwość nieodpłatnego skorzystania z przestrzeni do spotkań b2b, gdzie można zaprosić zagranicznych partnerów na umówione wcześniej spotkania biznesowe. Na stoisku można też prezentować materiały promocyjne – ulotki, foldery i filmy.

Takie stoiska od 2017 roku organizuje Polska Agencja Rozwoju Przedsiębiorczości na zlecenie Ministerstwa Rozwoju, Pracy i Technologii, obecnie w ramach Branżowego Programu Promocji sektora sprzętu medycznego, finansowanego z Funduszy Europejskich. – Z promocji na organizowanych do tej pory stoiskach narodowych każdorazowo skorzystało ponad 150 polskich firm. Jeśli sytuacja pozwoli, do końca 2022 roku zorganizujemy osiem stoisk w Europie, Azji i w Ameryce Północnej – mówi Michał Polański, dyrektor Departamentu Wsparcia Przedsiębiorczości PARP.

W czasach pandemii, kiedy wszystkie najważniejsze stacjonarne wydarzenia branżowe zostały odwołane, Agencja zdecydowała się na organizację międzynarodowych spotkań b2b online za pośrednictwem specjalnie zaprojektowanej platformy internetowej. Do udziału w Med2Meet zgłosili się uczestnicy z 46 państw – 105 z Polski i aż 188 z pozostałych krajów.

Med2Meet nie tylko wypełnił lukę po stacjonarnych wydarzeniach branżowych, które nie mogą się odbywać ze względu na pandemię, ale też ułatwił

wielu polskim MŚP dotarcie do partnerów biznesowych z odległych zakątków świata – w wirtualnych spotkaniach b2b udział wzięło m.in. ponad 50 uczestników z Azji, Bliskiego Wschodu, Afryki oraz Ameryki Północnej.

Najbliższą okazją do tego, by po kilkunastomiesięcznej przerwie spowodowanej pandemią ponownie spotkać się twarzą w twarz z zagranicznymi partnerami biznesowymi, będą targi Arab Health w Dubaju, gdzie w dniach 21–24 czerwca 2021 r. zorganizowane zostanie również polskie stoisko informacyjno-promocyjne.

COVID-19 „akceleratorem" usług telemedycznych?

Analitycy rynku medycznego zwracają uwagę, że z powodu pandemii przełożono lub anulowano miliony zabiegów planowych, aby móc obsłużyć pacjentów zarażonych SARS-CoV-2. Tym samym spadło zapotrzebowanie na takie produkty jak implanty ortopedyczne, zastawki, soczewki czy urządzenie do diagnostyki słuchu. Wzrosło zaś na pulsoksymetry, aparaturę podtrzymującą życie (głównie respiratory) oraz strzykawki i igły wykorzystywane do szczepień. To jednak nie jedyne następstwa pandemii, która może być również katalizatorem zmian w sposobie świadczenia wybranych usług medycznych – konsultacji lekarskich, a nawet badań.

Według prognoz Global Market Insights, globalny rynek rozwiązań dla telemedycyny będzie rósł w tempie blisko 20% rocznie w ciągu najbliższych pięciu lat, osiągając niebagatelną wartość 175 mld dolarów. Wydaje się, że pandemia SARS-CoV-2 może ten trend jeszcze przyspieszyć. Dystans społeczny jest jedną z głównych strategii ograniczających rozprzestrzenianie się koronawirusa. Większość państw, w których pojawił się SARS-CoV-2, na pewnym etapie wprowadziła całkowity lub częściowy *lockdown*. W takich warunkach telemedycyna była (a w wielu przypadkach nadal jest) w zasadzie jedyną możliwością uzyskania konsultacji medycznych przez pacjentów.

Pierwszą polską firmą telemedyczną, która z sukcesami dokonała ekspansji zagranicznej, jest Medicalgorithmics. Założona w 2005 roku przez Marka Dziubińskiego firma zatrudnia około 500 osób na całym świecie, a jej usługi są dostępne w Ameryce Północnej, Europie Zachodniej w Południowo-Wschodniej Azji, w tym w Australii. Co roku, Medicalgorithmics diagnozuje zdalnie pracę serca u 150 tysięcy pacjentów pod kątem arytmii, używając w tym celu urządzenia o nazwie PocketECG oraz zaawansowanych algorytmów sztucznej inteligencji.

Co ważne, Medicalgorithmics udało się skomercjalizować usługi telemedyczne w Stanach Zjednoczonych, jednym z najbardziej wymagających rynków na świecie. Tak naprawdę to był to pierwszy rynek, na którym firma z Warszawy stawiała komercyjne kroki. Dlaczego? Otóż to właśnie tam wielodobowy monitoring serca podlega w całości refundacji. – W branży medycznej największym wyzwaniem nie jest stworzenie produktu, a jego komercjalizacja. Wymyślenie fajnego rozwiązania, nawet jeśli ktoś chce je kupić,

nie jest gwarantem tego, że ono się sprzeda. Problem polega na tym, że kupujący nie nabywa sprzętu za własne pieniądze, a ze środków ubezpieczyciela. Żeby skomercjalizować produkt, musimy wcześniej wiedzieć, jak wyglądają mechanizmy płatności – mówi prezes Dziubiński. Jego zdaniem jest to jedna z bardziej skomplikowanych branż pod kątem zrozumienia zależności pomiędzy interesariuszami.

Firmie udało się jednak nakłonić partnerów z innych państw do tego, by skorzystali z usług Medicalgorithmics, ponieważ jest to dla nich nadal opłacalne, nawet jeśli wielodobowy monitoring serca nie jest objęty refundacją. Dla przykładu w Danii, która jest jednym z prężniej rozwijających się rynków dla tej warszawskiej firmy, wiele szpitali zaprzestało tradycyjnych sesji holterowych, w zamian zaś wprowadziło usługi Medicalgorithmics. Ostatnio zaś firma podpisała umowy w kolejnych państwach, gdzie nie ma refundacji tego typu usług – w Austrii, Hiszpanii i Szwajcarii.

– Kliniczne, operacyjne i finansowe zalety usługi opartej na naszej technologii sprawiają, że ciągle jesteśmy lepsi od światowej konkurencji, co przekłada się na wzrost biznesu poza Stanami Zjednoczonymi. System jest online i daje zarówno możliwość zapisu najwyższej jakości sygnału EKG, jak i dostępu do danych diagnostycznych pacjenta w czasie rzeczywistym. Gdy pacjent jest w domu z naszym urządzeniem, lekarz może zdalnie podjąć decyzję jak długo chce jeszcze danego pacjenta diagnozować – mówi Jarosław Jerzakowski, dyrektor ds. międzynarodowego rozwoju biznesu w Medicalgorithmics.

Wpływ efektu pandemii na sposób świadczenia usług telemedycznych widoczny jest również na przykładzie firmy prezesa Dziubińskiego. Na popularności zyskuje model *„ship to patients home"*, czyli bezpośrednia wysyłka urządzenia do domu pacjenta, bez konieczności fatygowania go po osobisty odbiór do szpitala. O ile w Kanadzie taki model dominował już wcześniej (98% badanych), o tyle w Stanach odsetek ten znacząco zwiększył się z powodu pandemii i wynosi już blisko 50% wszystkich badań wykonywanych przez Medicalgorithmics.

Jarosław Jerzakowski przewiduje, że na rozwój Medicalgorithmics będzie miał też wpływ aspekt zdrowotny związany z COVID-19, ponieważ choroba ta wywołuje zaburzenia rytmu serca, co zostało już opisane w kilku publikacjach naukowych. Do tego dojdzie potrzeba outsourcingu usług kardiologicznych, aby ograniczyć ryzyko niewydolności systemu opieki zdrowotnej, kiedy osoby z chorobami serca wznowią wstrzymane na czas pandemii wizyty u kardiologów.

Rynek telemedyczny to przede wszystkim domena startupów, które nierzadko wykorzystują algorytmy sztucznej inteligencji do tego, by wspomagać pracę lekarzy. Rynek ma ogromny potencjał wzrostu, ale bariery wejścia są bardzo wysokie, a czas potrzebny od opracowania gotowej wersji rozwiązania do jego komercjalizacji – stosunkowo długi. Wymagane są badania kliniczne, pilotaże i niezbędne certyfikaty. Do tego dochodzą różnice w architekturze systemów opieki zdrowotnej państw, strukturze interesariuszy czy świadczeń objętych refundacją. Niełatwo jest też znaleźć inwestorów gotowych wyłożyć kapitał na ryzykowne przedsięwzięcie. Z tych też powodów niewielu firmom udaje się skomercjalizować rozwiązania, nad którymi nierzadko pracują całe lata.

Eryk Rutkowski
Departament Wsparcia
Przedsiębiorczości PARP

Dyrektywa o ochronie praw sygnalistów

„Blockbuster" na miarę RODO?

Błażej Wągiel

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii, zwana powszechnie dyrektywą o ochronie praw sygnalistów, zacznie obowiązywać już 17 grudnia 2021 r. Nakłada ona na przedsiębiorców, co warto podkreślić – nie tylko tych dużych, wiele nowych obowiązków związanych z zapewnieniem szeroko pojętej zgodności organizacji w obszarze ochrony sygnalistów. Co istotne, podmioty zatrudniające powyżej 250 pracowników są zobowiązane do wdrożenia odpowiednich mechanizmów raportowania nieprawidłowości już od 17 grudnia 2021 r. Natomiast dla podmiotów zatrudniających od 50 do 249 pracowników okres ten został wydłużony tj. do 17 grudnia 2023 r.

Czy dyrektywa o ochronie sygnalistów zmieni zasady gry w zakresie compliance przedsiębiorstw działających na terenie Polski? Z pewnością. W jakiej skali? Trudno powiedzieć. Wszak do tej pory nie ma nawet projektu polskiej ustawy mającej wdrożyć dyrektywę, a to w niej znajdą się kluczowe dla przedsiębiorców szczegóły. Jednak jedno jest pewne – to idealny moment na bliższe poznanie nowych regulacji i sposobów reagowania na zgłaszane przez sygnalistów wątpliwości.

Etiologia wdrożenia dyrektywy o ochronie praw sygnalistów

Zacznijmy od początku. Jak to się w ogóle stało, że Unia Europejska (UE) wprowadziła rewolucję w zakresie ochrony sygnalistów?

Do tej pory bowiem ochrona sygnalistów była domeną raczej systemu anglosaskiego, o czym świadczy m.in. bogaty dorobek amerykańskiej kinematografii. W obszarze Europy kontynentalnej, zwłaszcza w krajach byłego bloku wschodniego, anonimowe zgłaszanie nieprawidłowości kojarzyć się mogło, delikatnie mówiąc, negatywnie.

Do czasu. W ostatnich latach sygnaliści ujawnili szereg skandali związanych m.in. z uchylaniem się od płacenia podatków i naruszeniami konkurencji. Jeśli w przypadku afery Panama Papers tożsamość sygnalistów pozostała anonimowa, to sygnaliści Antoine Deltour i Raphaël Halet ujawniający aferę LuxLeaks pozostali praktycznie bez jakiejkolwiek ochrony prawnej. Dotychczasowy brak regulacji na poziomie unijnym oraz rozbieżności między przepisami poszczególnych państw członkowskich regulującymi ochronę sygnalistów powodował zatem, że niektórzy sygnaliści w ogóle nie korzystali z ochrony.

W wyniku takich ujawnień UE dostrzegła rolę sygnalistów w skutecznym wykrywaniu przypadków naruszenia prawa, na etapie postępowań wyjaśniających i ścigania tych naruszeń. W marcu 2017 r. rozpoczęły się prace nad europejskimi ramami ochrony sygnalistów. Rozwiązania przyjęte przez Parlament UE mają znaleźć szerokie zastosowanie w obszarach takich jak:

- zamówienia publiczne,
- ochrona środowiska,
- zdrowie publiczne,
- ochrona żywności,
- cyberbezpieczeństwo,
- ochrona danych osobowych.

Sytuacja sygnalistów w Polsce

W polskim porządku prawnym nie ma jednej kompleksowej regulacji zapewniającej ochronę sygnalistów. Żaden z aktów prawnych nie zawiera też definicji osoby, która zgłasza naruszenia.

Przepisy służące ochronie sygnalistów można znaleźć m.in. w:

- ustawie o Policji,
- kodeksie postępowania karnego,
- ustawie o ochronie i pomocy dla pokrzywdzonego i świadka,
- prawie pracy,
- ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

W kodeksie postępowania karnego znajdziemy regulacje dotyczące ochrony osób składających zawiadomienie o przestępstwie. Te instytucje to: świadek incognito, utajnienie zeznań stanowiących podstawę wniosku o tymczasowe aresztowanie i utajnienie danych dotyczących świadków i pokrzywdzonych występujących w postępowaniu karnym.

Ustawa o ochronie i pomocy dla pokrzywdzonego i świadka stanowi implementację dyrektywy europejskiej 2012/29 UE. Ustawa ta zawiera rozwiązania, które mają zapewnić kompleksową ochronę życia i zdrowia pokrzywdzonych i świadków będących uczestnikami postępowania karnego oraz ochronę tych osób przed odwetem lub zastraszaniem w związku z tym postępowaniem karnym. Wprowadza ona przede wszystkim środki takie jak: ochrona osobista świadka i pokrzywdzonego, pomoc w zakresie zmiany miejsca pobytu czy udzielenie pomocy finansowej.

W prawie pracy znajdziemy rozwiązania, które w założeniu mają chronić pracowników w przypadku ujawnienia naruszeń. Zakaz dyskryminacji czy przeciwdziałanie mobbingowi zawarte w kodeksie pracy sprawiają, że przynajmniej teoretycznie zachowanie pracownika ujawniające nieprawidłowości nie może stanowić dla niego negatywnych konsekwencji w postaci np. rozwiązania stosunku pracy. Mimo zawarcia w kodeksie pracy tych rozwiązań coraz częściej w mediach pojawiają się informacje o zwalnianiu pracowników

z powodu ujawnienia takich informacji. Oczywiście można podnieść, że sygnaliści zwolnieni w ten sposób mają możliwość dochodzenia swoich praw w sądzie, zawiadamiać prokuraturę czy nawet Rzecznika Praw Obywatelskich. Jednak po pierwsze taki sygnalista musiałby wykazać się samozaparciem w dochodzeniu do prawdy, a po drugie musiałby liczyć się z koniecznością udowodnienia, że swoim działaniem nie zaszkodził reputacji pracodawcy lub nie przyczynił się swoim zachowaniem do naruszeń, które zgłosił.

Podkreślenia wymaga jeszcze, że przepisy dotyczące ochrony sygnalistów w prawie pracy odnoszą się tylko do stosunków pracy. Oznacza to, że inne formy, takie jak np. umowa zlecenia czy umowa o dzieło, nie skorzystają z ochrony tam zawartej.

Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu odgrywa kluczową rolę w zapewnieniu bezpieczeństwa w obszarze usług finansowych. Dlatego też ustawodawca zawarł w niej mechanizmy, które mają wspierać i chronić sygnalistów zgłaszających naruszenia w tym sektorze. Ustawa ta nakłada obowiązek opracowania i wdrożenia wewnętrznej procedury anonimowego sygnalizowania rzeczywistych lub potencjalnych naruszeń przepisów. Ponadto ustawa ta w art. 53 wskazuje elementy, jakie powinna zawierać procedura zgłaszania naruszeń. Elementy te mogą być wskazówką podczas wdrażania systemu ochrony sygnalistów po 17 grudnia 2021 r.

Jak widać, w Polsce istnieje kilka rozwiązań, które dotyczą ochrony osób zgłaszających naruszenia. Nie można jednak uznać ich za spójny i wzajemnie uzupełniający się system. Stanowi to zdecydowaną przeszkodę w zakresie zgłaszania nieprawidłowości przez sygnalistów; nie mogą oni mieć pewności, że w razie ujawnienia naruszeń zapewnione zostanie im bezpieczeństwo. Nie ma się czemu dziwić – głównym celem przytoczonych regulacji nie była ochrona sygnalistów. Pokazuje to tylko, że w polskim porządku prawnym jest miejsce i potrzeba na kompleksowy akt prawny regulujący te kwestie.

Jakich zmian należy się spodziewać po 17 grudnia 2021 r.?

Zacznijmy od podmiotów, które będą zobowiązane do wdrożenia procedur zgodnych z dyrektywą. Dyrektywę zobowiązane będą wdrożyć wszystkie podmioty prawne w sektorze publicznym. Dotyczy to również podmiotów będących własnością lub znajdujących się pod kontrolą takich podmiotów. Ponadto przewiduje się, że procedury zgłaszania nieprawidłowości mają zostać wprowadzone przez podmioty, które zatrudniają co najmniej 50 pracowników. To nie koniec. Państwa członkowskie mogą zobowiązać podmioty w sektorze prywatnym, które zatrudniają mniej niż 50 pracowników, do ustanowienia wewnętrznych kanałów i procedur dokonywania zgłoszeń przez sygnalistów. Procedury te będą też zobowiązani wdrożyć mikro- i mali przedsiębiorcy, jeśli w ramach swojej działalności biorą udział w przetargach na zamówienia publiczne lub wykorzystują środki unijne.

Dyrektywa obejmie swoją ochroną także te kategorie osób, które, mimo braku zatrudnienia u danego pracodawcy i nieotrzymywania wynagrodzenia, mogą doświadczyć działań odwetowych za zgłoszenie naruszeń. Chodzi tutaj przede wszystkim o stażystów i wolontariuszy.

Zmiany wprowadzone dyrektywą wymagać będą od przedsiębiorców przede wszystkim utworzenia bezpiecznych kanałów raportowania. Bezpieczne kanały raportowania to narzędzia (w formie programu informatycznego lub innego powszechnie przyjętego w organizacji sposobu, np. fizycznej skrzynki pocztowej lub gorącej linii), które umożliwiać będą swobodne zgłaszanie naruszeń bez obawy o ujawnienia tożsamości.

Dyrektywa przewiduje dokonywanie zgłoszeń przez trzy rodzaje kanałów raportowania – wewnętrzny, zewnętrzny i publiczny. W pierwszej kolejności sygnalista powinien wykorzystać wewnętrzny kanał raportowania i dokonać zgłoszenia np. pracodawcy. Wobec tego pracodawcy będą zmuszeni do stworzenia i wdrożenia skutecznych procedur raportowania o nieprawidłowościach oraz monitoringu wpływających zgłoszeń.

Dyrektywa pozostawia pracodawcom wybór co do organizacji obsługi wewnętrznego kanału raportowania zgłoszeń. Może on być obsługiwany w ramach organizacji (poprzez np. zwiększenie zakresu obowiązków Inspektora Ochrony Danych lub wyznaczenie innej osoby lub działu) albo zadania te mogą zostać zlecone na zasadach outsourcingu podmiotowi dającemu gwarancję poufności i ochrony danych objętych zleceniem (np. kancelarii prawnej lub zewnętrznemu dostawcy oprogramowania do zgłaszania nieprawidłowości).

Parlament dostrzegł też, że niewłaściwe lub niedziałające procedury ochrony sygnalistów są słabym punktem wielu systemów i mogą negatywnie wpłynąć na liczbę zgłoszeń. Dlatego dyrektywa nakłada na państwa członkowskie obowiązek wprowadzenia u pracodawców (publicznych i prywatnych) mechanizmów monitorowania skuteczności kanałów wewnętrznych poprzez wprowadzenie ewidencji każdego zgłoszenia otrzymanego poprzez wewnętrzny kanał raportowania.

Niestety dyrektywa nie określa, jak taki monitoring będzie wyglądał. W tym zakresie należy poczekać na ustawę krajową. Jednak zasadne wydaje się, by przynajmniej w pierwszym okresie obowiązywania dyrektywy pracodawcy rejestrowali wszystkie zgłoszenia

(łącznie z tymi, które uznano za niezasadne i nie przeprowadzano postępowania wyjaśniającego) także te świadomie fałszywe.

W przypadku zewnętrznych kanałów raportowania dyrektywa przewiduje ich regularny audyt tzn. co najmniej raz na trzy lata. W wyniku takich audytów organy kontrolne mają dopracować istniejące uregulowania i zdobyć doświadczenie, które pozwoli jeszcze lepiej chronić sygnalistów.

Dodatkowo kraje członkowskie będą corocznie przekazywać Komisji Europejskiej raport zawierający liczbę zgłoszeń oraz liczbę podjętych postępowań wyjaśniających. Raport ma też zawierać wyliczenie szacunkowych szkód oraz informacje o środkach, jakie odzyskano w wyniku podjętych na podstawie zgłoszenia postępowań wyjaśniających. Ma się to przyczynić do poprawy skuteczności aktualnych środków ochrony sygnalistów na poziomie unijnym. Należy się więc spodziewać, że prawodawca będzie kładł szczególny nacisk na zebranie tych danych od pracodawców.

A co z sankcjami? Wiemy tyle, że mają być skuteczne, proporcjonalne i odstraszające. Ich zakres oraz wysokość pozostawiono krajom członkowskim. Tylko w taki sposób państwa członkowskie będą w stanie zapewnić skuteczność przepisów dotyczących ochrony sygnalistów oraz zapobiegania działaniom odwetowym.

Jakie wymagania muszą spełniać procedury zgłaszania nieprawidłowości w firmie?

Dyrektywa zwraca uwagę na konieczność zapewnienia, by wdrażane przez pracodawców procedury umożliwiały zachowanie pełnej poufności oraz uniemożliwiały (bezpośrednio lub pośrednio) identyfikację osoby sygnalisty. Zapewnienie anonimowości sygnalistów nie będzie mogło być iluzoryczne bowiem na pracodawcach ciążyć będzie obowiązek przeprowadzenia testu skuteczności kanału raportowania.

Nieuprawnieni pracownicy, którzy nie są wyraźnie umocowani do odbioru zgłoszeń w utworzonej polityce informowania o nieprawidłowościach, nie powinni mieć dostępu do zgłoszenia. Sygnaliści muszą mieć zapewnioną możliwość zgłaszania naruszeń w sposób anonimowy pisemnie lub ustnie. Zgłoszenie ustne powinno być dokonywane telefonicznie lub za pośrednictwem innych wdrożonych w organizacji systemów komunikacji głosowej, ale też, na wniosek sygnalisty, w wyniku bezpośredniego spotkania zorganizowanego w rozsądnym terminie. W przypadku zgłoszeń pisemnych, niezależnie od wyboru formy komunikacji (tj. skrzynka pocztowa, dedykowany adres e-mail, system informatyczny), musi ona spełniać kryteria anonimowości i poufności.

Oprócz oczywistych wymogów, takich jak zapewnienie sygnalistom możliwości anonimowego zgłaszania naruszeń i związanych z tym procedur ochrony danych osobowych, pracodawcy zobowiązani będą również podjąć działania następcze wynikające ze zgłoszeń sygnalistów. Działania następcze mają doprowadzić do zbadania i oceny prawdziwości zarzutów zawartych w zgłoszeniu oraz zaradzenia naruszeniom będącym przedmiotem zgłoszenia. Polegać one mają w szczególności na dochodzeniu wewnętrznym, postępowaniu wyjaśniającym oraz podjęciu wszelkich możliwych działań mających na celu zapobieżenie incydentom objętym zgłoszeniem w przyszłości.

Wobec powyższego dyrektywa wskazuje, że procedury na potrzeby zgłoszeń wewnętrznych i działań następczych powinny obejmować takie elementy jak:

- kanały przyjmowania zgłoszeń zaprojektowane, ustanowione i obsługiwane w sposób zapewniający poufność i ochronę tożsamości sygnalisty (ale też osoby trzeciej wymienionej w zgłoszeniu) oraz uniemożliwiające uzyskanie do nich dostępu osobom nieupoważnionym,
- wyznaczenie bezstronnych osób lub działu właściwego do podejmowania działań następczych w związku ze zgłoszeniami oraz do komunikacji z sygnalistą,
- ustalenie rozsądnego terminu na przekazanie informacji zwrotnych (nie dłuższego jednak niż trzy miesiące od potwierdzenia otrzymania zgłoszenia),
- zapewnienie zrozumiałych i łatwo dostępnych informacji na temat procedur na potrzeby dokonywania zgłoszeń zewnętrznych do właściwych organów.

Jaką ochronę przed działaniami odwetowymi zyskają sygnaliści?

Zacznijmy od tego, czym są działania odwetowe. To bezpośrednie lub pośrednie działania lub zaniechania mające miejsce w kontekście związanym z pracą, które są spowodowane zgłoszeniem wewnętrznym lub zewnętrznym lub ujawnieniem publicznym i które wyrządzają lub mogą wyrządzić nieuzasadnioną szkodę dla sygnalisty.

Dyrektywa kładzie szczególny nacisk na przeciwdziałanie tego typu działaniom – przyjęto bowiem domniemanie, że osoby dokonujące zgłoszenia informacji na temat naruszeń lub dokonujące ujawnienia publicznego nie naruszają żadnych ograniczeń w zakresie ujawniania informacji i nie ponoszą żadnej odpowiedzialności w związku ze zgłoszeniem pod warunkiem, że miały uzasadnione podstawy, by sądzić,

że ujawnienie takich informacji jest niezbędne do ujawnienia naruszenia. Dodatkowo sygnalista nie będzie ponosił odpowiedzialności w związku z uzyskaniem informacji będących przedmiotem zgłoszenia, jeśli takie uzyskanie nie stanowi odrębnego czynu zabronionego.

Ponadto w postępowaniach przed sądem lub innym organem rozpoznającym sprawę szkody, jaką poniósł sygnalista w związku z prowadzonymi wobec niego działaniami następczymi, obowiązywać będzie odwrócony ciężar dowodu. Oznacza to, że na osobie, która podjęła działania powodujące szkodę, spoczywać będzie ciężar udowodnienia, że działania te przeprowadziła z należycie uzasadnionych powodów.

Zgłaszanie nieprawidłowości a ochrona danych osobowych

Podczas tworzenia nowej dyrektywy słusznie uznano, że nie ma potrzeby tworzenia *lex specialis* dla nowych czynności przetwarzania. Wobec tego w zakresie ochrony danych osobowych dyrektywa wskazuje wprost, że ich przetwarzanie ma się odbywać zgodnie z rozporządzeniem (UE) 2016/679 i dyrektywą (UE) 2016/680 ze szczególnym uwzględnieniem zasad dotyczących przetwarzania danych osobowych określonych w art. 5 rozporządzenia (UE) 2016/679, art. 4 dyrektywy (UE) 2016/680 i art. 4 rozporządzenia (UE) 2018/1725. Jednak RODO nie zawiera wprost przepisów dotyczących ochrony danych osobowych sygnalistów. Nic dziwnego, nie było przecież tworzone w tym celu.

Gdzie zatem pracodawcy powinni szukać wskazówek? Pomocny może okazać się dokument o nazwie „Opinia 1/2006 w sprawie stosowania unijnych przepisów o ochronie danych do celów wewnętrznych systemu zgłaszania nieprawidłowości w zakresie rachunkowości, wewnętrzne kontrole księgowe, audyt, walka z przekupstwem, przestępstwami bankowymi i finansowymi" wywodzący się co prawda z czasów „przed RODO", niemniej jedyny zawierający ogólnounijne wytyczne dotyczące ochrony danych sygnalistów w sektorze prywatnym.

Wadą tego dokumentu jest też to, że skupia się na elementach, które były w tym czasie istotne. Dlatego warto mieć na uwadze, że nie obejmuje on swą treścią wszystkich obszarów objętych dyrektywą o ochronie praw sygnalistów.

Podsumowanie

Podobnie jak w wielu europejskich krajach w polskim porządku prawnym funkcjonują szczątkowe regulacje dotyczące zgłaszania naruszeń i ochrony sygnalistów. Są one jednak niespójne oraz stanowią barierę dla skutecznego ujawniania naruszeń i zapobiegania im. Aktualnie obowiązujące przepisy nie pozwalają sygnalistom mieć pewności, że w razie zgłoszenia naruszenia ich status będzie odpowiednio chroniony.

Prawodawca unijny na kanwie ostatnich afer ujawnionych przez sygnalistów, dostrzegając ich niebagatelną rolę w skutecznym wykrywaniu przypadków naruszenia prawa oraz brak właściwej ich ochrony w krajach członkowskich, podjął pracę nad wzmocnieniem ich ochrony.

Nowa dyrektywa unijna o ochronie praw sygnalistów, która ma zostać implementowana do polskiego porządku prawnego 17 grudnia 2021 roku nakłada na pracodawców szereg obowiązków, które mają zmienić ten stan, wzmacniając poziom i skuteczność ochrony sygnalistów przed ujawnieniem ich tożsamości i odwetem.

Istotne jest, że dyrektywa daje pracodawcom z sektora prywatnego i publicznego swobodę ustanowienia kanałów dokonywania zgłoszeń. Dzięki temu będą oni mogli dostosować swój system ochrony sygnalistów do swojej struktury organizacyjnej.

Nie jest jasne, jakie dokładnie sankcje będą przewidziane za naruszenie praw sygnalistów, jednak pewne jest, że przewidziane kary będą miały charakter karny, cywilny lub administracyjny.

Błażej Wągiel
radca prawny zarządzający kancelarią IPSO LEGAL (www.ipsolegal.pl), specjalista m.in. w dziedzinie prawa medycznego i farmaceutycznego, compliance oraz w obszarze tworzenia i rozwoju spółek; entuzjasta nowych technologii

Dyrektywa NIS 2

Jakie zmiany wprowadzi dla cyberbezpieczeństwa na rynku wewnętrznym UE?

Agnieszka Wachowska, Aleksander Elmerych

Na przestrzeni ostatnich lat coraz silniej można odczuć przyspieszający rozwój cyfryzacji, która jest obecnie jednym z podstawowych narzędzi niezbędnych do funkcjonowania i rozwoju przedsiębiorstw. Z uwagi na coraz większą przystępność cyfryzacji (zarówno w aspekcie organizacyjnym, jak i finansowym) korzystanie z narzędzi informatycznych w celu optymalizacji procesów biznesowych nie jest już domeną dużych przedsiębiorstw z zapleczem finansowym i technologicznym, lecz stało się powszechne również w sektorze mikro- i małych przedsiębiorców. Wraz ze wzrostem zainteresowania usługami cyfrowymi wśród przedsiębiorców i konsumentów, coraz więcej podmiotów decyduje się świadczyć tego rodzaju usługi, starając się sprostać oczekiwaniom i potrzebom rynku. Taki stan rzeczy, poza oczywistymi korzyściami wynikającymi z cyfryzacji gospodarki, rodzi również pewne zagrożenia – są one związane przede wszystkim z konsekwencjami awarii czy niedostępności kluczowych usług informatycznych, stanowiących podstawę funkcjonowania przedsiębiorstw, jak również z coraz częściej zdarzającymi się wyciekami danych osobowych czy informacji poufnych, czy też działaniami grup przestępczych wyspecjalizowanych w cyberprzestępczości, w tym coraz popularniejszymi atakami typu *ransomware*.

Motywy opracowania projektu dyrektywy NIS 2

Dostrzegając te zagrożenia, Unia Europejska w 2016 r. doprowadziła do uchwalenia dyrektywy NIS[1], która zobowiązywała państwa członkowskie do wprowadzenia w ustawodawstwie krajowym odpowiednich środków i mechanizmów dążących do zapewnienia bezpieczeństwa cyfrowego sieci i systemów informatycznych. W motywach wprowadzenia tej dyrektywy dostrzeżono zasadnicze znaczenie niezawodności i bezpieczeństwa sieci, systemów oraz usług informatycznych dla działalności gospodarczej i społecznej, w szczególności dla funkcjonowania unijnego rynku wewnętrznego. Wskazano również na coraz większą skalę i częstotliwość incydentów bezpieczeństwa, a także na ich wpływ na funkcjonowanie sieci i systemów informatycznych. Skutki ich wystąpienia są bowiem odczuwalne nie tylko na płaszczyźnie finansowej, lecz także wizerunkowej – doprowadzają do utraty zaufania użytkowników usług cyfrowych. Dyrektywa NIS dała jednak państwom członkowskim stosunkowo dużą dowolność w zakresie sposobu jej implementacji. Pozostawiła do ich decyzji m.in. kwestie ustalenia kryteriów identyfikacji operatorów usług kluczowych, a także środków technicznych i organizacyjnych koniecznych do podjęcia przez operatorów usług kluczowych i dostawców usług cyfrowych dla zarządzania ryzykiem, sposobu raportowania incydentów bezpieczeństwa czy środków nadzorczych i kontrolnych przysługujących odpowiednim organom państwowym. W Polsce dyrektywa NIS została implementowana ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[2].

Rozwój cyfryzacji w Unii Europejskiej na przestrzeni ostatnich lat był na tyle dynamiczny, że środki zapewnione dyrektywą NIS okazały się w ocenie organów unijnych niewystarczające dla zapewnienia odpowiedniego poziomu cyberbezpieczeństwa w państwach członkowskich. W związku z tym, w grudniu 2020 r. opublikowano projekt nowej dyrektywy NIS 2[3], która ma zastąpić obowiązującą dotychczas dyrektywę NIS i doprowadzić do większej harmonizacji przepisów z zakresu cyberbezpieczeństwa na terytorium Unii Europejskiej. Projekt dyrektywy jest elementem unijnego pakietu na rzecz zapewniania cyberbezpieczeństwa. W uzasadnieniu dla wprowadzenia nowej dyrektywy wskazano między innymi, że konieczność zmiany unijnych przepisów związana jest z pandemią COVID-19, która znacząco przyspieszyła transformację cyfrową społeczeństwa i przedsiębiorstw, oraz z rosnącą liczbą ataków cybernetycznych. Projekt nowej dyrektywy ma również wyeliminować słabości związane ze stosowaniem przepisów dyrektywy NIS, spowodowane głównie różnicami w zakresie sposobu jej implementacji w poszczególnych krajach, brakiem zapewniania odpowiedniej współpracy i wymiany informacji pomiędzy państwami członkowskimi, jak również z brakiem właściwego egzekwowania wprowadzonych regulacji przez państwa członkowskie. W uzasadnieniu do dyrektywy NIS 2 wskazano, że właściwe organy niechętnie nakładały dotychczas kary na przedsiębiorstwa, które nie wykonywały swoich obowiązków. Ponadto zauważono, że zakres zastosowania dyrektywy NIS jest już nieaktualny i nie obejmuje wszystkich podmiotów, które powinny mieć dodatkowe obowiązki w zakresie cyberbezpieczeństwa. Zwrócono jednocześnie uwagę na przyjmowanie przez państwa członkowskie niejednolitych kryteriów służących wyznaczeniu operatorów usług kluczowych, przez co niektóre podmioty – mimo takiego pierwotnego założenia ze strony unijnego ustawodawcy – nie podlegają przepisom dyrektywy. W opinii autorów projektu dyrektywy NIS 2, dyrektywa ta, po jej implementacji do porządków krajowych, ma wyeliminować wymienione wyżej słabości i doprowadzić do zwiększenia bezpieczeństwa usług cyfrowych świadczonych na terytorium Unii Europejskiej.

Nowe obowiązki państw członkowskich w zakresie cyberbezpieczeństwa

Na początku warto podkreślić, że zgodnie z założeniami projektu dyrektywy

NIS 2 obowiązki państw członkowskich w zakresie cyberbezpieczeństwa nie ulegną znaczącym zmianom. W świetle projektu dyrektywy NIS 2 władze państw członkowskich powinny przede wszystkim:

- zapewnić funkcjonowanie odpowiednich organów związanych z zapewnieniem cyberbezpieczeństwa (w tym m.in. wyznaczyć pojedyncze punkty kontaktu i właściwe zespoły reagowania na incydenty bezpieczeństwa komputerowego – CSIRT),
- opracować krajowe strategie cyberbezpieczeństwa (w ramach których powinny zostać wdrożone odpowiednie polityki, m.in. w zakresie rozwoju i promowania kompetencji dotyczących cyberbezpieczeństwa), a także
- zapewnić współpracę z właściwymi organami i CSIRT innych państw członkowskich (m.in. w ramach sieci CSIRT oraz Grupy Współpracy państw członkowskich).

Nowością w stosunku do obecnej dyrektywy NIS jest natomiast wprowadzenie w projekcie dyrektywy NIS 2 obowiązku opracowania przez państwa członkowskie narodowego planu reagowania na kryzysy i incydenty bezpieczeństwa o dużej skali (*incident and crisis response plan*). Plan ten powinien zawierać m.in. odpowiednie procedury, kanały przepływu informacji, czy środki mające na celu przygotowanie organów państw członkowskich na wypadek wystąpienia incydentów cyberbezpieczeństwa o dużej skali.

Zgodnie z założeniami projektu dyrektywy NIS 2 dla zapewnienia współpracy międzynarodowej przy reagowaniu na tego rodzaju incydenty utworzony ma być nowy organ – organizacja łącznikowa państw członkowskich, której głównym zadaniem będzie wsparcie w zakresie współpracy przy zarządzaniu incydentami bezpieczeństwa na dużą skalę (*European Cyber Crises Liaison Organisation Network – EU – CyCLONe*).

Tym samym, w stosunku do już obowiązującej dyrektywy NIS, najważniejsze zmiany w odniesieniu do obowiązków państw członkowskich, jakie mają być wprowadzone przez dyrektywę NIS 2, związane są zatem z zapewnieniem odpowiedniego poziomu przygotowania państw członkowskich i samej Unii Europejskiej na wystąpienie poważnych incydentów bezpieczeństwa sieci o szerokim zasięgu.

Podstawowym zadaniem państw członkowskich i powołanych przez nie właściwych organów krajowych pozostaje natomiast nadzór nad wypełnianiem obowiązków z zakresu cyberbezpieczeństwa przez podmioty podlegające nadzorowi. I to w zakresie sposobu kategoryzacji tych podmiotów widoczne są największe zmiany, jakie mają zostać prowadzone przez dyrektywę NIS 2 w stosunku do dyrektywy NIS.

Rozszerzenie katalogu podmiotów podlegających obowiązkom w zakresie cyberbezpieczeństwa

Najważniejszą i zarazem najbardziej istotną zmianą, w szczególności z perspektywy przedsiębiorców świadczących usługi cyfrowe, jest zmiana podmiotów objętych zakresem dyrektywy, a więc tych, na które nałożone zostaną dodatkowe obowiązki w zakresie cyberbezpieczeństwa.

W pierwszej kolejności należy zwrócić uwagę na to, że w przedstawionym projekcie dyrektywy NIS 2 zrezygnowano z dotychczasowego podziału podmiotów podlegających dyrektywie na dostawców usług cyfrowych oraz operatorów usług kluczowych, a zamiast tego posłużono się kategoriami **podmiotów kluczowych** *essential entities* oraz **podmiotów istotnych** *important entities*. Zdecydowano również, że dla zapewnienia jednolitej transpozycji przepisów dyrektywy w państwach członkowskich, kwestia tego, które podmioty należy uznać za kluczowe, a które za istotne, zostanie uregulowana wprost w załącznikach do dyrektywy, bez pozostawiania w tym zakresie swobody ustawodawcom krajowym. W tym kontekście należy zwrócić uwagę na wyraźne rozszerzenie zakresu podmiotów uznawanych

za „kluczowe" w porównaniu do katalogu podmiotów mogących stanowić operatorów usług kluczowych na gruncie dyrektywy NIS. Jako podmioty kluczowe z perspektywy zapewnienia cyberbezpieczeństwa, oprócz podmiotów z sektora energetycznego, transportowego, bankowego, finansowego, czy zdrowotnego, uznano m.in.:

- dostawców usług przetwarzania w chmurze obliczeniowej (*cloud computing service providers*) – należących wcześniej do „niższej" kategorii dostawców usług cyfrowych;
- dostawców usług centrów danych (*data centre service providers*) – nowej kategorii usług, obejmującej w szczególności usługi scentralizowanego przechowywania, przetwarzania i transportu danych łącznie z zapewnieniem wszelkich niezbędnych do tego celu narzędzi (np. obiektów i infrastruktury) oraz środków (np. dostaw energii);
- dostawców usług CDN (*content delivery network providers*) – nowej kategorii usług, polegających na udostępnianiu sieci serwerów w celu zapewnienia możliwości dalszego udostępniania użytkownikom treści internetowych;
- dostawców usług zaufania;
- dostawców publicznych sieci oraz usług łączności elektronicznej;
- jednostek centralnej administracji rządowej.

Wśród podmiotów kluczowych wskazano również operatorów infrastruktury naziemnej, wspierających świadczenie usług kosmicznych – to obecnie można traktować w kategoriach ciekawostki, jednak dobrze pokazuje spójne i przyszłościowe podejście Unii Europejskiej do kwestii cyberbezpieczeństwa.

Do kategorii podmiotów istotnych (a więc podmiotów, których usługi charakteryzują się mniejszą krytycznością z perspektywy cyberbezpieczeństwa niż podmioty kluczowe) zaliczono dostawców wyszukiwarek internetowych i internetowych platform handlowych (zaliczanych wcześniej do kategorii dostawców usług cyfrowych), a także podmioty, które wcześniej w ogóle nie podlegały przepisom dyrektywy, takie jak dostawcy serwisów społecznościowych czy dostawcy usług pocztowych. Poza tym kategoria podmiotów istotnych obejmuje m.in. podmioty zajmujące się zarządzaniem odpadami, produkcją i dystrybucją chemikaliów czy produkcją i dystrybucją żywności.

Niezwykle istotne jest również to, że zgodnie z projektem nowej dyrektywy szczególnym obowiązkom w zakresie cyberbezpieczeństwa mogą podlegać również mikro- i mali przedsiębiorcy, którzy spełniają określone kryteria, na przykład:

- świadczą usługi określonego rodzaju (np. usługi zaufania czy usługi łączności elektronicznej);
- posiadają szczególny status (np. są podmiotami publicznymi lub jedynymi dostawcami usług określonego rodzaju w danym państwie członkowskim);
- zakłócenia w działaniu usług świadczonych przez te podmioty mogłyby mieć istotny skutek np. dla bezpieczeństwa publicznego czy zdrowia publicznego.

W takich przypadkach obowiązki wynikające z dyrektywy NIS 2 będą miały zastosowanie nawet do mikro- i małych przedsiębiorców, o ile stanowią one podmioty kluczowe lub istotne. Jest to ważna zmiana w stosunku do obecnie obowiązujących regulacji dyrektywy NIS, które wyłączyły z pojęcia dostawców usług cyfrowych mikro- i małych przedsiębiorców, którzy nie są zobowiązani do wypełniania obowiązków wynikających z dyrektywy NIS, nawet jeśli ich usługi stanowią usługi cyfrowe na gruncie tej dyrektywy.

Nowe obowiązki dla podmiotów kluczowych i istotnych

W projekcie dyrektywy NIS 2 zrezygnowano z rozróżnienia zakresu obowiązków w zakresie cyberbezpieczeństwa w zależności od kategorii podmiotu obowiązanego – a zatem jednolite obowiązki stosowane są zarówno do podmiotów kluczowych, jak

i istotnych. Podobnie jak w przypadku dyrektywy NIS, podmioty te mają obowiązek podjęcia odpowiednich i proporcjonalnych środków technicznych i organizacyjnych w celu zarządzania ryzykami, na jakie narażone są sieci i systemy informatyczne wykorzystywane przez nie do świadczenia usług. Przepisy dyrektywy określają jednocześnie „niezbędne minimum" środków zmierzających do ograniczenia ryzyka wystąpienia incydentu bezpieczeństwa, które muszą zostać zapewnione przez każdy podmiot kluczowy lub istotny, w tym m.in.:

- prowadzenie analizy ryzyka;
- zapewnienie bieżącej obsługi incydentów;
- opracowanie planu ciągłości działania;
- opracowanie odpowiednich polityk i procedur w zakresie testowania i przeprowadzania audytów zabezpieczeń;
- korzystanie z kryptografii i szyfrowania.

Należy podkreślić jednocześnie, że mimo rozciągnięcia konieczności zastosowania powyższych środków na wszystkie podmioty kluczowe i istotne, to sposób ich realizacji (np. rodzaj stosowanego szyfrowania) powinien być adekwatny do poziomu ryzyka wystąpienia incydentu bezpieczeństwa. Inne środki będą musiały zostać zatem powzięte przez niewielkie podmioty publiczne, a inne – przez dużych dostawców chmury obliczeniowej, zarządzających zlokalizowanymi w Polsce centrami przetwarzania danych. Co istotne, projekt dyrektywy NIS 2 daje państwom członkowskim możliwość dodatkowego doprecyzowania środków organizacyjnych i technicznych służących zapewnieniu bezpieczeństwa. Warto jednocześnie zaznaczyć, że już sam projekt dyrektywy NIS 2 opisuje je w sposób dosyć szczegółowy.

Kolejnym ważnym obowiązkiem nałożonym na wszystkie podmioty kluczowe oraz istotne jest obowiązek raportowania incydentów bezpieczeństwa, który istniał już co prawda na gruncie dyrektywy NIS, ale w projekcie dyrektywy NIS 2 zarówno procedura raportowania incydentów, jak i konsekwencje jej niedochowania, zostały uregulowane w dużo bardziej precyzyjny i szczegółowy sposób.

Procedura raportowania incydentów i kary administracyjne za naruszenie obowiązków przez podmioty istotne i kluczowe

Wszystkie podmioty istotne i kluczowe objęte są na gruncie projektu dyrektywy NIS 2 obowiązkiem raportowania do CSIRT lub innego kompetentnego organu dwóch kategorii informacji:

- informacji o incydentach bezpieczeństwa mających istotny wpływ na świadczenie usług przez te podmioty;
- informacji o wszelkich zidentyfikowanych zagrożeniach cybernetycznych, które mogą doprowadzić do wystąpienia istotnego incydentu bezpieczeństwa – przy czym jako incydent istotny należy traktować incydent powodujący znaczące utrudnienia organizacyjne lub straty finansowe dla danego podmiotu albo mający choćby potencjalny wpływ na inne osoby fizyczne lub prawne i mogący spowodować po stronie tych osób znaczne straty materialne lub niematerialne.

Należy zwrócić uwagę na to, że obowiązek raportowania dotyczy zarówno samego faktu wystąpienia incydentu, jak i wszelkich zagrożeń mogących doprowadzić do jego powstania – projekt dyrektywy NIS 2 akcentuje zatem nie tylko konieczność niezwłocznego podjęcia działań zmierzających do zredukowania negatywnych skutków wystąpienia incydentu bezpieczeństwa, ale również istotność podejmowania działań prewencyjnych zapobiegających w ogóle jego wystąpieniu.

Zgłoszenia powinny być dokonywane niezwłocznie, przy czym w przypadku raportowania incydentów bezpieczeństwa dyrektywa przewiduje w tym zakresie specjalną, dwuetapową procedurę. Podmiot zobowiązany powinien w pierwszej kolejności najpóźniej w ciągu 24 godzin dokonać wstępnego zgłoszenia incydentu, na które właściwy organ lub CSIRT powinien odpowiedzieć również w terminie 24 godzin, wskazując wstępną ocenę incydentu. Następnie, na żądanie CSIRT lub właściwego organu, podmiot zgłaszający może zostać zobowiązany do przedstawienia informacji o statusie incydentu, a na koniec (najpóźniej w terminie miesiąca od zgłoszenia incydentu) powinien przedstawić szczegółowy raport zawierający co najmniej opis incydentu, jego przyczynę oraz powzięte środki w celu złagodzenia jego skutków, a także zapobieżenia ponownemu wystąpieniu w przyszłości. Przewidziane dyrektywą NIS 2 terminy są stosunkowo krótkie, co wydaje się dostrzegać sam ustawodawca unijny – dlatego też właściwy organ lub CSIRT w razie zaistnienia uzasadnionych przyczyn ma możliwość ich wydłużenia.

Niezastosowanie się podmiotów istotnych i kluczowych do zasad obsługi incydentów oraz do innych obowiązków przewidzianych dyrektywą może skutkować zastosowaniem przez właściwy organ krajowy środków nadzorczych, a w uzasadnionych przypadkach – administracyjnych kar pieniężnych. Projekt dyrektywy NIS 2 pozostaje w tym zakresie dużo bardziej szczegółowy, niż przepisy dyrektywy NIS, wskazując wprost środki nadzorcze, które mogą być zastosowane w stosunku do podmiotów podlegających przepisom dyrektywy – środki te różnią się w zależności od kategorii podmiotu (istotny lub kluczowy) i obejmują m.in. możliwość kierowania ostrzeżeń, wiążących instrukcji i poleceń, nałożenie obowiązku poinformowania osób zagrożonych wystąpieniem incydentu bezpieczeństwa o ryzyku z tym związanym, czy zobowiązanie danego podmiotu do podania do publicznej wiadomości informacji o niedopełnieniu obowiązków przewidzianych dyrektywą (co – w przypadku dużych podmiotów – może mieć istotne, negatywne konsekwencje wizerunkowe).

Dodatkowo, w odniesieniu do podmiotów kluczowych, w przypadku, gdyby zastosowane środki nie doprowadziły do przestrzegania przez ten podmiot nałożonych obowiązków, właściwy organ krajowy powinien mieć dodatkowo możliwość:

- cofnięcia lub zawieszenia zezwolenia na prowadzenie przez dany podmiot określonego rodzaju działalności – co może mieć szczególne znaczenie

dla podmiotów działających na rynkach regulowanych, np. dla branży finansowej, telekomunikacyjnej czy energetycznej;
- zakazać sprawowania funkcji kierowniczych w danym podmiocie osobie odpowiedzialnej za naruszenie obowiązków wynikających z dyrektywy.

Niezależnie od powyższego, w stosunku do podmiotów istotnych i kluczowych naruszających swoje obowiązki wynikające z dyrektywy, właściwe organy państw członkowskich powinny mieć możliwość nałożenia administracyjnych kar pieniężnych, łącznie z zastosowaniem środków nadzorczych lub zamiast tych środków. Wartość tych kar nie może przekroczyć kwoty 10 mln euro lub kwoty stanowiącej wartość 2% rocznego obrotu danego podmiotu (zależnie od tego, która suma jest wyższa). Wysokość administracyjnej kary pieniężnej powinna być proporcjonalna w stosunku do dokonanego naruszenia.

Co jednak istotne, w przypadku, gdyby incydent bezpieczeństwa stanowił również naruszenie przepisów RODO[4], za które to naruszenie została już wymierzona administracyjna kara pieniężna na podstawie RODO, właściwy organ nie może za to samo naruszenie nałożyć drugiej kary na podstawie przepisów dyrektywy NIS 2, co nie wyłącza możliwości zastosowania innych środków nadzorczych, m.in. cofnięcia zezwolenia na prowadzenie działalności regulowanej.

Podsumowanie

Projekt dyrektywy NIS 2 podąża ścieżką wytyczoną wcześniej przez dyrektywę NIS, będąc jednocześnie jej bardziej doprecyzowaną i surowszą wersją. W przypadku przyjęcia dyrektywy w obecnym kształcie, szczególnymi obowiązkami w zakresie cyberbezpieczeństwa zostanie objęty znacznie szerszy krąg podmiotów, niż dotychczas, w tym niektórzy mikro- i mali przedsiębiorcy. Podmioty te będą przy tym musiały spełnić szereg specyficznych wymagań, za których nieprzestrzeganie będą grozić surowe konsekwencje, w tym możliwe do nałożenia bardzo wysokie kary finansowe. Warto mieć jednak na uwadze, że projekt dyrektywy NIS 2 jest obecnie w trakcie prac legislacyjnych i może jeszcze zostać zmieniony, choć zakładać należy, że ogólny kierunek regulacji zostanie raczej zachowany. Zgodnie z założeniami projektu dyrektywy NIS 2, po jej uchwaleniu powinna ona zostać implementowana do krajowego porządku prawnego w ciągu 18 miesięcy.

Agnieszka Wachowska
radczyni prawna, partner
w kancelarii Traple Konarski
Podrecki i Wspólnicy sp.j.

Aleksander Elmerych
aplikant radcowski, junior associate
w kancelarii Traple Konarski
Podrecki i Wspólnicy sp.j.

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L z 2016 r. nr 194, str. 1).

[2] (t.j. Dz. U. z 2020 r. poz. 1369 z późn. zm.).

[3] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final, dostępny pod adresem: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166.

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L z 2016 r. nr 119, str. 1 z późn. zm.).

Imię i nazwisko jako znak towarowy

Przesłanki oraz ograniczenia ochrony w charakterze znaku towarowego

Marta Lampart

W obecnych czasach imię i nazwisko to nie tylko dane identyfikujące konkretną osobę fizyczną. Najnowsze trendy pokazują, że nierzadko stanowią one markę osobistą wykorzystywaną przez wiele osób w biznesie. Na przestrzeni lat można zaobserwować coraz więcej rejestracji znaków towarowych stanowiących imię i nazwisko, samo nazwisko lub pseudonim. Zdarzają się też rejestracje imienia i nazwiska przez osoby znane lub nazwy postaci fikcyjnych. Tendencję tę można zaobserwować na całym świecie, nie tylko w Polsce i w Unii Europejskiej.

Uzyskanie ochrony imienia i nazwiska jako znaku towarowego pozwala na uzyskanie prawa wyłącznego, jednak trzeba liczyć się z jego pewnymi ograniczeniami. W artykule poruszane są zagadnienia związane z ochroną imienia i nazwiska jako znaku towarowego w świetle polskich i unijnych przepisów prawa. Ochrona ta może przysługiwać niezależnie od ochrony wynikającej z przepisów o prawie autorskim oraz w zakresie dóbr osobistych.

Kiedy imię i nazwisko lub pseudonim mogą być znakiem towarowym?

W świetle przepisów ustawy z dnia 30 czerwca 2000 r. Prawo własności przemysłowej[1] znakiem towarowym może być każde oznaczenie umożliwiające odróżnienie towarów jednego przedsiębiorstwa od towarów innego przedsiębiorstwa oraz możliwe do przedstawienia w rejestrze znaków towarowych w sposób pozwalający na ustalenie jednoznacznego i dokładnego przedmiotu udzielonej ochrony (art. 120 ust. 1). Znakami towarowymi mogą być między innymi wyraz, włącznie z nazwiskiem, grafika, dźwięk, czy kształty. Katalog przykładowych oznaczeń mogących stanowić znak towarowy nie jest zamknięty, nie jest więc wykluczone, że w charakterze znaku towarowego ochronę uzyska imię i nazwisko lub pseudonim. Możliwość ochrony nazwiska jako znaku towarowego została potwierdzona także w orzecznictwie sądów administracyjnych[2].

Istotne jest zatem, aby taki znak towarowy posiadał zdolność odróżniającą oraz był możliwy do przedstawienia w rejestrze znaków towarowych w sposób pozwalający na ustalenie jednoznacznego i dokładnego przedmiotu udzielonej ochrony. Analogiczne rozwiązania znajdujemy w przepisach unijnych – art. 4 rozporządzenia Parlamentu Europejskiego[3] i Rady (UE) 2017/1001 z dnia 14 czerwca 2017 r. w sprawie znaku towarowego Unii Europejskiej. Imię i nazwisko lub pseudonim, jeśli mają uzyskać ochronę w charakterze znaku towarowego, to muszą spełniać wszystkie przesłanki ochrony oznaczeń odróżniających jako znaków towarowych w rozumieniu wyżej wymienionych przepisów. Również zastosowanie znajdą tutaj bezwzględne i względne przeszkody rejestracji, które, jeśli wystąpią w sprawie danego zgłoszenia, spowodują odmowę udzielenia prawa ochronnego. Może się także okazać, że w przyszłości znak towarowy zostanie unieważniony. Zasady ochrony takich oznaczeń są takie same jak innych zgłoszonych do właściwego urzędu ds. własności przemysłowej – ani przepisy polskiej ustawy, ani unijnego rozporządzenia nie przewidują odmiennych rozwiązań w tym zakresie.

Bezwzględne i względne przeszkody rejestracji

W procesie zgłaszania znaku towarowego znaczenie mają bezwzględne i względne przeszkody rejestracji, mające zastosowanie także w przypadku imienia i nazwiska lub pseudonimu. Z bezwzględną przeszkodą rejestracji będziemy mieć do czynienia przede wszystkim wówczas, gdy imię, nazwisko lub pseudonim nie nadają się do oznaczania towarów lub usług, dla których zostały zgłoszone. Inne bezwzględne przeszkody rejestracji dotyczą sytuacji, gdy np. zgłoszone oznaczenia składają się wyłącznie z elementów mogących służyć w obrocie do wskazania (w szczególności rodzaju towaru, jego pochodzenia, jakości, ilości, wartości, przeznaczenia, sposobu wytwarzania, składu, funkcji lub przydatności) lub zostały zgłoszone w złej wierze, lub są sprzeczne z porządkiem publicznym, lub dobrymi obyczajami (art. 129[1] ustawy Prawo własności przemysłowej). Te przeszkody brane są pod uwagę z urzędu przez urząd rozpatrujący zgłoszenie.

Inaczej jest z względnymi przeszkodami rejestracji, które podnoszone są w sprzeciwie do zgłoszenia znaku towarowego na odpowiednim etapie postępowania przed właściwym urzędem ds. własności przemysłowej. W przypadku imienia i nazwiska lub pseudonimu w sprzeciwie wskazywane może być zaistnienie przede wszystkim względnej przeszkody rejestracji, gdy zgłoszone oznaczenie odróżniające narusza prawa osobiste lub majątkowe osób trzecich[4]. Z ryzykiem zgłoszenia sprzeciwu przez osobę do tego uprawnioną można liczyć się również m.in. wtedy, gdy następuje kolizja z wcześniej zarejestrowanym lub zgłoszonym znakiem towarowym (art. 132[1] ustawy Prawo własności przemysłowej).

Przykłady chronionych imion i nazwisk oraz pseudonimów

Ochrona imienia i nazwiska lub pseudonimu już od dawna praktykowana jest przez Urząd Patentowy Rzeczpospolitej

Polskiej (UPRP) lub Urząd Unii Europejskiej ds. Własności Intelektualnej (EUIPO). Takie oznaczenia chronione są najczęściej jako znaki słowne, słowno-graficzne lub graficzne. Nie jest wykluczone, że imię i nazwisko lub pseudonim mogą zostać umieszczone także w niekonwencjonalnym znaku towarowym, np. przestrzennym lub ruchomym znaku towarowym. Inwencja twórcza jest niograniczona, więc możemy spodziewać się w niedalekiej przyszłości uzyskiwania ochrony również na niektóre niekonwencjonalne znaki towarowe zawierające imię, nazwisko lub pseudonim.

Przeglądając ogólnodostępne polskie i unijne bazy danych znaków towarowych można znaleźć wiele przykładów imion i nazwisk lub pseudonimów chronionych w charakterze znaku towarowego.

Zgodnie z obecnymi trendami celebryci, w tym piosenkarze lub sportowcy, a także ich rodziny rejestrują imiona lub imiona i nazwiska swoich dzieci. Na przykład w 2017 r. w EUIPO został zarejestrowany słowny znak towarowy „Brooklyn Beckham" należący do jednego z dzieci Victorii Beckham[5]. Inny tego typu przypadek to słowny znak towarowy „Marek Grechuta" zgłoszony przez Danutę Grechutę[6]. Kombinacja nazwisk także może uzyskać ochronę jako znak towarowy – tutaj przykładem może być słowno-graficzny znak towarowy „paprocki&brzozowski"[7] używany w branży modowej.

Dobrym przykładem pseudonimu chronionego jako znak towarowy jest słowne oznaczenie „Violetta Villas", zmarłej w 2011 r. znanej polskiej piosenkarki, zgłoszone do UPRP przez Krzysztofa Gospodarka[8], czy „Stachursky"[9].

Samo imię również może podlegać ochronie – np. „Agata" dla mebli jako słowny znak towarowy[10] czy „Barbara" dla wyrobów czekoladowych i czekoladopodobnych oraz cukierniczych jako słowno-graficzny znak towarowy[11] lub „karolina" dla m.in. herbat, kaw, napojów bezalkoholowych i owocowych jako słowny znak towarowy[12]. Ochronie podlegają nawet powszechnie występujące nazwiska jak „Nowak" jako słowny znak towarowy[13] lub jako słowno-graficzny „Nowak N" – z dodatkiem litery N[14].

Imię i nazwisko lub pseudonim jako znak towarowy a dobra osobiste

Z przepisów Kodeksu cywilnego[15] wynika, że nazwisko lub pseudonim stanowią dobra osobiste człowieka, które pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.

Zgłaszając do właściwego urzędu ds. własności przemysłowej znak towarowy składający się z nazwiska, trzeba brać pod uwagę to, czy nie spowoduje się takim działaniem naruszenia dobra osobistego innej osoby w postaci nazwiska. Dokonując rejestracji cudzego nazwiska lub pseudonimu, można spodziewać się reakcji prawnej osoby, której to nazwisko lub pseudonim dotyczą, ale każdy stan faktyczny wymagać będzie odrębnej analizy. Podobnie będzie w sytuacji, gdy nazwisko osoby zostanie wykorzystane bez jej zgody. Nie ma tutaj znaczenia, czy jest to nazwisko osoby znanej, czy osoby, która nie jest znana na przykład z uwagi na swoją działalność artystyczną, zawodową, czy sportową. Nazwisko każdego człowieka podlega ochronie jako dobro osobiste. Co do zasady nie powinno być problemu z rejestracją własnego imienia i nazwiska, ponieważ należą do zgłaszającego i stanowią jego dobra osobiste, wszystko jednak będzie zależało od danych okoliczności sprawy.

Prezes UPRP w Wytycznych opublikowanych na stronie internetowej UPRP wyjaśnia, że do naruszenia prawa osobistego do nazwiska dojdzie w sytuacji, gdy oznaczenie stanowiące nazwisko może wywołać skojarzenie konkretnej osoby ze zgłoszonym do ochrony znakiem towarowym, tym bardziej jeśli znak ten zawiera również imię tej osoby[16]. Jak przyjmuje się w orzecznictwie Sądu Najwyższego, *Prawa osób trzecich mogą być naruszone zarówno stosowaniem znaku towarowego zarejestrowanego, jak i niezarejestrowanego. W razie kolizji między formalnym prawem z rejestracji znaku towarowego, w którym nazwisko zostało użyte jako motyw, a prawem podmiotowym do nazwiska, osoba, której dobro osobiste (prawo do nazwiska) zostało naruszone, może żądać zaprzestania działań naruszających jej prawa bądź uniemożliwienia rejestracji przed Urzędem Patentowym (art. 20 i 29 ustawy), co nie wyłącza roszczenia o ochronę dóbr z art. 23 i 24 KC*[17].

Trzeba pamiętać, że zgodnie z przepisami Kodeksu cywilnego ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne (art. 24 Kodeksu cywilnego). Jeśli doszło już do naruszenia dobra osobistego, można żądać dopełnienia czynności potrzebnych do usunięcia jego skutków. Można również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny, a gdy wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, to poszkodowany może żądać jej naprawienia na zasadach ogólnych określonych w Kodeksie cywilnym.

Czy imiona i nazwiska osób znanych również korzystają z ochrony?

Wspomniana tendencja do rejestrowania imion i nazwisk lub pseudonimów przez osoby znane nie jest przypadkowa.

Są to najczęściej efekty dobrze przemyślanych strategii ochrony własności intelektualnej oraz inwestowania we własne nazwisko rodziny lub pseudonim. Uzyskanie jednak ochrony cudzego imienia i nazwiska, tym bardziej osoby znanej, może okazać się nieopłacalne.

Ciekawym przykładem sporu na styku rejestracji znaku towarowego zawierającego imię oraz znaku zawierającego imię i nazwisko stanowi spór związany z naruszeniem praw do znaku towarowego „Coco Chanel" przez właścicielkę salonu piękności, która używała w nazwie tego salonu słowa „Chanel" stanowiącego jednocześnie jej imię (Chanel Jones). Ostatecznie sąd zakazał używania słowa „Chanel" w nazwie salonu, pomimo argumentacji właścicielki, że jest to jej imię[18].

W praktyce orzeczniczej sądów unijnych można odnaleźć orzeczenia, które nawiązują do przepisów włoskich (włoski kodeks własności przemysłowej) przewidujących, że nazwiska osób używane w sferach m.in. artystycznej, literackiej, czy sportowej, pod warunkiem, że są powszechnie znane, mogą być rejestrowane jako znaki towarowe wyłącznie przez właściciela lub za jego zgodą[19]. Trybunał w jednej ze spraw rozpoznawanych w 2011 r., mając na uwadze przepisy włoskie, przyjął, że *właściciel nazwiska powszechnie znanego ma prawo przeciwstawić się używaniu tego nazwiska jako znaku towarowego, wówczas gdy utrzymuje on, iż nie wyraził swojej zgody na rejestrację rzeczonego znaku towarowego*[20]. Podobnie sąd orzekł w wyroku z 29 czerwca 2017 r. *należy odmówić rejestracji oznaczenia jako włoskiego znaku towarowego, jeśli nazwa, o której rejestrację wniesiono, jest nazwiskiem osoby powszechnie znanej we Włoszech i jeśli właściciel wspomnianego nazwiska nie wyraził zgody na rejestrację wspomnianej nazwy*[21].

Ustawa Prawo własności przemysłowej nie przewiduje wprost analogicznych rozwiązań jak we wspomnianych przepisach włoskich, jednak zasada ta powinna stanowić także punkt odniesienia dla zgłoszeń polskich znaków towarowych zawierających imię i nazwisko innej osoby, w tym znanej, ponieważ stanowić to może naruszenie jej dóbr osobistych oraz prowadzić do wprowadzania w błąd odbiorców towarów lub usług.

Czy imię i nazwisko postaci fikcyjnej może podlegać ochronie jako znak towarowy?

Mówiąc o postaci fikcyjnej najczęściej mamy na myśli jej ochronę na gruncie prawa autorskiego, która nie wymaga odpowiedniego zgłoszenia i wpisania do odpowiedniego rejestru[23]. Postać fikcyjna, jej imię i nazwisko, może podlegać ochronie również jako znak towarowy, o ile spełnione zostaną przesłanki do rejestracji w charakterze znaku towarowego oraz nie będą zachodzić przeszkody rejestracji. W przeciwieństwie do ochrony prawnoautorskiej, która trwa co do zasady do 70 lat od śmierci twórcy, ochrona prawnoznakowa może trwać w nieskończoność, o ile uprawniony do znaku towarowego będzie co 10 lat przedłużał ochronę swojego znaku na kolejne okresy dziesięcioletnie. Jest to zatem odpowiednie narzędzie dla podmiotów, które chcą zapobiec wykorzystywaniu ich twórczości przez inne osoby przez dłuższy czas oraz zainwestować w marketing postaci fikcyjnej.

Przykładami zarejestrowanych postaci fikcyjnych są: szereg znaków „Hello Kitty" (w bazie EUIPO odnaleźć można aż 12 graficznych znaków towarowych z wizerunkiem lub nazwą Hello Kitty), znany wszystkim Batman[24], czy wiele znaków towarowych stanowiących słynne postacie fikcyjne zarejestrowane przez Disneya – m.in. Ariel[25], Winnie the Pooh[26], czy Mickey Mouse[27].

Czy przyznanie ochrony dla imienia i nazwiska lub pseudonimu jako znaku towarowego napotyka na pewne ograniczenia?

To pytanie zadają sobie zapewne wszystkie osoby, które w niedalekiej przyszłości zamierzają dokonać rejestracji nazwiska w charakterze znaku towarowego. Takie wątpliwości są jak najbardziej zasadne w sytuacji, gdy weźmie się pod uwagę, że uzyskanie prawa ochronnego do znaku towarowego oznacza nabycie prawa wyłącznego używania znaku towarowego w sposób zarobkowy lub zawodowy na całym obszarze Rzeczypospolitej Polskiej (analogicznie w przypadku znaku towarowego chronionego na terytorium Unii Europejskiej).

Inwestowanie we własne nazwisko, tworzenie marki osobistej czy rodzinnej, wymaga rozważenia wszystkich okoliczności i ograniczeń wynikających z przepisów prawa. Warto zatem wiedzieć, że ochrona nazwiska jako znaku towarowego nie zawsze daje możliwość skorzystania przez uprawnionego do znaku towarowego z prawa zakazywania używania w obrocie przez inne osoby tego oznaczenia.

Zgodnie z art. 156 ust. 1 ustawy Prawo własności przemysłowej nie można zabronić używania w obrocie przez inne osoby ich nazwisk w przypadku, gdy osoby te są osobami fizycznymi. Inaczej rzecz ujmując – nie można co do zasady odmówić innej osobie używania jej nazwiska na podstawie posiadanego prawa ochronnego na znak towarowy. Analogiczne rozwiązanie przewidziane zostało w art. 14 ust. 1 lit. a) rozporządzenia nr 2017/1001. Nie można wykluczyć także sytuacji, że zgłoszony do ochrony znak towarowy stanowiący pseudonim czy postać fikcyjną mogą stanowić jednocześnie czyjeś nazwisko. Takiej osobie również co do zasady nie można wtedy zakazać używania jej własnego nazwiska w obrocie. Trzeba jednak mieć tutaj na uwadze także reguły uczciwej konkurencji.

Podsumowanie

Imię i nazwisko lub pseudonim stanowią dobra osobiste, mogą też uzyskać ochronę prawnoznakową. Przesłanki uzyskania takiej ochrony nie różnią się od reguł określonych w polskich i unijnych przepisach dla pozostałych znaków towarowych. Podążając za najnowszymi trendami, trzeba pamiętać, aby nie naruszyć praw innych osób. Warto zweryfikować, czy zgłaszany znak towarowy, nie widnieje już w bazach danych UPRP, EUIPO lub TM View, ogólnodostępnych dla wszystkich. Również weryfikacja rynku może dać wiele odpowiedzi.

Uzyskanie rejestracji cudzego imienia i nazwiska bez jego zgody może prowadzić do sporych komplikacji prawnych, których lepiej unikać, prowadząc swoją działalność.

Marta Lampart
radca prawny, specjalizuje się w prawie własności intelektualnej, w tym prawie znaków towarowych, prawie dotyczącym przedsiębiorców, prowadzi kancelarię radcy prawnego w Krakowie, autorka bloga prawniczego Legalny znak towarowy (https://www.legalnyznaktowarowy.pl/).

[1] Tekst jednolity: Dz. U. z 2021 r. poz. 324 z późn. zm., dalej jako ustawa Prawo własności przemysłowej.
[2] Wyrok NSA z dnia 20 września 2006 r., II GSK 115/06, Legalis 83397.
[3] Dz. Urz. UE L 154 z 16.06.2017, s. 1–99, dalej jako rozporządzenie nr 2017/1001.
[4] Zob. też M. Witkowska, A. Michalak, *Dział I. Znaki towarowe i prawa ochronne,* [w:] A. Michalak (red.), *Prawo własności przemysłowej. Komentarz,* Warszawa 2016, s. 419.
[5] EUTM 016191835 (EUIPO).
[6] UPRP: R.221031.
[7] UPRP: R.245409.
[8] UPRP: R.274541.
[9] UPRP: R.167484.
[10] UPRP: R.111387.
[11] UPRP: R.093307.
[12] UPRP: R.163205.
[13] UPRP: R.181954 dla towarów wskazanych w klasie 29, m.in. mięsa, przetworów mięsnych, wędlin.
[14] UPRP: R.190715 dla towarów wskazanych w klasie 2, 37 i 40.
[15] Kodeks cywilny z dnia 23 kwietnia 1964 r. (tekst jednolity: Dz. U. z 2020 r. poz. 1740), dalej jako: Kodeks cywilny.
[16] Ogólne wytyczne Prezesa UPRP, Wytyczne w zakresie znaków towarowych, Naruszenie praw osobistych lub majątkowych, Prawo do imienia, nazwiska, pseudonimu, https://uprp.gov.pl/pl/przedmioty-ochrony/ogolne-wytyczne-prezesa-uprp/wytyczne-w-zakresie-znako-w-towarowych-/naruszenie-praw-osobistych-lub-majatkowych/prawo-do-imienia-nazwiska-pseudonimu, [dostęp: 21.05.2021 r.].
[17] Wyrok Sądu Najwyższego z dnia 17 marca 1988 r., IV CR 60/88 (Legalis 26198). Zasady ochrony ujęte w tym orzeczeniu pozostają nadal aktualne pomimo tego, że zapadło ono jeszcze na gruncie poprzednio obowiązującej ustawy o znakach towarowych z 1985 r. Zob. też Ogólne wytyczne Prezesa UPRP, Wytyczne w zakresie znaków towarowych, Naruszenie praw osobistych lub majątkowych, Prawo do imienia, nazwiska, pseudonimu, https://uprp.gov.pl/pl/przedmioty-ochrony/ogolne-wytyczne-prezesa-uprp/wytyczne-w-zakresie-znako-w-towarowych-/naruszenie-praw-osobistych-lub-majatkowych/prawo-do-imienia-nazwiska-pseudonimu, [dostęp: 21.05.2021 r.].
[18] Zob. *Chanel Won its Lawsuit Against Salon Owner Named Chanel*, by TFL, THE FASHION LAW, 22.12.2014 r., https://www.thefashionlaw.com/chanel-won-its-lawsuit-against-salon-owner-named-chanel/, [dostęp: 21.05.2021 r.].
[19] Wyrok Trybunału z dnia 5 lipca 2011 r. w sprawie Edwin Co. Ltd p-ko EUIPO i Elio Fiorucci, C-263/09 P, ECLI:EU:C:2011:452, pkt 10.
[20] Ibidem, pkt 55.
[21] Wyrok Sądu z dnia 29 czerwca 2017 r. w sprawie Arrigo Cipriani p-ko EUIPO, T-343/14, ECLI:EU:T:2017:458, pkt 88.
[22] Zob. więcej na temat ochrony postaci fikcyjnej na gruncie prawa autorskiego: J. Jezierski, *Prawo a komercyjne wykorzystanie znanych postaci fikcyjnych. Co jest dozwolone?*, 18.09.2020 r., https://www.parp.gov.pl/component/content/article/64027:prawo-a-komercyjne-wykorzystanie-znanych-postaci-fikcyjnych-co-jest-dozwolone, [dostęp: 21.05.2021 r.].
[23] e-search Plus, The EUIPO database, https://euipo.europa.eu/eSearch/#basic/1+1+1+1/100+100+100+100/hello%20kitty, [dostęp: 21.05.2021 r.]. Więcej na temat historii i sporów co do praw do znaków towarowych „Hello Kitty" zob.: K. Grzybczyk, *Ikony popkultury a prawa własności intelektualnej. Jak znani i sławni chronią swoje prawa*, Warszawa 2018, s. 373-376.
[24] EUTM: 000038125.
[25] EUTM: 000421529.
[26] EUTM: 000983122.
[27] EUTM: 002827426.

Naruszenie ochrony danych przez podmiot przetwarzający

Czym jest i jak postępować, kiedy do niego dojdzie

Monika Macura

Administrator danych osobowych (ang. *controller*) i podmiot przetwarzający (ang. *processor*) to podstawowe role, w których występują firmy i inne organizacje w prawie ochrony danych osobowych.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), dalej „RODO", definiuje oba te pojęcia.

Administrator

W myśl RODO administratorem jest podmiot (osoba fizyczna, prawna lub jednostka organizacyjna), który samodzielnie ustala cele i sposoby przetwarzania danych osobowych. W myśl tej definicji, każdy podmiot, który korzysta z danych osobowych do własnych celów jest administratorem danych. O tym, że dany podmiot jest administratorem danych, zatem decyduje to, że przetwarza dane osobowe, czyli np. wykorzystuje je w swoich procesach biznesowych, samodzielnie ustalając cele, w jakich dane przetwarza oraz sposoby tego przetwarzania danych.

Rola podmiotu przetwarzającego w procesie przetwarzania danych przez administratora

Rola w procesie przetwarzania danych i obowiązki podmiotu przetwarzającego określone są odmiennie od roli administratora danych osobowych. Podmiot przetwarzający działa w imieniu i na rzecz administratora, a jego obowiązki względem administratora wynikają z umowy zawartej z administratorem i z przepisów RODO. W znakomitej większości przypadków rolę podmiotu przetwarzającego w procesie przetwarzania danych przez administratora określa umowa zawarta pomiędzy administratorem a tym podmiotem przetwarzającym.

Jednym z istotnych wymogów stawianych podmiotowi przetwarzającemu jest obowiązek współpracy z administratorem w przypadku wystąpienia naruszenia ochrony danych osobowych.

Podstawowym obowiązkiem podmiotu przetwarzającego jest zgłaszanie administratorowi przypadków naruszeń ochrony danych osobowych, jakie miały miejsce w odniesieniu do danych przetwarzanych na polecenie tego administratora. Obowiązek ten wynika wprost z art. 33 ust. 2 RODO, który przewiduje, że po stwierdzeniu naruszenia ochrony danych osobowych podmiot przetwarzający bez zbędnej zwłoki zgłasza je administratorowi. Najczęściej obowiązek ten jest także wprost wskazywany w umowie pomiędzy administratorem i podmiotem przetwarzającym. Podmiot przetwarzający ma zatem obowiązek niezwłocznego informowania administratora o stwierdzonych przypadkach naruszenia bezpieczeństwa danych osobowych.

W celu należytego wykonywania tych obowiązków względem administratora podmiot przetwarzający powinien zatem umieć identyfikować sytuacje, w których doszło do naruszenia ochrony danych osobowych.

Naruszenie ochrony danych osobowych – identyfikacja

Umowa powierzenia przetwarzania danych, nakładając na podmiot przetwarzający określone obowiązki związane z naruszeniem, nie określa, na czym polega „naruszenie ochrony danych osobowych", czyli jakie przypadki naruszenia ma zgłaszać podmiot przetwarzający.

Zatem to na podmiocie przetwarzającym spoczywa obowiązek każdorazowego ustalenia, czy konkretny incydent dotyczący danych osobowych stanowił przypadek naruszenia ochrony danych osobowych. Pomocna w ustaleniu, czy doszło do naruszenia ochrony danych osobowych, jest definicja zawarta w art. 4 pkt 12) RODO. W myśl tej definicji „naruszenie" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Przepisy RODO, określając pojęcie „naruszenia" odnoszą się wyłącznie do takich przypadków, w których doszło do naruszenia bezpieczeństwa zabezpieczeń, rozumianych jako techniczne i organizacyjne środki służące zabezpieczeniu przetwarzanych danych, pociągającego za sobą określone w tym przepisie skutki. Naruszeniem bezpieczeństwa danych nie będzie więc jakiekolwiek naruszenie przepisów o ochronie danych, a tylko takie, które stanowi naruszenie bezpieczeństwa mające określone skutki dla danych osobowych.

Przepisy RODO wymagają zatem, aby naruszenie było przypadkowe, czyli nieumyślne, niezamierzone. Naruszeniem bezpieczeństwa danych osobowych nie będzie więc działanie podmiotu przetwarzającego, a więc działanie celowe, zamierzone, np. celowe zniszczenie lub zmodyfikowanie danych, które jest zgodne z prawem, czyli np. jest efektem usunięcia lub modyfikacji danych, a wyłącznie takie, które było poza kontrolą przetwarzającego.

Jakie skutki dla danych osobowych może powodować naruszenie bezpieczeństwa danych?

Zgodnie z definicją zawartą w RODO o naruszeniu ochrony danych mówimy w przypadkach, gdy wywołuje ono co najmniej jeden z następujacych skutków:

1) przypadkowe lub niezgodne z prawem zniszczenie danych – czyli sytuację, w której dane przestają istnieć w formie nadającej się do użytku. Przykładem „zniszczenia danych" może być zniszczenie nośnika, na którym dane zostały zapisane, lub skasowanie danych zapisanych na nośniku informatycznym w sposób, który uniemożliwi ich odzyskanie. Do przykładów zniszczenia danych możemy zakwalifikować także spalenie się archiwum z dokumentami, wykasowanie plików z pamięci komputera i fizyczne zniszczenie kopii zapasowych, czy zalanie archiwum zgód na przetwarzanie danych osobowych.
2) przypadkową lub niezgodną z prawem utratę danych – czyli sytuację, w której dane mogą wprawdzie nadal istnieć, ale podmiot przetwarzający utracił nad nimi kontrolę lub dostęp do nich, lub nie jest już w ich posiadaniu. Utrata danych nie musi jednak wiązać się z ich zniszczeniem, a jedynie ze zmianą podmiotu, który staje się dysponentem danych (jeden podmiot uzyskuje dane, a inny je traci).
3) przypadkową lub niezgodną z prawem modyfikację danych – modyfikacja danych oznacza dokonanie zmiany treści informacji, które są zawarte w danych, w konsekwencji czego stały się niekompletne, częściowo nieczytelne, nieprawidłowe.
4) nieuprawnione ujawnienie danych – czyli sytuację, w której dostęp do danych ma osoba, która nie posiada stosownego uprawnienia, nadanego przez podmiot uprawniony. Dochodzi do niego np. w przypadku udostępnienia korespondencji mailowej osobie nieuprawionej, czyli wysyłki korespondencji na nieprawidłowy adres.
5) nieuprawniony dostęp do danych – uzyskanie nieuprawnionego dostępu do danych to najczęstszy i najbardziej typowy przypadek naruszenia bezpieczeństwa danych. W praktyce do nieuprawnionego dostępu do danych dochodzi w przypadku kradzieży danych.

Wspomniany na wstępie obowiązek zgłoszenia administratorowi naruszenia ochrony danych osobowych wymusza na podmiocie przetwarzającym ustalenie, czy konkretne zdarzenie dotyczące danych osobowych, stanowi przypadek naruszenia ochrony danych osobowych. Ocena, czy doszło do naruszenia, to obowiązek podmiotu przetwarzającego.

Moment stwierdzenia naruszenia następuje w przypadku, gdy podmiot przetwarzający ma wystarczający stopień pewności co do tego, że doszło do zdarzenia zagrażającego bezpieczeństwu, które doprowadziło w konsekwencji do naruszenia bezpieczeństwa danych osobowych. W tym celu podmiot przetwarzający, z uwzględnieniem powyższych wytycznych powinien ocenić, czy doszło do naruszenia bezpieczeństwa prowadzącego do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Zgłoszenie naruszenia administratorowi

Zgłaszanie przez podmiot przetwarzający stwierdzonego przypadku naruszenia powinno nastąpić niezwłocznie (czyli bez zbędnej zwłoki) po stwierdzeniu naruszenia. Przepisy RODO nie nakładają na podmiot przetwarzający obowiązku powiadomienia administratora w konkretnym przedziale czasu, jednakże umowa powierzenia przetwarzania najczęściej taki termin wyznacza. Wiąże się to z tym, że w przypadku stwierdzenia naruszenia, administrator ma obowiązek rozważyć, czy dany przypadek należy zgłosić do Urzędu Ochrony Danych Osobowych.

Zgłoszenie przypadku naruszenia administratorowi powinno zawierać co najmniej informacje o:

a) dacie, czasie trwania oraz lokalizacji naruszenia ochrony danych osobowych;
b) charakterze i skali naruszenia, tj. w szczególności o kategoriach i przybliżonej liczbie osób, których dane dotyczą, oraz kategoriach i przybliżonej liczbie wpisów danych osobowych, których dotyczy naruszenie, a w razie możliwości, także wskazania podmiotów danych, których dotyczyło naruszenie;
c) systemie informatycznym, w którym wystąpiło naruszenie (jeżeli naruszenie nastąpiło w związku

z przetwarzaniem danych w systemie informatycznym);
d) przewidywanym czasie potrzebnym do naprawienia szkody spowodowanej naruszeniem;
e) charakterze i zakresie danych osobowych objętych naruszeniem;
f) możliwych konsekwencjach naruszenia, z uwzględnieniem konsekwencji dla osób, których dane dotyczą;
g) środkach podjętych w celu zminimalizowania konsekwencji naruszenia oraz proponowanych działaniach zapobiegawczych i naprawczych;
h) danych kontaktowych osoby mogącej udzielić dalszych informacji o naruszeniu.

Jeśli w organizacji powołano inspektora ochrony danych, to na nim zwykle spoczywa obowiązek komunikacji z administratorem, w szczególności z wyznaczonym przez niego inspektorem ochrony danych. Komunikacja odbywa się zwykle elektronicznie w sposób uzgodniony w umowie powierzenia.

Procedury wewnętrzne i dokumentacja naruszenia

W celu zapewnienia prawidłowego współdziałania pomiędzy podmiotem przetwarzającym a administratorem, każdy z nich powinien opracować i wdrożyć (a więc także przeszkolić osoby odpowiedzialne) procedury zapewniające:
a) wykrycie i natychmiastowe powstrzymanie naruszenia,
b) ocenę ryzyka dla osób, których dane zostały naruszone,
c) ustalenie, czy konieczne jest powiadomienie właściwego organu nadzoru,
d) powiadomienie o naruszeniu osób, których dane zostały naruszone (w razie potrzeby),
e) prowadzenia wewnętrznego rejestru naruszeń.

Obowiązek prowadzenia rejestru naruszeń spoczywa na każdym podmiocie przetwarzającym. Poprawne prowadzenie tego rejestru ułatwia realizację obowiązków względem administratora i upraszcza proces zgłoszenia naruszenia administratorowi. Rejestr naruszeń prowadzony jest przez podmiot przetwarzający w formie elektronicznej. Powinien on zawierać następujące informacje:
a) informacje o wystąpieniu zdarzenia i stwierdzeniu naruszenia, czyli: data zdarzenia, data i źródło uzyskania informacji o zdarzeniu, data i godzina stwierdzenia naruszenia;
b) okoliczności naruszenia – w tym opis charakteru naruszenia (opis, na czym polegało), opis kategorii i liczby osób, których dotyczyło naruszenie, opis kategorii i liczby wpisów);
c) skutki naruszenia (czyli opis konsekwencji naruszenia);
d) środki naprawcze i zaradcze, w tym informację, czy poinformowano osoby, których dane dotyczą;
e) zgłoszenie naruszenia do Prezesa Urzędu Ochrony Danych, obejmujące informację, czy dokonano zgłoszenia, a w przypadku odpowiedzi twierdzącej wskazanie daty tego zgłoszenia.

Zgłaszanie naruszenia do Prezesa Urzędu Ochrony Danych

RODO wymaga, aby niektóre z przypadków naruszeń były zgłaszane do Urzędu Ochrony Danych. Decyzję o konieczności zgłoszenia danego naruszenia do Urzędu Ochrony Danych Osobowych podejmuje administrator danych i to on dokonuje zgłoszenia. Podmiot przetwarzający, u którego w związku z powierzeniem mu danych doszło do przypadku naruszenia bezpieczeństwa danych, nie zgłasza nigdy naruszenia do Urzędu Ochrony Danych, a jedynie powiadamia administratora o naruszeniu.

Kiedy administrator zgłasza naruszenie do Urzędu Ochrony Danych?

Z chwilą stwierdzenia, że doszło do naruszenia ochrony danych administrator jest zobowiązany przeprowadzić analizę, pod kątem ryzyka naruszenia praw lub wolności osób, których dane dotyczą. Właśnie ta pozwoli administratorowi stwierdzić, czy należy wypełnić obowiązek z art. 33 ust. 1 RODO (tj. zgłosić naruszenie organowi nadzorczemu) oraz art. 34 ust. 1 RODO (tj. zawiadomić osoby, których dane dotyczą, o naruszeniu).

Naruszenie należy zgłosić w terminie 72 godzin od chwili stwierdzania naruszenia.

Kiedy mimo wystąpienia incydentu naruszenia ochrony danych nie trzeba powiadamiać organu nadzorczego?

RODO wskazuje przypadki, kiedy wystąpienie naruszenia ochrony danych osobowych nie obliguje administratora do zgłaszania takiego incydentu organowi nadzorczemu. Ma to miejsce wtedy, kiedy jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (art. 33 ust. 1 RODO).

Jedną z najprostszych i mierzalnych metod oceny ryzyka naruszenia, która pomoże podjąć decyzję, czy dany incydent należy zgłosić do organu nadzoru, jest rozważenie negatywnych skutków naruszenia. Należy wtedy odpowiedzieć na pytanie, czy i jak bardzo prawdopodobna jest materializacja ryzyka:
a) dyskryminacji;
b) kradzieży tożsamości lub oszustwa dotyczącego tożsamości;
c) straty finansowej dla podmiotu danych;
d) naruszenia dobrego imienia podmiotu danych;
e) wystąpienia znaczącej szkody gospodarczej lub społecznej;
f) utraty kontroli nad danymi;
g) możliwości pozbawienia podmiotu danych przysługujących mu praw i wolności.

Dokonując oceny ryzyka, należy także ocenić, czy dotyczyło ono danych, które podlegają szczególnej ochronie przewidzianej w przepisach, tzn.:
a) danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe,

lub przynależność do związków zawodowych;
b) danych osobowych ujawniających dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa, lub związanych z tym środków bezpieczeństwa;
c) danych, z wykorzystaniem których oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych;
d) danych dotyczących osób wymagających szczególnej opieki, w tym dzieci;
e) danych osobowych prawnie chronionych, np. tajemnicą zawodową.

A także, czy naruszenie dotyczy:
a) danych, które uległy nieuprawnionemu odwróceniu pseudonimizacji lub odszyfrowaniu;
b) dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

Jeśli analiza doprowadzi do stwierdzenia, że naruszenie dotyczyło którejkolwiek z wymienionych grup danych, to ryzyko tego naruszenia jest wysokie. Takie podejście umożliwia szybką i obiektywną ocenę, jakie konsekwencje mogą grozić osobie, której dane dotyczą, i jaka jest szansa wystąpienia negatywnych skutków tego naruszenia.

Generalną zasadą wynikającą z RODO jest obowiązek zgłoszenia naruszenia do organu nadzorczego. W razie wątpliwości, czy dany przypadek należy zgłosić, rekomendujemy raczej podjąć działania w celu dokonania zgłoszenia, niż ich zaniechać. Z niezgłoszenia wynika bowiem duże ryzyko, a z decyzji o zgłoszeniu tylko konieczność uzupełnienia formularza, w oparciu o dane, które zostały już zgromadzone w procesie ustalenia naruszenia.

Ponadto RODO określa przypadki, w których, mimo że wystąpiło naruszenie ochrony danych, praw i wolności podmiotów danych w wyniku incydentu, administrator jest zwolniony z obowiązku powiadamiania osób, których dane dotyczą. Chodzi o sytuacje, gdy administrator wdrożył takie środki ochrony jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych, lub zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności.

Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych

O ile nie zachodzą przesłanki opisane w poprzednim akapicie na administratorze danych spoczywa także kolejny obowiązek, a mianowicie powiadomienie osoby, której dane dotyczą, o takim naruszeniu. Obowiązek ten istnieje w przypadku, jeśli naruszenie ochrony danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Administrator, rozważając czy w danym przypadku jest zobowiązany do powiadomienia podmiotów, powinien uwzględnić kryteria podobne jak w przypadku zgłaszania naruszeń organowi nadzorczemu.

Zawiadomienie powinno mieć formę pisemną lub e-mailową, tak aby podmiot danych miał możliwość wielokrotnego przeczytania treści powiadomienia. Forma ta jest też istotna pod względem rozliczalności działań administratora i ewentualnej możliwości wykazania przed UODO dokonanych czynności. Zawiadomienie należy skierować do podmiotu danych „bez zbędnej zwłoki", tzn. właściwie tak szybko, jak to możliwe. Administrator w zawiadomieniu do podmiotu danych wykorzysta opis i charakter naruszenia, który przekazany został mu przez podmiot przetwarzający. Do sytuacji, w których należy powiadomić podmiot danych, zalicza się utratę kontroli nad danymi na przykład na skutek działań hakerskich. W takiej sytuacji jest wysoce prawdopodobne, że dane zostaną wykorzystane w sposób, który naruszy prawa klientów, np. staną się oni ofiarami późniejszych kradzieży (wysokie ryzyko naruszenia praw lub wolności osób).

Monika Macura
radca prawny,
Partner w Kancelarii Konieczny Wierzbicki Spółka Partnerska,
specjalista w zakresie ochrony danych i nowych technologii

Przedmiotowe środki dowodowe w nowym Prawie zamówień publicznych

Jak potwierdzić spełnianie kryteriów?

Tomasz Sułkowski

1 stycznia 2021 r. po ponad rocznym vacatio legis weszła w życie ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 ze zm Dz. U. z 2021 r. poz. 1492, 2275, 288, 2320, 1517) (dalej: ustawa Pzp), która uchyliła i zastąpiła dotychczasową, wielokrotnie nowelizowaną ustawę z dnia 29 stycznia 2004 r. (dalej: ustawa uchylona). Wśród licznych i gruntownych zmian ustawodawca przemodelował i usystematyzował przepisy, zmodyfikował w różnym stopniu znane instytucje, wprowadził również szereg nowości. W kwestii podmiotowej i przedmiotowej oceny ofert ustawodawca wprowadził wyraźne rozróżnienie, a w ramach tej ostatniej wyróżnił etap badania wymogów podstawowych (zgodność z opisem zamówienia), etap badania parametrów preferowanych (określonych w opisie kryteriów oceny ofert) i wreszcie etap wykonawczy (wymagania związane z realizacją zamówienia).

Jak było wcześniej?

W dotychczasowym akcie prawnym kwestia dokumentów przedmiotowych była uregulowana szczątkowo w art. 25 ust. 1 pkt 2 uchylonej ustawy. Treść tego przepisu stanowiła, że:
W postępowaniu o udzielenie zamówienia zamawiający może żądać od wykonawców wyłącznie oświadczeń lub dokumentów niezbędnych do przeprowadzenia postępowania. Oświadczenia i dokumenty potwierdzające :
1) spełnianie warunków udziału w postępowaniu lub kryteria selekcji;
2) spełnianie przez oferowane dostawy, usługi lub roboty budowlane wymagań określonych przez zamawiającego
3) *brak podstaw do wykluczenia;*
– zamawiający wskazuje w ogłoszeniu o zamówieniu, specyfikacji istotnych warunków zamówienia lub zaproszeniu do składania ofert".

Zgodnie z § 13 uchylonego rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia:
W celu potwierdzenia, że oferowane roboty budowlane, dostawy lub usługi odpowiadają wymaganiom określonym przez zamawiającego, zamawiający może żądać w szczególności:
1) próbek, opisów, fotografii, planów, projektów, rysunków, modeli, wzorów, programów komputerowych oraz innych podobnych materiałów, których autentyczność musi zostać poświadczona przez wykonawcę na żądanie zamawiającego;
2) certyfikatu wydanego przez jednostkę oceniającą zgodność lub sprawozdania

z badań przeprowadzonych przez tę jednostkę, jako środka dowodowego potwierdzającego zgodność z wymaganiami lub cechami określonymi w opisie przedmiotu zamówienia, kryteriach oceny ofert lub warunkach realizacji zamówienia;

3) *zaświadczenia niezależnego podmiotu uprawnionego do kontroli jakości potwierdzającego, że dostarczane produkty odpowiadają określonym normom lub specyfikacjom technicznym;*
4) *zaświadczenia niezależnego podmiotu zajmującego się poświadczaniem spełniania przez wykonawcę określonych norm zapewnienia jakości, jeżeli zamawiający odwołuje się do systemów zapewniania jakości opartych na odpowiednich seriach norm europejskich;*
5) *zaświadczenia niezależnego podmiotu zajmującego się poświadczaniem spełnienia przez wykonawcę wymogów określonych systemów lub norm zarządzania środowiskowego, jeżeli zamawiający wskazuje środki zarządzania środowiskowego, które wykonawca będzie stosował podczas wykonywania zamówienia publicznego, odwołując się do unijnego systemu zarządzania środowiskiem i audytu (EMAS) lub do innych norm zarządzania środowiskowego opartych na odpowiednich normach europejskich lub międzynarodowych opracowanych przez akredytowane jednostki.*

Jak jest obecnie?

Przepisy art. 104–107 ustawy Pzp wprowadzają nową regulację dotyczącą przedmiotowych środków dowodowych. Odpowiadają one oświadczeniom i dokumentom potwierdzającym spełnianie przez oferowane dostawy, usługi lub roboty budowlane wymagań określonych przez zamawiającego, o którym mowa w art. 25 ust. 1 pkt 2 ustawy Pzp.

Definicja przedmiotowych środków dowodowych znajduje się w art. 7 pkt 20 ustawy Pzp, gdzie pod tym pojęciem należy rozumieć *„przewidziane ustawą środki służące potwierdzeniu zgodności oferowanych dostaw, usług lub robót budowlanych z wymaganiami, cechami lub kryteriami określonymi w opisie przedmiotu zamówienia lub opisie kryteriów oceny ofert, lub wymaganiami związanymi z realizacją zamówienia”*.

Podkreślenia wymaga, że żądanie przedmiotowych środków dowodowych jest zasadne jedynie w przypadku, gdy zamawiający określił cechy, wymagania i kryteria, które środki te mają potwierdzić. Brak takiego określenia powoduje, że żądanie przedłożenia konkretnego przedmiotowego środka dowodowego jest nieuzasadnione i niezgodnie z ustawą Pzp, gdyż nie jest niezbędne do przeprowadzenia postępowania. Powyższe znajduje swoje potwierdzenie np. w wyroku KIO 295/20 z dnia 27 lutego 2020 r. (LEX nr 2946261), w którym Izba wskazała:

„Żądanie przez zamawiającego dokumentów przedmiotowych, w sytuacji gdy w treści SIWZ nie przedstawiono wymagań odnoszących się do danego elementu dostaw, usług czy robót budowlanych, którego dotyczyć ma składany dokument, jest żądaniem nieskutecznym jako pozbawione podstawy prawnej i faktycznej. Analogicznie żądanie należy uznać za nieuzasadnione w przypadku, gdy dokument, którego zamawiający wymagał na potwierdzenie spełnienia określonych wymagań, nie jest niezbędny do przeprowadzenia postępowania”.

Przedmiotowe środki dowodowe są merytorycznie powiązane z opisem przedmiotu zamówienia, a nie kryteriami kwalifikacji wykonawcy. Odnoszą się one

bezpośrednio do właściwości przedmiotu przyszłego zobowiązania wykonawcy (przedmiotu zamówienia) i co do zasady są również w znaczeniu materialnym i formalnym częścią oferty rozumianej jako oświadczenie woli wyrażające zobowiązanie do określonego wykonania zamówienia. Dokumenty przedmiotowe należy traktować jako formę potwierdzenia zgodności oferowanego świadczenia z wymaganym przez zamawiającego, co oznacza, że zadeklarowana przez wykonawcę treść oferty musi znaleźć potwierdzenie w dokumentach przedmiotowych. W konsekwencji brak takiego potwierdzenia również jest podstawą do odrzucenia oferty.

Dokumenty

Podstawowym dokumentem składanym w celu potwierdzenia zgodności oferowanych robót budowlanych, dostaw lub usług z wymaganymi cechami lub kryteriami określonymi w opisie przedmiotu zamówienia lub opisie kryteriów oceny ofert, lub wymaganiami związanymi z realizacją zamówienia jest **certyfikat** wydany przez jednostkę oceniającą zgodność lub sprawozdania z badań przeprowadzonych przez tę jednostkę (art. 105 ust. 1 ustawy Pzp).

W przypadku zamówień o szczególnych cechach środowiskowych, społecznych lub innych, w celu potwierdzenia zgodności oferowanych robót budowlanych, dostaw lub usług z wymaganymi cechami, jeżeli spełnione są łącznie warunki określone w art. 104 ustawy Pzp, zamawiający może w opisie przedmiotu zamówienia, opisie kryteriów oceny ofert lub w wymaganiach związanych z realizacją zamówienia żądać od wykonawcy określonej **etykiety**. Etykieta oznacza *każdy dokument, w tym zaświadczenie lub poświadczenie, który potwierdza, że obiekt budowlany, produkt, usługa, proces lub procedura spełniają wymagania konieczne do uzyskania etykiety*. W przypadku, gdy zamawiający nie wymaga, aby roboty budowlane, dostawy lub usługi spełniały wszystkie wymagania etykiety, w opisie przedmiotu zamówienia wskazuje tylko wybrane, niezbędne dla zaspokojenia jego potrzeb wymagania z etykiety.

Katalog przedmiotowych środków dowodowych jest katalogiem otwartym, o czym świadczy treść art. 106 ust. 1 ustawy Pzp, zgodnie z którym zamawiający może żądać innych niż wskazane w art. 104 i 105 Pzp przedmiotowych środków dowodowych na potwierdzenie, że oferowane dostawy, usługi lub roboty budowlane spełniają określone przez zamawiającego wymagania, cechy lub kryteria, jeżeli są one niezbędne do przeprowadzenia postępowania. W ramach tego katalogu mieścić się będą dokumenty wymienione w § 13 uchylonego rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia. Nie może budzić wątpliwości, że inne przedmiotowe środki dowodowe żądane przez zamawiającego muszą zostać wskazane w dokumentach zamówienia lub ogłoszeniu o zamówieniu.

Funkcja przedmiotowa i podmiotowa

Konkretny dokument nie może pełnić w danym postępowaniu obu funkcji (podmiotowej i przedmiotowej), jednakże problemy mogą pojawić się z przyporządkowaniem danego środka dowodowego do środka podmiotowego lub przedmiotowego. Kryterium rozróżniającym i decydującym o odmiennej kwalifikacji dokumentów przedmiotowych jest cel ich składania oraz zakres informacji wynikający z ich treści. Zatem na poziomie typów środków dowodowych (np. certyfikatów, próbek, opisów) przyporządkowanie danego typu środka dowodowego do środka podmiotowego lub przedmiotowego będzie uzależnione od celu, jaki chce uzyskać zamawiający, żądając jego przedłożenia. Dokument w formie certyfikatu (np. ISO) potwierdzający, że wykonawca wdrożył odpowiednie normy produkcyjne co do zasady będzie środkiem dowodowym podmiotowym weryfikującym zdolność techniczną wykonawcy. Certyfikat wystawiany zaś na konkretny produkt oferowany przez wykonawcę w konkretnym postępowaniu będzie środkiem dowodowym przedmiotowym.

Problem kwalifikacji danego środka dowodowego dodatkowo komplikuje się ze względu na odmienne, w stosunku do dotychczasowego stanu prawnego, zakwalifikowanie części środków jako podmiotowe, a nie – tak jak dotychczas – przedmiotowe środki dowodowe. Zgodnie z § 9 ust. 1 pkt 11–13 rozporządzenia Ministra Rozwoju, Pracy i Technologii z 23.12.2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz. U. poz. 2415) *„W celu potwierdzenia*

spełniania przez wykonawcę warunków udziału w postępowaniu lub kryteriów selekcji dotyczących zdolności technicznej lub zawodowej, zamawiający może, w zależności od charakteru, znaczenia, przeznaczenia lub zakresu robót budowlanych, dostaw lub usług, żądać następujących podmiotowych środków dowodowych: (...)

11) w przypadku dostarczania produktów:
   a) próbek, opisów lub fotografii dostarczanych produktów, których autentyczność musi zostać poświadczona przez wykonawcę na żądanie zamawiającego,
   b) zaświadczenia niezależnego podmiotu uprawnionego do kontroli jakości potwierdzającego, że dostarczane produkty odpowiadają określonym normom lub specyfikacjom technicznym;

12) zaświadczenia niezależnego podmiotu zajmującego się poświadczaniem spełniania przez wykonawcę określonych norm zarządzania jakością, w tym dostępności dla osób niepełnosprawnych, jeżeli zamawiający odwołuje się do systemów zarządzania jakością opartych na odpowiednich seriach norm europejskich oraz certyfikowanych przez akredytowane jednostki;

13) zaświadczenia niezależnego podmiotu zajmującego się poświadczaniem spełnienia przez wykonawcę wymogów określonych systemów lub norm zarządzania środowiskowego, jeżeli zamawiający odwołuje się do systemu ekozarządzania i audytu, o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 1221/2009 z dnia 25 listopada 2009 r. w sprawie dobrowolnego udziału organizacji w systemie ekozarządzania i audytu we Wspólnocie (EMAS), uchylającym rozporządzenie (WE) nr 761/2001 oraz decyzje Komisji 2001/681/WE i 2006/193/WE (Dz. Urz. UE L 342 z 22.12.2009, str. 1, z późn. zm.), lub do innych norm zarządzania środowiskowego opartych na odpowiednich normach europejskich lub międzynarodowych oraz certyfikowanych przez akredytowane jednostki.".

Należy jednak podkreślić, że obowiązkiem zamawiającego będzie przyporządkowanie żądanego środka dowodowego do kategorii podmiotowej lub przedmiotowej, zależnie od celu, w jakim go żąda.

Żądanie przedmiotowego środka dowodowego jest możliwe tylko wówczas, gdy zamawiający w ogłoszeniu lub dokumentach zamówienia jednoznacznie wskaże wymagany środek. Zamawiający jest ograniczony w tym żądaniu koniecznością uwzględnienia zasad określonych w art. 106 ust. 2 ustawy, tj.:

- może żądać jedynie środków niezbędnych do przeprowadzenia postępowania – żądanie określonych przedmiotowych środków dowodowych bez równoczesnego określenia wymagań przedmiotowych jest niezgodne z przepisami ustawy Pzp, ale też nieskuteczne. Dokumenty te mają bowiem charakter wtórny w stosunku do określonych przez zamawiającego wymagań wobec przedmiotu zamówienia. W sytuacji gdy zamawiający nie określi w ogłoszeniu o zamówieniu lub dokumentach zamówienia wymagań wobec przedmiotu zamówienia, nie ma podstaw do żądania złożenia odpowiadających im przedmiotowych środków dowodowych;
- żądane środki powinny być proporcjonalne i związane z przedmiotem zamówienia. Zasada proporcjonalności przedmiotowych środków dowodowych oznacza konieczność doboru tych środków w sposób adekwatny do osiągnięcia celu postępowania o udzielenie zamówienia, czyli wyboru wykonawcy, który będzie zdolny realizować zamówienie zgodnie z wymaganiami, cechami lub kryteriami określonymi przez zamawiającego, przy jednoczesnym zachowaniu naczelnych zasad systemu zamówień publicznych (uczciwej konkurencji i równego traktowania wykonawców). Proporcjonalność przedmiotowego środka dowodowego będzie przejawiała się zatem we właściwym doborze tych środków w kontekście wymagań, które będą podlegały badaniu przez zamawiającego. Podobnie jest ze zwrotem „związany z przedmiotem zamówienia", który oznacza, że zasadność żądania określonych środków dowodowych winna być oceniana przez pryzmat celu, jakiemu ma on służyć, a więc zapewnieniu wyboru wykonawcy, który sprosta oczekiwaniom zamawiającego opisanym w dokumentach zamówienia i zrealizuje zamówienie zgodnie z wymaganiami. Nie można zatem wymagać przedłożenia przedmiotowych środków dowodowych, które wykraczają poza realizację tego celu;
- swoim żądaniem nie może ograniczać uczciwej konkurencji i równego traktowania wykonawców;
- musi zaakceptować równoważne przedmiotowe środki dowodowe, jeśli potwierdzają one spełnianie określonych przez zamawiającego wymagań, cech lub kryteriów. Ocena w tym zakresie będzie należała do zamawiającego, natomiast to na wykonawcy będzie spoczywał obowiązek udowodnienia równoważności danego dokumentu.

Powyższe zasady mają zabezpieczać prawidłowy przebieg postępowania i uniemożliwiać zamawiającemu żądanie dokumentów zbędnych lub do których dostęp jest utrudniony. Obowiązują one zarówno w przypadku etykiet oraz certyfikatów, jak i innych środków przedmiotowych.

Ponieważ przedmiotowe środki dowodowe są środkami służącymi zweryfikowaniu poprawności merytorycznej złożonej oferty, zamawiający musi mieć możliwość zapoznania się z nimi już na etapie badania oferty. Wobec powyższego na gruncie art. 107 ustawy Pzp ustanowiono nową regulację dotyczącą składania przedmiotowych środków dowodowych odmienną od tej, która dotyczy obowiązku składania środków podmiotowych. Przedmiotowe środki dowodowe wykonawcy składają wraz z ofertą.

Uzupełnienia

Ustawa Pzp wprowadza również uregulowania dotyczące uzupełniania przedmiotowych środków dowodowych, jednak jedynie w sytuacji, gdy nie zostały one złożone lub są niekompletne. Norma z art. 107 ust. 2 ustawy jest wzorowana na dotychczasowej normie z art. 26 ust. 3 ustawy Pzp, Po pierwsze, dopuszczalne będzie tylko uzupełnienie „braków formalnych", tj. braku dokumentu lub niekompletnego dokumentu, który nie pozwala przesądzić merytorycznie o wartości oferty. Nie będzie dopuszczalne uzupełnianie dokumentów przedmiotowych, jeśli przedłożone potwierdzają, że oferta jest niezgodna z opisem

przedmiotu zamówienia. Oznacza to, że przedmiotowe środki dowodowe nie będą uzupełniane, jeżeli na skutek merytorycznej oceny zamawiający uzna, że nie odpowiadają one wymaganiom przedmiotu zamówienia (nie potwierdzają, że wykonawca oferuje produkt lub usługę spełniającą oczekiwania zamawiającego). Powyższe koresponduje z dotychczasowym orzecznictwem, w którym przyjmuje się, że uzupełnieniu mogą podlegać takie dokumenty, które nie powodują zmiany oferowanego towaru/usługi, a jedynie stanowią doprecyzowanie parametrów technicznych, gdyż *w przeciwnym przypadku wystąpiłaby możliwość dokonywania dowolnego uzupełniania, zmiany oraz wszelkich modyfikacji oświadczeń i dokumentów, a w konsekwencji treści oferty, po upływie terminu składania ofert, co całkowicie burzyłoby porządek prawny w tym zakresie*. (Wyrok KIO 990/16 z 1.07.2016 r.) Tak jak dotychczas, uzupełnienie będzie mogło być jednokrotne w odniesieniu do danego przedmiotowego środka dowodowego.

Po drugie, regulacja dotycząca uzupełniania dokumentów jest regulacją fakultatywną. Oznacza to, że zamawiający będzie mógł skorzystać z przepisu, o ile przewidział tę możliwość w ogłoszeniu lub dokumentach zamówienia.

Po trzecie ustawa wyraźnie wyłączyła możliwość uzupełnienia przedmiotowego środka dowodowego służącego potwierdzeniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert. Zamawiający nie może zatem przewidzieć procedury poprawy przedmiotowych środków dowodowych w odniesieniu do tych spośród nich, które służą potwierdzeniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert. Takich środków nie można uzupełnić, oznaczałoby to bowiem uzupełnienie przedmiotu oferty. Postanowienie art. 107 ust. 3 uwzględnia dotychczasowy dorobek orzecznictwa KIO. Izba wielokrotnie wskazała, że nie jest możliwe uzupełnianie dokumentów składanych na potwierdzenie spełnienia kryteriów oceny ofert.

Ponadto przedmiotowy środek dowodowy nie podlega uzupełnieniu w sytuacji, gdy pomimo jego złożenia oferta podlega odrzuceniu lub zachodzą przesłanki unieważnienia postepowania (art. 107 ust. 3 ustawy Pzp).

Przykłady:

- KIO 1030/15 z dnia (LEX nr 1801855) – wyrok z dnia 3 czerwca 2015 r.

„Ustawodawca nie przewidział możliwości zastosowania trybów z art. 26 ust. 3 i 4 Pzp w zakresie kryteriów oceny ofert. Stosowanie uzupełnienia lub wyjaśnienia dokumentów na użytek kryteriów oceny oferty mogłoby w prosty sposób prowadzić do naruszenia zasady równego traktowania wykonawców i uczciwej konkurencji".

- KIO 638/17 LEX nr 2288066 – wyrok z dnia 19 kwietnia 2017 r.

„Informacje zawarte w ofertach wykonawców i oceniane w kryteriach oceny ofert nie podlegają uzupełnieniu i modyfikacji po upływie terminu na składanie ofert".

- KIO 81/20 LEX nr 2923312 – wyrok z dnia 27 stycznia 2020 r.

„Dopuszczenie możliwości uzupełniania dokumentów podlegających ocenie w ramach kryteriów oceny ofert jest niedopuszczalne. Zakres oferty służący do jej oceny w ramach kryteriów oceny ofert nie podlega uzupełnieniu po upływie terminu składania ofert".

Ustawa przewiduje również możliwość zastosowania instytucji wyjaśnienia w odniesieniu do przedmiotowych środków dowodowych. Bez względu na to, czy zamawiający przewidział możliwość wzywania o uzupełnienie przedmiotowych środków dowodowych, może on żądać wyjaśnień dotyczących tych środków dowodowych. Jeżeli będą one służyć potwierdzeniu zgodności oferowanych dostaw, usług lub robót budowlanych z wymaganiami określonymi w opisie przedmiotu zamówienia, podstawą wyjaśniania ich treści będzie art. 107 ust. 4 ustawy Pzp, natomiast w przypadku, gdy przedmiotowe środki dowodowe będą służyć potwierdzeniu zgodności oferowanych dostaw, usług lub robót budowlanych z kryteriami określonymi w opisie kryteriów oceny ofert, będą one stanowić treść oferty, a podstawą wyjaśniania ich treści będzie art. 223 ust. 1 zdanie pierwsze ustawy Pzp (Józef Edmund Nowicki „NOWE PZP. Składanie, uzupełnianie i wyjaśnianie przedmiotowych środków dowodowych").

Podsumowanie

Warto pamiętać o następujących rzeczach:

- kwalifikacja danego środka dowodowego wymaganego przez zamawiającego jako podmiotowego lub przedmiotowego jest zależna od celu, w jakim jest żądany;
- zamawiający może żądać przedłożenia przedmiotowego środka dowodowego na potwierdzenie zgodności oferowanych dostaw, usług lub robót budowlanych wyłącznie w związku z określonymi w opisie przedmiotu zamówienia lub opisie kryteriów oceny ofert wymaganiami, cechami lub kryteriami, lub określonymi wymaganiami związanymi z realizacją zamówienia, a więc gdy są one niezbędne do przeprowadzenia postępowania;
- żądane środki dowodowe muszą być proporcjonalne i związane z przedmiotem zamówienia, nie mogą ograniczać uczciwej konkurencji i równego traktowania wykonawców;
- zamawiający ma obowiązek akceptacji równoważnych przedmiotowych środków złożonych przez wykonawcę, jeśli potwierdzają one, że oferowane dostawy, usługi lub roboty budowlane spełniają określone wymagania, cechy lub kryteria;
- przedmiotowe środki dowodowe wykonawca składa wraz z ofertą. Podlegają one uzupełnieniu jedynie w sytuacji gdy zamawiający przewidział taką możliwość w ogłoszeniu o zamówieniu lub w dokumentach zamówienia i jedynie w razie ich braku lub niekompletności
- nie można uzupełnić przedmiotowego środka dowodowego składanego na potwierdzenie zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert;
- zamawiający może żądać wyjaśnień dotyczących treści przedmiotowych środków dowodowych.

Tomasz Sułkowski
Wspólnik Zarządzający w Kancelarii Prawa Gospodarczego GRAVIS LEGAL GROUP Widera, Sułkowski Spółka jawna, twórca blogu Między młotem a kowadłem

Oferty współpracy

Dania

Duński startup działający w branży meblowej zaprojektował ergonomiczne biurko do użytku domowego z regulacją wysokości. Aktualnie firma poszukuje partnera, który zajmie się produkcją tego wyrobu zgodnie z wytycznymi zamawiającego. Biurko składa się głównie z elementów aluminiowych, które należy pomalować proszkowo. Inne materiały użyte podczas produkcji biurka to płyta kompaktowa/drewno laminowane na blat biurka, okucia z polioksymetylenu (POM), plastikowe uchwyty, metalowe sprężyny i amortyzator gazowy. Pierwsza partia zamówienia obejmować będzie 500 sztuk, a do końca 2021 r. duńska firma planuje zamówić do 3000 sztuk biurek. Firma oferuje współpracę w oparciu o umowę produkcyjną. Numer referencyjny BRDK20210507001

Francja

Francuska firma specjalizująca się w handlu produktami dla niemowląt, poszukuje europejskiego producenta szkła do produkcji pojemników na żywność dla niemowląt. Poszukiwane pojemności szklane to 140 ml i 250 ml, z podziałką na ml i oz. Pojemniki muszą być wyposażone w szczelną pokrywę i odporne na nagłe zmiany temperatur. Firma oferuje współpracę w ramach umowy produkcyjnej. Numer referencyjny BRFR20210518001

Holandia

Holenderski producent opakowań z 40-letnim doświadczeniem poszukuje nowych rozwiązań, bardziej przyjaznych dla środowiska, np. monomateriałowych, łatwo poddających się recyklingowi. Poszukiwany partner musi wykazać się doświadczeniem w produkcji wysokiej jakości opakowań na żywność, spełniających określone normy. Firma oferuje współpracę w ramach umowy produkcyjnej. Numer referencyjny BRNL20210517001

Kosowo

Firma z Kosowa specjalizująca się w dystrybucji produktów z różnych sektorów zainteresowana jest wprowadzeniem na lokalny rynek nowych produktów, takich jak: środki czystości oraz produkty HORECA. Klient zainteresowany jest nawiązaniem współpracy w ramach umowy o świadczenie usług dystrybucyjnych. Numer referencyjny BRXK20210527001

Litwa

Litewska firma poszukuje producentów profili wytłaczanych z PCV. Firma specjalizuje się m.in. w produkcji mebli do przechowywania z tworzyw sztucznych. Tworzywo oferowanych profili powinno być dopuszczone do kontaktu z żywnością i zgodne z dyrektywą REACH. Profile powinny mieć 6 m długości. Firma szacuje wielkość zamówienia na 70 000–100 000 metrów rocznie. Numer referencyjny BRLT20210524001

Niemcy

Niemiecka firma cateringowa poszukuje partnera wyspecjalizowanego w obróbce tworzyw sztucznych (formowanie wtryskowe/tłocznie) do produkcji niestandardowych pokrywek do opakowań do żywności na wynos (silikon i guma termoplastyczna (TPE), polipropylen (PP), polietylen (PE)) spełniających wymagania projektowe wskazane przez przedsiębiorstwo. Firma oferuje współpracę w ramach umowy produkcyjnej. Numer referencyjny BRDE20210511002

Więcej ofert współpracy zagranicznej znajdą Państwo w bazie POD na stronie: www.een.org.pl (zakładka Oferty współpracy).

Rosja

Rosyjska firma stworzyła oprogramowanie do analizy wyników tomografii komputerowej klatki piersiowej, pozwalające na wykrywanie zachorowania na COVID-19 z pomocą sztucznej inteligencji. Firma oferuje roczną licencję placówkom medycznym, centrom diagnostycznym i producentom sprzętu medycznego. Numer referencyjny BORU20210430001

Rumunia

Rumuńska firma działająca jako agent handlowy reprezentujący swoich klientów na rynkach arabskich nawiąże współpracę z producentami lub dystrybutorami produktów spożywczych i farmaceutycznych, takich jak np. świeże warzywa i owoce, konserwy i żywność suszona, artykuły medyczne, kosmetyki (szampony, odżywki, kremy, balsamy, dezodoranty, środki higieny osobistej), produkty farmaceutyczne. Rumuńska firma zainteresowana jest zawarciem umowy dystrybucyjnej lub agencyjnej. Numer referencyjny BRRO20210429001

Wielka Brytania

Doświadczony brytyjski dystrybutor poszukuje nowych, unikalnych rozwiązań stworzonych z myślą o osobach z niepełnosprawnościami, przewlekle chorych i starszych. Oferowane produkty powinny przyczyniać się do samodzielności osób o ograniczonej mobilności, zarówno dzieci jak i dorosłych, i wspomagać ich opiekunów. Firma zainteresowana jest również rozwiązaniami z zakresu higieny i prewencji zakażeń. Numer referencyjny BRUK20210223001

Brytyjska firma działająca jako przedstawiciel handlowy poszukuje nowych produktów zdrowotnych i żywności ekologicznej do wprowadzenia na rynek brytyjski. Firma oferuje współpracę w oparciu o umowę agencyjną. Numer referencyjny BRUK20210427001

Skorzystaj z bezpłatnych porad ekspertów

Ośrodek Enterprise Europe Network przy PARP oferuje bezpłatne usługi informacyjne z zakresu prawa oraz polityk i programów UE, internacjonalizacji przedsiębiorstw, innowacji i transferu technologii

Nasi konsultanci

Odpowiedzą na pytania dotyczące kwestii prawnych związanych z prowadzeniem działalności gospodarczej na wspólnym rynku europejskim (Polska i inne kraje Unii Europejskiej), obejmujących w szczególności dziedziny takie jak:

- sprzedaż towarów i świadczenie usług na wspólnym rynku UE
- rozpoczynanie działalności gospodarczej
- zatrudnianie pracowników
- wprowadzanie produktów do obrotu, bezpieczeństwo produktów, oznakowanie CE
- podatki i cła
- ochrona konkurencji i konsumentów
- własność intelektualna i przemysłowa
- zamówienia publiczne

Pomogą w nawiązaniu współpracy biznesowej i technologicznej z zagranicznymi partnerami

Udzielą informacji na temat wsparcia finansowego i organizacyjnego dostępnego w ramach programów Unii Europejskiej, np. HORYZONT 2020 i COSME

Zapraszamy do zadawania pytań za pośrednictwem formularza kontaktowego na stronie

https://www.een.org.pl/een/bezplatne-porady-naszych-ekspertow

PARP Grupa PFR / Centrum Rozwoju MŚP

enterprise europe network

Wsparcie dla biznesu w zasięgu ręki

Komisja Europejska