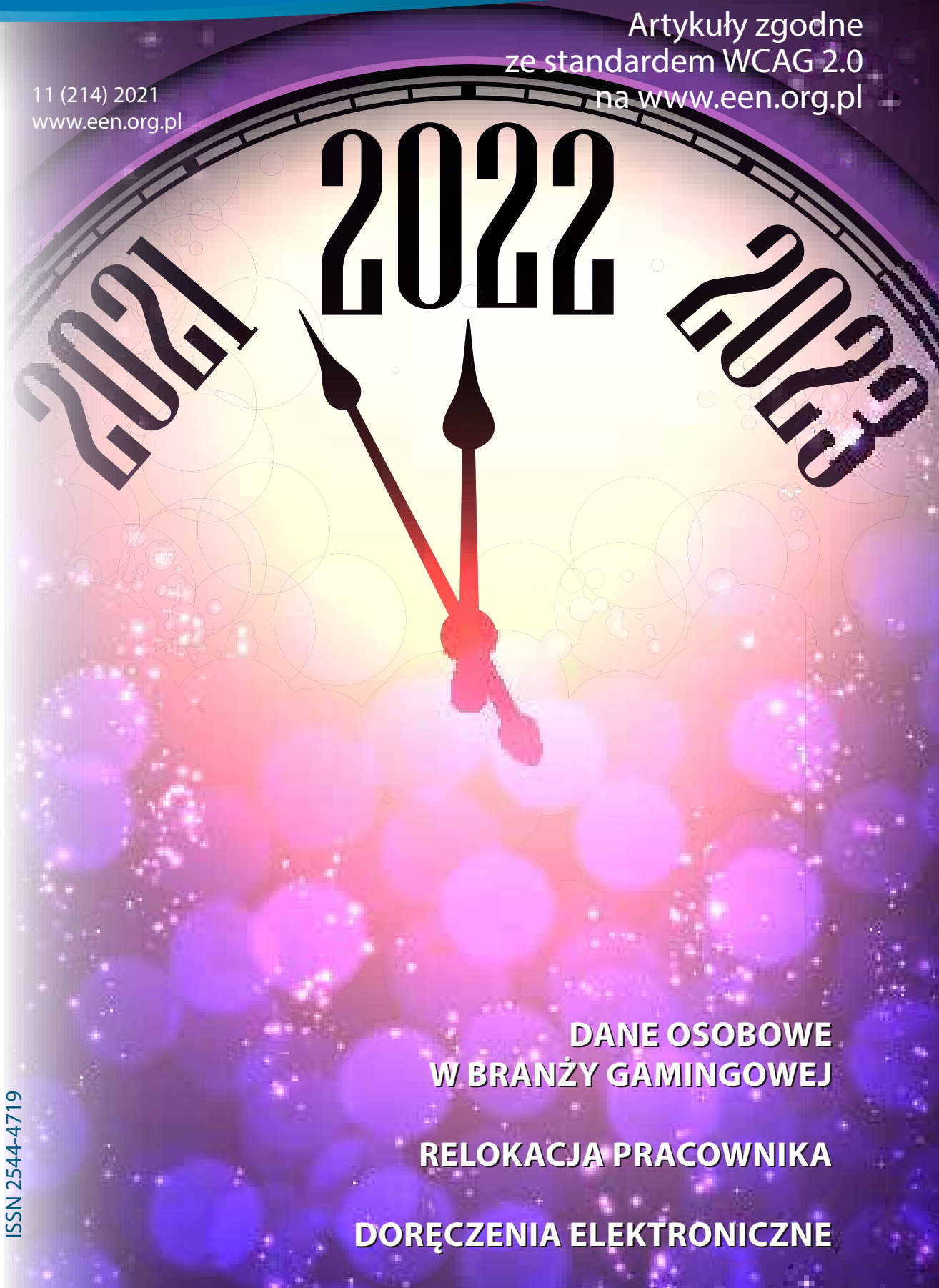


Artykuły zgodne
ze standardem WCAG 2.0
na www.een.org.pl

11 (214) 2021
www.een.org.pl

BIULETYN EURO INFO

ISSN 2544-4719

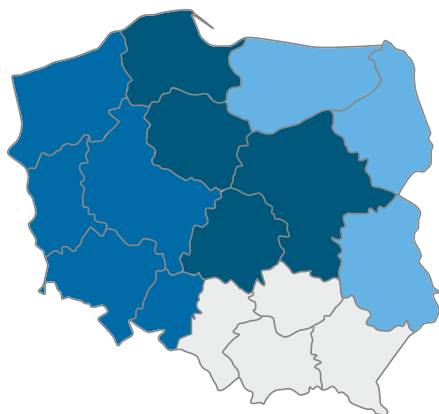


**DANE OSOBOWE
W BRANŻY GAMINGOWEJ**

RELOKACJA PRACOWNIKA

DORĘCZENIA ELEKTRONICZNE

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

Institut 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/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 Kiszelin
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,

„Rozwój jednolitego rynku europejskiego oraz fakt, że Polska wkrótce stanie się jego częścią, niesie ze sobą wiele korzyści, ale i zagrożeń...” – tak rozpoczynał się artykuł wstępny w pierwszym numerze Biuletynu Sieci EURO INFO CENTRES (EIC), który został wydany w maju 1998 r. Był to czas, kiedy po zakończeniu pierwszego etapu transformacji gospodarczej, Polska rozpoczęła negocjacje w sprawie członkostwa w Unii Europejskiej. Co się działo przez 23 lata? Mnóstwo. Udało się nam przebudować i dostosować gospodarkę do wymogów Unii Europejskiej. Wstąpiliśmy do UE i dzisiaj jesteśmy jej pełnoprawnym członkiem. W latach 2008-11 przeszliśmy najgłębszy od 1929 r. kryzys ekonomiczny ze wszystkimi jego negatywnymi konsekwencjami. Jednak, pomimo wszelkich perturbacji, należy stwierdzić, że wyszliśmy z tego wzmocnieni, czego najlepszym dowodem jest spektakularny wzrost gospodarczy i spadek bezrobocia w ostatnich kilku latach.

Przez cały ten czas nasze pismo starało się dołożyć swoją drobną cegiełkę do przybliżenia polskim przedsiębiorcom zasad działania wspólnego rynku, przedstawienia najważniejszych aspektów prawa unijnego, poinformowania, na jakie mogą liczyć dofinansowanie z funduszy unijnych, wskazania, w jakich spotkaniach biznesowych mogą wziąć udział itd. Nasze starania będziemy kontynuować w kolejnych latach, jednak – zgodnie z duchem czasu – chcieliśmy zaprosić naszych Czytelników do skorzystania z naszej oferty dostępnej na portalu www.een.org.pl. Obiecujemy dostarczyć Wam równie ciekawe i wartościowe informacje co do tej pory. Przy tym zrobimy to w sposób szybszy, wygodniejszy i bardziej przyjazny środowisku.

Wszystkiego dobrego w Nowym Roku i do zobaczenia na www.een.org.pl.

Zespół Redakcyjny
Biuletynu Euro Info

Redakcja nie zwraca materiałów niezamówionych oraz zastrzega sobie prawo do ich zmiany i redagowania. Uwagi i komentarze prosimy kierować na adres: biuletyn_ei@parp.gov.pl.

Wszystkie teksty zawarte w Biuletynie Euro Info mogą być przedrukowane wyłącznie po uzyskaniu zgody redakcji. Zainteresowanych prenumeratą prosimy o kontakt z najbliższym ośrodkiem Enterprise Europe Network.

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 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”.

Komisja Europejska lub osoby występujące w jej imieniu nie są odpowiedzialne za informacje przedstawione w publikacji. Poglądy wyrażone w publikacji są poglądami Autorów i nie muszą pokrywać się z działaniami Komisji Europejskiej.

Spis treści

- 4 | **Ochrona danych osobowych**
Prawnie uzasadniony interes administratora

- 10 | **Prawo pracy**
Outsourcing pracowników

- 14 | **Sztuczna inteligencja**
Odpowiedzialność za szkody wynikające z działania systemów sztucznej inteligencji

- 18 | **Ochrona własności intelektualnej**
Rejestracja znaku towarowego a prawo autorskie

- 21 | **Działalność gospodarcza**
Tajemnica przedsiębiorcy i tajemnica przedsiębiorstwa, cz. II

- 25 | **Publikacja Enterprise Europe Network**
Sprzedaż internetowa na nowych zasadach

- 31 | **Oferty współpracy**

Redaktor naczelny: Paweł Sikorski
Zespół: 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.ccp.com.pl
Zdjęcia: AdobeStock
Nakład: 1400 egz.

Prawnie uzasadniony interes administratora

Przesłanka legalnego przetwarzania danych osobowych

Jędrzej Klatka

Przetwarzanie danych jest zgodne z prawem między innymi wtedy, gdy wynika to z prawnie uzasadnionych interesów administratora. Jest to jedna z sześciu przesłanek. Zgodnie z art. 6 ust. 1 lit. f RODO przetwarzanie jest zgodne z prawem, gdy i w takim zakresie, w jakim jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią. Wyjątkiem są sytuacje, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Przepis nie ma zastosowania do przetwarzania, którego dokonują organy

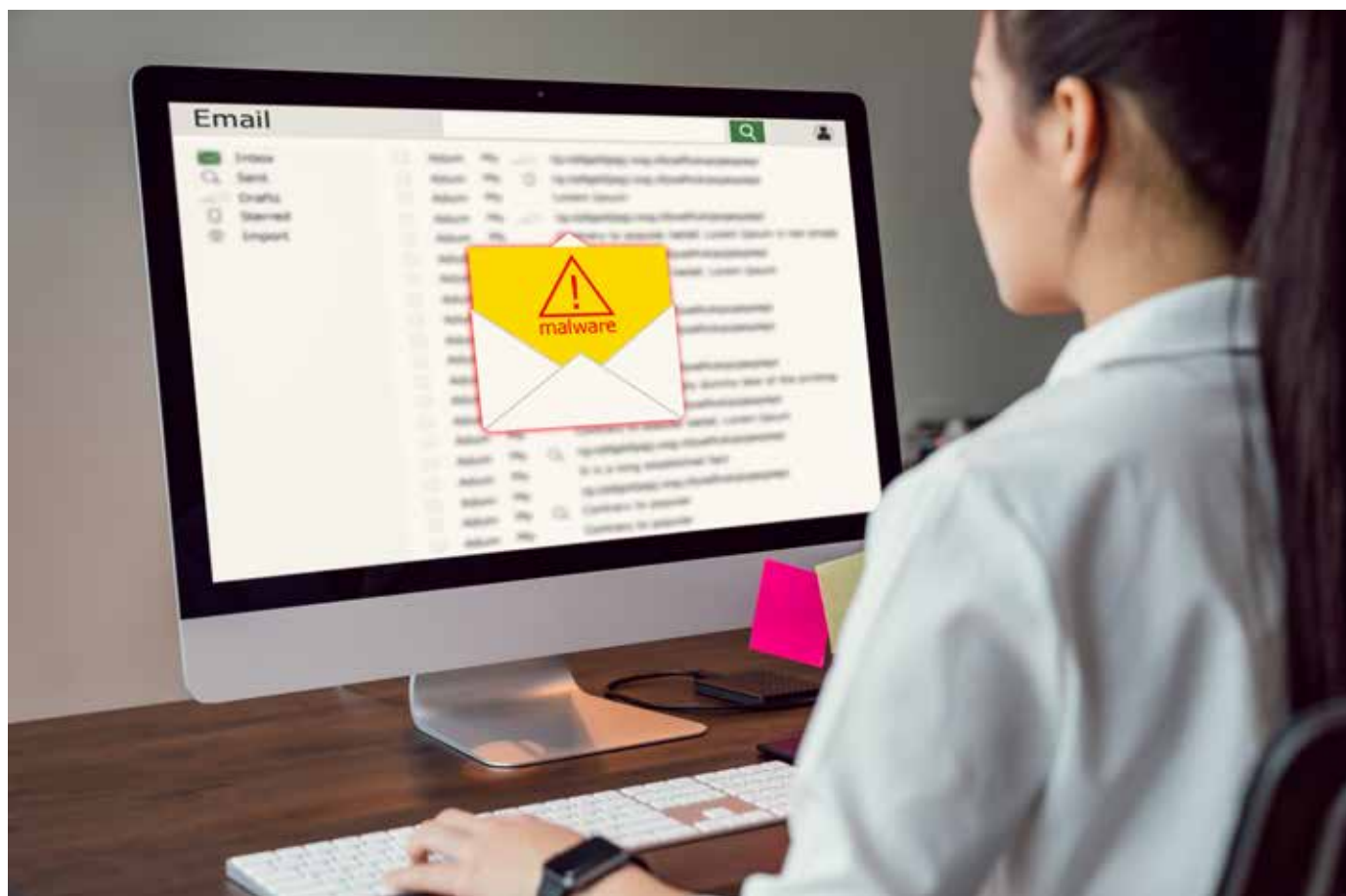
publiczne w ramach realizacji swoich zadań.

Przetwarzanie danych

Zgodnie z art. 4 pkt 2 RODO przetwarzanie to operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub nieautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie².

Wybór podstawy przetwarzania

Rozpoczynając działalność, która wiąże się z przetwarzaniem danych osobowych, administrator musi zawsze zastanowić się, jaka podstawa planowanego przetwarzania będzie odpowiednia. Decydując się na przetwarzanie danych na podstawie PUI administrator nie uzyskuje już zgody osoby, której dane dotyczą³. Administrator przy tym nie może stosować uzasadnionego interesu z mocą wsteczną jako podstawy uzasadniającej przetwarzanie danych w sytuacji powstania wątpliwości co do ważności zgody. Konsekwencją niespełnienia wymogów dotyczących świadomej





zgody będzie nieważność zgody i naruszenie art. 6 RODO⁴.

Przetwarzanie na podstawie art. 6 ust. 1 lit. f RODO jest możliwe, gdy nie ma innej podstawy prawnej.

Niedookreślone brzmienie przepisu w sposób zamierzony umożliwia większą swobodę decyzyjną. Ponadto za pomocą określeń wartościujących odsyła do norm pozaprawnych, które ocenia się w każdym przypadku indywidualnie. Zatem art. 6 ust. 1 lit. f ma charakter klauzuli generalnej. Jak podnosi się w doktrynie: *pozwała to na bieżącą aktualizację katalogu przypadków uzasadnionego przetwarzania opartego na interesie administratora, niezależnie od pojawiających się nowości technologicznych, czy modeli biznesowych*⁵. Interes administratora powinien wynikać z prawa, co należy rozumieć szeroko⁶.

Motywy nr 47-49 RODO wskazują przykładowe uzasadnione interesy administratora dla przetwarzania danych osobowych. Są to m.in. przypadki, gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz, mające na celu zapobieganie oszustwom. Możliwe jest również uzasadnione przetwarzanie do celów marketingu bezpośredniego.

Zgodnie z motywem 48 administratorzy, którzy są częścią grupy przedsiębiorstw lub instytucji powiązanych z podmiotem centralnym, mogą mieć prawnie uzasadniony interes w przesyłaniu danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych, co dotyczy też przetwarzania danych osobowych klientów lub pracowników.

Zgodnie z motywem 49 dane osobowe powinny być przetwarzane w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji – tj. zapewnienia odporności sieci lub systemu informacyjnego na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzejazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych – oraz bezpieczeństwa związanych z nimi usług.

Aby stwierdzić istnienie prawnie uzasadnionego interesu, należałoby w każdym

przypadku przeprowadzić dokładną ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w tym celu. Interesy i prawa podstawowe osoby, której dane dotyczą, mogą być nadrzędne wobec interesu administratora danych w szczególności w przypadkach, gdy dane osobowe są przetwarzane w sytuacji, w której osoby, których dane dotyczą, nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania.

Warto także podkreślić, że pomimo możliwości szerokiego zastosowania omawianego przepisu, w dalszym ciągu spełnia on wysokie standardy ochrony, ze względu na uprzednią konieczność każdorazowej oceny stanu faktycznego i wykonania testu równowagi opartego na wazieniu interesów.

Kiedy można przetwarzać na podstawie prawnie uzasadnionego interesu?

Stosowanie przez przedsiębiorcę podstawy przetwarzania danych osobowych z art. 6 ust. 1 lit. f RODO wymaga łącznego spełnienia wszystkich wymienionych tam przesłanek. Ocena, czy przesłanki zostały spełnione, musi nastąpić przed przetwarzaniem danych osobowych.

Po pierwsze należy ocenić, **czy przetwarzanie danych jest niezbędne** i konieczne. Pomocne może być rozważenie, czy nie ma innego sposobu na osiągnięcie danego celu albo czy inny sposób wymagałby nieproporcjonalnego wysiłku⁷. Aby uznać, że przetwarzanie jest niezbędne, musi występować bezpośredni związek pomiędzy realizacją interesu a potrzebą przetwarzania danych osobowych. Każdą kategorię przetwarzanych danych⁸ (np. imię nazwisko, PESEL), należy odrębnie przeanalizować i ocenić, czy wszystkie przetwarzane dane są niezbędne administratorowi, uwzględniając zasadę minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c. RODO.

Po drugie należy ocenić, **czy dane osobowe są wykorzystywane do celów**

wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią. Oceniając interes można zadać sobie następujące pytania:

- W jakim celu chcę przetwarzać dane, co chcę tym osiągnąć?
- Jak ważne są korzyści z przetwarzania i kto je czerpie?
- Jakie byłyby skutki, gdybym nie mógł kontynuować przetwarzania?
- Czy wykorzystywanie danych po ustaniu przetwarzania byłoby w jakikolwiek sposób nieetyczne lub niezgodne z prawem?⁹

Po trzecie należy **wykonać test równowagi**¹⁰, który na wazieniu interesów administratora oraz osoby, której dane są przetwarzane¹¹.

Jeżeli choć jedna z ww. przesłanek nie zostanie spełniona, wtedy administrator może zmniejszyć zakres przetwarzanych danych, zmienić charakter przetwarzania lub wprowadzić dodatkowe zabezpieczenia. Bez względu na to, jakie działania zostaną podjęte, administrator jest zobowiązany do ponownego przeprowadzenia testu równowagi. Gdy wprowadzone zmiany nie zmienią wyniku testu, administrator nie może przetwarzać danych na tej podstawie i powinien znaleźć alternatywną podstawę prawną albo nie rozpoczynać przetwarzania¹². Sprzeczne z art. 6 ust. 1 lit. f RODO będzie nadmierna ingerencja w prywatność osób fizycznych lub znaczne ryzyko wyrządzenia im szkody. Administrator nie może przetwarzać danych na podstawie art. 6 ust. 1 lit. f RODO, jeżeli przetwarzanie jest dopuszczalne na innej podstawie prawnej.

Zgodnie z art. 5 ust. 2 RODO (zasadą rozliczalności) administrator musi być w stanie wykazać przestrzeganie RODO, a więc przetwarzając dane na podstawie art. 6 ust. 1 lit. f RODO administrator musi wykazać, że wszystkie trzy przesłanki były łącznie spełnione¹³. Wyniki wykonanej przez administratora analizy powinny być utrwalone, ponieważ w razie ewentualnej kontroli może to być jedyny sposób wykazania, że wybierając tę podstawę przetwarzania administrator ocenił zasadność tego wyboru oraz uwzględnił prawa i interesy osób, których dane były przetwarzane¹⁴.



Nawet spełnienie przesłanek wymienionych w art. 6 ust. 1 RODO nie wystarcza do przetwarzania danych wrażliwych wymienionych w art. 9 ust. 1 RODO¹⁵. Wyjątki od zakazu przetwarzania danych wrażliwych są wymienione w art. 9 ust. 2 RODO¹⁶.

Przetwarzając dane na podstawie art. 6 ust. 1 lit. f RODO administrator powinien:

- przeprowadzić i udokumentować wyniki trzystopniowego testu,
- poinformować osoby, których dane dotyczą, o tym jakie uzasadnione interesy są realizowane,
- umożliwić im wyrażenie sprzeciwu wobec operacji opartych na tej podstawie¹⁷.

Test równowagi

Test równowagi polega na porównaniu z jednej strony prawnie uzasadnionego interesu administratora danych (lub osoby trzeciej), a z drugiej strony, praw i wolności osoby, której dane dotyczą. Jeżeli przeważające będą prawa podmiotu danych, to administrator nie powinien opierać przetwarzania danych na podstawie art. 6 ust. 1 lit f RODO¹⁸.

Celem testu równowagi jest sprawdzenie, czy podstawowe wolności, prawa i interesy osób są nadrzędne względem prawnie uzasadnionego interesu administratora. Test równowagi z założenia powinien być przeprowadzony jak najbardziej obiektywnie. Dobrą praktyką jest przeprowadzenie testu przez możliwe niezależnego pracownika na przykład Inspektora Ochrony Danych.

Przy wykonywaniu testu równowagi należy wziąć pod uwagę zarówno charakter interesów, jak i zakres i kategorie przetwarzanych danych. Należy uwzględnić:

- czy osoby, których dane będą przetwarzane, mogą spodziewać się takiego przetwarzania oraz jaki to wywrze na nie wpływ,
- status osoby i administratora,
- sposób przetwarzania danych,
- czy dokonywana jest publikacja bądź czy ujawnia się dane dużej liczbie osób/podmiotów,
- czy przetwarzanie odbywa się na dużą skalę¹⁹,
- interes podmiotu danych,

- rodzaj prawa lub wolności,
- zagrożenia wynikające z przetwarzania danych,
- relacje między podmiotami przetwarzającym i podmiotem danych,
- łatwość z jaką podmiot danych może doprowadzić do zaniechania przetwarzania,
- indywidualną sytuację podmiotu danych, w tym jego wiek²⁰.

Podczas wykonywania testu równowagi należy pamiętać, że dane osobowe nie są równorzędne. Inaczej traktuje się przetwarzanie numeru PESEL czy karty kredytowej, a inaczej przetwarzanie adresu e-mail lub imienia i nazwiska. Wynika to z odmiennych zagrożeń i konsekwencji przetwarzania dla podmiotu danych. Dla wyważenia interesów wskazanych podmiotów mają również znaczenie środki prawne, które przysługują podmiotowi w celu ochrony jego interesów i praw. Za szybki i efektywny należy uznać sprzeciw, który powoduje zablokowanie możliwości przetwarzania danych.

Dane dzieci są pod szczególną ochroną i zazwyczaj uznaje się ich nadrzędność wobec interesów administratora. Zgodnie z art. 8 ust. 1 RODO, można wyróżnić dwa progi wiekowe dzieci podlegające różnej ochronie. Przetwarzanie danych osobowych dzieci do 13 roku życia powinno nastąpić tylko w wyjątkowych i szczególnych przypadkach. Natomiast w przypadku dzieci powyżej wskazanego wieku przetwarzanie jest bardziej zliberalizowane, ale również w tym przypadku należy brać pod uwagę prymat interesów dziecka.

Przykładowymi zabezpieczeniami, które mają wpływ na wynik testu równowagi, są:

- minimalizacja danych,
- anonimizacja *bądź* pseudonimizacja,
- wielopoziomowe uwierzytelnianie,
- ograniczony czas i dostęp przetwarzania danych,
- szyfrowanie²¹.

Zgodnie z wytycznymi Grupy Roboczej art. 29: „konkretny interes musi zostać zidentyfikowany, jako dający korzyści osobie, której dane dotyczą. W ramach najlepszej praktyki administrator może udzielić osobie, której dane dotyczą, informacji z testu równowagi, który musi zostać wykonany przed każdym

zbieraniem danych osobowych od osób, których dane dotyczą, w celu umożliwienia oparcia się na art. 6 ust. 1 lit. f. Niniejsze może zostać zawarte w warstwowym oświadczeniu/informacji o prywatności, aby uniknąć zmęczenia informacją. Informacja powinna wyjaśniać, że można uzyskać informacje dotyczące testu równowagi na żądanie. Jest to istotne dla efektywnej przejrzystości, gdy osoby, których dane dotyczą, mają wątpliwości co do rzetelnego przeprowadzenia testu bilansującego lub chcą złożyć skargę do organu nadzorczego²².

Czym jest prawnie uzasadniony interes w kontekście działalności przedsiębiorcy?

Przedsiębiorca ma możliwość przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f RODO w związku z prowadzeniem przedsiębiorstwa. Poniżej wskazano przykłady, które związane są z przedsiębiorcą jako podmiotem, który prowadzi działalność gospodarczą, a w ramach tej działalności pozyskuje klientów. Ponadto możliwe jest również skorzystanie z ww. podstawy prawnej dla ochrony praw przedsiębiorcy, zwłaszcza prawa do zachowania dobrego imienia. Kolejnymi przykładami są interesy, które dotyczą przedsiębiorcy jako pracodawcy.

Zgodnie z poglądami doktryny uzasadniony interes administratora może przejawiać się m.in. przy identyfikowaniu podejrzanych płatności, monitoringu osób, które mają dostęp do pieniędzy czy systemów weryfikujących klientów (np. w bankach, czy w celu zapobiegania kradzieżom i aktom wandalizmu, jednak z zastrzeżeniem miejsc w których podstawowe prawa i wolności mogą być poprzez monitoring naruszone, np. w przebiegach²³, działalności wyszukiwarek internetowych (umożliwienie dostępu do informacji podmiotowi danych, chyba że dane mają charakter pomówień)²⁴, wyświetlaniu reklam czy ofert kolejnych zakupów klientom sklepów internetowych podających swoje dane przy zamówieniu²⁵, ocenie ryzyka potencjalnych klientów (np. określenie



zdolności kredytowej), jak również przy działaniach compliance polegających na dochodzeniu roszczeń, ustaleniem, dochodzeniem lub obroną przed roszczeniami, także tymi, które wynikają z zawartych umów ubezpieczeniowych.

W przypadku powołania się na interes administratora do celów marketingu bezpośredniego należy mieć na uwadze przepisy szczególne, które wymagają uzyskania zgody od osoby, do której są kierowane²⁶ (np. ustawa o prawie telekomunikacyjnym²⁷, ustawa o świadczeniu usług drogą elektroniczną²⁸). Przedsiębiorca powinien w klauzuli informacyjnej w związku z marketingiem bezpośrednim wskazać, na czym konkretnie polega uzasadniony interes – np. na promowaniu posiadanego asortymentu lub obowiązujących promocji. Ponieważ może to być związane z ryzykiem ujawnienia danych dotyczących sfery prywatnej lub życia rodzinnego, w sytuacji gdy używanie tych danych w konkretnej sytuacji nie jest niezbędne²⁹.

Orzecznictwo przesądziło, że istnieje możliwość powoływania się na klauzulę prawnie usprawiedliwionego celu w przypadku przetwarzania danych dłużnika w związku z cesją wiarytelności konsumenckiej³⁰.

Możliwe jest w tym trybie uzyskanie adresu IP³¹ osoby, która anonimowo za pomocą strony internetowej zgłosiła³² przedsiębiorcę³³.

Trybunał Unii Europejskiej orzekł, że art. 6 ust. 1 lit. f) RODO nie stoi na przeszkodzie systematycznej rejestracji adresów IP użytkowników sieci, których łącza internetowe miały być wykorzystywane do naruszeń prawa, tj. udostępniania plików zawierających utwory bez zezwolenia. Nie sprzeciwia się też podawaniu nazw i adresów pocztowych użytkowników do wiadomości podmiotu praw własności intelektualnej lub osoby trzeciej w celu wniesienia powództwa o odszkodowanie. Jednak wnioski i żądania kierowane w tym zakresie powinny być uzasadnione, proporcjonalne i nie mieć znamion nadużycia³⁴.

Należy podkreślić, że ww. podobieństwo do ww. przykładów nie są wystarczające dla zgodnego z prawem przetwarzania w świetle art. 6 ust. 1 lit. f) RODO. Niezbędna jest każdorazowa ocena, czy

występuje nadrzędny interes podmiotu, którego dane osobowe są przetwarzane i wykonanie testu równowagi³⁵.

Przedsiębiorca jako pracodawca

Przetwarzanie danych pracowniczych na podstawie art. 6 ust. 1 lit. f) RODO uzasadnione jest w aspekcie dbania o dobro zakładu pracy³⁶. Możliwe jest prowadzenie rejestru osób odwiedzających³⁷.

W każdym z tych przypadków interesem jest zapewnienie bezpieczeństwa pracowników i innych osób przebywających na terenie zakładu pracy i zapewnienie przez pracodawcę bezpiecznych i higienicznych warunków pracy, zgodnie z art. 207 Kodeksu pracy³⁸.

Interes pracodawcy, który jest przedsiębiorcą oraz jednocześnie administratorem danych osobowych oraz interes pracowników często jest wspólny³⁹. Dlatego pracodawca jest uprawniony zwłaszcza w pewnych zawodach do ujawniania m.in. służbowego adresu e-mail⁴⁰ czy imienia i nazwiska pracownika⁴¹. Dlatego podnosi się, że w czasach rozwoju gospodarczego i cywilizacyjnego rozwoju gospodarczego należy zastanowić się nad liberalizacją poglądów dotyczących wizerunku pracownika⁴².

Warto zauważyć, że Prezes UODO nakazał usunięcie ze strony internetowej danych osobowych osoby fizycznej w upadłości likwidacyjnej pozyskanych z Monitora Sądowego i Gospodarczego uznając, że z uwagi na sytuację osobistą, takie udostępnienie narusza prawa i wolności osobiste, w szczególności powoduje dyskryminację w zatrudnieniu („negatywnie wpływa na prowadzone przez niego rozmowy kwalifikacyjne i naraża go na nieprzyjemności”)⁴³.

Przykłady przetwarzania danych na podstawie art. 6 ust. 1 lit. f) RODO

Prezes Urzędu Ochrony Danych Osobowych w swoich dotychczasowych decyzjach uznał, że warunek istnienia ważnego interesu administratora danych osobowych jest spełniony gdy:

- 1) administrator udostępnia w Internecie imię, nazwiska, adres zamieszkania oraz informacje o wysokości zadłużenia – ponieważ było to niezbędne dla podejmowania działań zmierzających do zawarcia umowy sprzedaży wierzytelności⁴⁴,
- 2) bank przetwarza dane w związku z art. 118 i art. 4421 oraz 731 Kodeksu cywilnego⁴⁵ – ponieważ dane były przetwarzane w celu dochodzenia i obrony przed ewentualnymi



- roszczeniami oraz w zw. z art. 105a ust. 5 Prawa bankowego w celu stosowania metod wewnętrznych oraz innych metod i modeli, o których mowa w części trzeciej rozporządzenia UE nr 575/2013⁴⁶,
- 3) Spółka przetwarza dane jedynie w celu wykonania ciężących na niej obowiązków prawnych związanych z rozpatrzeniem skargi, a nie w celu marketingu usług i produktów własnych⁴⁷,
- 4) dane są przetwarzane w celu obrony przed ewentualnymi roszczeniami, m.in. w związku z postępowaniem prowadzonym przed Prezesem UODO⁴⁸,
- 5) Spółka przetwarza (w tym udostępnianie) publicznie dostępne dane związane z jej dobrowolnym uczestnictwem w podmiocie podlegającym wpisowi do KRS⁴⁹,
- 6) bank przetwarza dane do celów jedynie do celów statystycznych⁵⁰,
- 7) bank przetwarza dane w zakresie numeru umowy kredytowej oraz ich usunięcia przez instytucję upoważnioną m.in. do zbierania i udostępniania informacji o wiarygodnościach, gdyż jest niezbędne dla dochodzenia roszczeń⁵¹,
- 8) towarzystwo ubezpieczeń dochodzi i broni się przed roszczeniami związanymi z zawartymi ze Skarżącym umowami ubezpieczenia i zgłoszoną szkodą i wypłatą świadczenia w związku z zajściem zdarzenia ubezpieczeniowego oraz w zw. z postępowaniem Inspektora Ochrony Danych Towarzystwa w sprawie sprzeciwu Skarżącego wobec przetwarzania jego danych w celach archiwalnych⁵²,
- 9) zarządca nieruchomości udostępnia dane jednostce budżetowej miasta na potrzeby windykacji należności z tytułu bezumownego korzystania z gruntu⁵³,
- 10) Prezes Sądu Okręgowego tylko w niezbędnym zakresie udostępnia dane, które udostępnił sam Skarżący, w oświadczeniu zamieszczonym na stronie internetowej Sądu i jako podmiot reprezentujący tę instytucję na zewnątrz odnosi się do wymawianych publicznie zarzutów kierowanych pod adresem sędziów, w tym personalnie do osoby je formułującej⁵⁴,
- 11) bank pozyskuje informacje o kraju rezydencji podatkowej klienta oraz jego statusu rezydenta podatkowego w innych krajach, gdyż Bank – jako płatnik zryczałtowanego podatku dochodowego od osób fizycznych, naliczanego od uzyskiwanych przez klienta dochodów z odsetek od środków pieniężnych zgromadzonych na jego rachunku bankowym jest zobowiązany do pozyskiwania tych danych celem wypełnienia ciężącego na nim obowiązku płatniczego oraz sprawozdawczego⁵⁵,
- 12) wierzyciel przetwarza dane: imiona, nazwiska, adres i datę zameldowania na pobyt stały oraz stopień pokrewieństwa ze spadkodawcą ponieważ wierzyciel ma prawnie uzasadniony interes do dochodzenia spłaty zadłużenia spadkodawcy od jego następców prawnych wynikających z art. 922 § 1 kodeksu cywilnego⁵⁶,
- 13) Zarząd spółki wykorzystuje adres email byłego współnika w celu poinformowania kontrahentów o zmianie we władzach spółki⁵⁷,
- 14) podmiot świadczący usługi drogą elektroniczną udostępnia adres IP ponieważ adres IP nie zawsze może być traktowany jako dane osobowe. Gdy adres IP jest na dłuższy okres czasu lub na stałe przypisany do konkretnego urządzenia, a urządzenie to przypisane jest konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową i pozwala na jego identyfikację⁵⁸,
- 15) spółdzielnia mieszkaniowa udostępnia najemcy lokalu dane o współwłaścicielach, o wysokości miesięcznych opłat należnych za ten konkretny lokal z podziałem na części składowe w związku z przepisami dot. ubiegania się, przyznawania i obliczania podatku mieszkaniowego⁵⁹,
- 16) prezydent miasta wykorzystuje przed sądem karnym w sprawie o pomówienie dane, które zostały zebrane w innym celu (co do zasady obrona praw przed sądem przy wykorzystaniu wszelkich środków dowodowych, podlegających ocenie niezawisłego sądu, jest działaniem w prawnie uzasadnionym interesie)⁶⁰.

Wnioski końcowe

Art. 6 ust. 1 lit. f RODO dotyczy przetwarzania danych osobowych osób, bez ich zgody przez administratora posiadającego uzasadniony prawnie interes. Przy zastosowaniu ww. przepisu za każdym razem należy:

1. dążyć do minimalizacji przetwarzanych danych,
2. ocenić, czy nie istnieje inna podstawa przetwarzania,
3. sprawdzić, czy wszystkie trzy przesłanki stosowania przepisu zostały wypełnione (niezbędność, interes przedsiębiorcy, test równowagi) oraz
4. przechowywać wyniki testu w formie dokumentu.

Administrator przetwarzający dane na podstawie art. 6 ust. 1 lit. f RODO ma obowiązek przeprowadzić i udokumentować wyniki testu, poinformować osoby, której dane dotyczą o tym, jakie uzasadnione interesy są realizowane oraz umożliwić jej zgłoszenia sprzeciwu wobec przetwarzania danych osobowych.

Jędrzej Klatka

radca prawny, partner zarządzający Kancelarii Radców Prawnych Klatka i Partnerzy w Katowicach, specjalizuje się w prawie administracyjnym, a zwłaszcza prawie ochrony środowiska i prawie zamówień publicznych, ekspert Banku Światowego w dziedzinie publicznego transportu zbiorowego, ekspert Rady Europy w dziedzinie zasad etyki prawników, ekspert Polskiej Izby Ekologii w dziedzinie Prawa ochrony środowiska
J.Klatka@radca.prawny.com.pl

¹ 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 (ogólnego rozporządzenia o ochronie danych), Dz. U. UE. L. 2016. 119. 1 (dalej jako: RODO).

² Odlanicka-Poczobutt M., Szyszka-Schuppik A., Bezpieczeństwo danych osobowych w świetle nowych przepisów (RODO) – przegląd historyczny, <http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-9622869c-4642-4535-93cf-68ae406d77de> [dostęp: 22.10.2021 r.].

³ Administrator jest natomiast zobowiązany do wypełnienia m.in. obowiązków informacyjnych wobec osób, których dane przetwarza, co umożliwia im złożenie sprzeciwu.

⁴ Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679 Wersja 1.1 Przyjęta dnia 4 maja 2020 r. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pl.pdf [dostęp: 16.10.2021 r.].

⁵ D. Lubasz, W. Chomiczewski [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielań-Jomaa, Warszawa 2018, art. 6. s. 392.



- ⁶ Ibidem.
- ⁷ <https://grantthornton.pl/publikacja/prawnie-uzasadniony-interes-administratora-jako-podstawa-przetwarzania-danych-osobowych/> [dostęp: 21.10.2021 r.].
- ⁸ Zgodnie z art. 5 ust. 1 lit. c. RODO: adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
- ⁹ <https://grantthornton.pl/publikacja/prawnie-uzasadniony-interes-administratora-jako-podstawa-przetwarzania-danych-osobowych/> [dostęp: 21.10.2021 r.].
- ¹⁰ Patrz dalej rozdz. III.
- ¹¹ *W opinii Grupy Roboczej art. 29 nr 6/201417 wskazano, że prawnie uzasadniony interes administratora danych (lub osoby trzeciej) musi być wyważony względem interesów związanych z podstawowymi prawami i wolnościami osoby, której dane dotyczą.* Kinga Kowalska, Monitoring wizyjny w zakładzie pracy w kontekście ogólnego rozporządzenia o ochronie danych (RODO), 2019, MOP 2019, Nr 6, str. 316, <https://sip.legalis.pl/documentfull.seam?documentId=mjxw62zogi3damrsgydimi#tab-metrical-info> [dostęp: 25.10.2021 r.].
- ¹² <https://grantthornton.pl/publikacja/prawnie-uzasadniony-interes-administratora-jako-podstawa-przetwarzania-danych-osobowych/> [dostęp: 21.10.2021 r.].
- ¹³ Np. WSA w Warszawie w wyroku z dnia 13.04.2021 r. sygn. akt II SA/Wa 1898/20, orzekł, że umowa sprzedaży bazy danych nie jest wystarczającą przesłanką legalizującą proces przetwarzania; *odmienne stanowisko oznaczałoby możliwość swobodnego następczego wykreowania podstawy prawnej dla procesu przetwarzania; tymczasem zachodziłby brak podstawy pierwotnej w przepisach o ochronie danych osobowych; takie działanie narusza interesy Wnioskodawcy; nie może się on bowiem spodziewać przetwarzania; w konsekwencji ograniczona to możliwość realizacji jego praw – w tym m.in. podjęcia czynności zmierzających do wstrzymania przetwarzania przez administratora; w tych okolicznościach interesy Wnioskodawcy są nadrzędne wobec interesu administratora; w związku z tym – pozyskując i przetwarzając dane – Spółka narusza art. 6 ust. 1 RODO.* <https://orzeczenia.nsa.gov.pl/doc/6F4D63ACA8> [dostęp: 24.10.2021 r.].
- ¹⁴ *Chodzi przykładowo o takie działania, jak: prowadzenie analityki korzystania z serwisu internetowego, przetwarzanie danych pracowników w celu organizacji wyjazdów służbowych lub szkoleń, udostępnianie przez agencję rekrutacyjną przesłanych aplikacji potencjalnym pracodawcom, przetwarzanie danych pracowników kontrahenta w celach kontaktowych czy śledzenie floty samochodów z wykorzystaniem technologii GPS.* <https://grantthornton.pl/publikacja/prawnie-uzasadniony-interes-administratora-jako-podstawa-przetwarzania-danych-osobowych/> [dostęp: 21.10.2021 r.].
- ¹⁵ *Obejmuje dane ujawniające: pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak i dane dotyczące zdrowia i życia seksualnego. Prawodawca wprowadził przy tym rozbudowany katalog odstępstw od zakazu (art. 9 ust. 2), w szczególności związanych z realizacją uzasadnionego interesu prawnego administratora danych (np. przetwarzanie danych w ramach stosunku pracy), ochrony żywotnych interesów podmiotu danych czy świadczenia usług medycznych.*
- ¹⁶ M. Rojszczak, 4.5.1. Podstawowe zasady przetwarzania [w:] Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji, Warszawa 2019, <https://sip.lex.pl/#/monograph/369454046/383364/rojszczak-marcin-ochrona-prywatnosci-w-cyberprzestrzeni-z-uwzględnieniem-zagrozen-wynikajacych-z-...?cm=URELATIONS> [dostęp: 24.10.2021 r.].
- ¹⁷ <https://prawo.gazetaprawna.pl/artykuly/1268725-prawnie-uzasadniony-interes-jako-podstawa-przetwarzania-danych.html> [dostęp: 19.10.2021 r.].
- ¹⁸ P. Fajgielski, Komentarz do art. 6 (w:) red. P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych.* Komentarz. Wolters Kluwer Polska, 2018.
- ¹⁹ <https://grantthornton.pl/publikacja/prawnie-uzasadniony-interes-administratora-jako-podstawa-przetwarzania-danych-osobowych/> [dostęp: 21.10.2021 r.].
- ²⁰ D. Lubasz, W. Chomiczewski [w:] RODO. Ogólne rozporządzenie..., str. 393.
- ²¹ D. Lubasz, W. Chomiczewski [w:] RODO. Ogólne rozporządzenie..., str. 399.
- ²² D. Lubasz, W. Chomiczewski [w:] RODO. Ogólne rozporządzenie..., str. 397.
- ²³ <https://capitallegal.pl/rodo-a-zgody-marketingowe/> [dostęp: 22.10.2021 r.].
- ²⁴ m.in. art. 172 ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t. j. Dz. U. z 2021 poz. 576) *Zakazane jest używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę.*
- ²⁵ m.in. art. 10 ust. 1 i 2 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t. j. Dz. U. 2020 poz. 344) *Zakazane jest przysyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. Informację handlową uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na otrzymywanie takiej informacji, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny.*
- ²⁶ P. Litwiński (red.), Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Legalis 2018. J. Glumińska-Pawlic, B. Przywora, A. Słysz (red.), *Identyfikacja barier prawnych w prowadzeniu działalności gospodarczej.* Wybrane zagadnienia, Warszawa 2020 Rozdz. XX RODO jako bariera w prowadzeniu działalności. <https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi3damrshydcmq#tab-metrical-info>
- ²⁷ Wyrok NSA z dnia 6.06.2005 r. sygn. akt I OPS 2/05 <https://orzeczenia.nsa.gov.pl/doc/B34A87CD32>.
- ²⁸ Wyrok NSA z 19.05.2011 r. sygn. akt I OSK 1079/10.
- ²⁹ NSA w wyroku z 21.08.2013 r. sygn. akt I OSK 1666/12 orzekł, że Nieuzasadnione niczym jest twierdzenie, że ktoś wypowiadający się anonimowo, w sposób naruszający dobra innych podmiotów ma podlegać szczególnej ochronie i to jego dane osobowe są dobrem, które ustawodawca miał zamiar chronić w pierwszej kolejności". Oceny w tym zakresie dokonuje bowiem właściwy sąd, a Skarżący ma prawo korzystać z ochrony przed sądem, o ile czuje się znieważony.
- ³⁰ Jeżeli skarżący wniósł prywatny akt oskarżenia w sprawie o przestępstwo z art. 212 k.k. Uzasadnione jest zatem uzyskanie numeru IP komputera użytkownika posługującego się nickiem na portalu internetowym, ponieważ podstawą jest ochrona prawa Skarżącego, w tym szczególnie jego dobrego imienia, której zamierzano dochodzić przed sądem. Wyrok WSA w Warszawie z 3.02.2010 r. sygn. akt II SA/Wa 1598/09.
- ³¹ K. Sztobryn, A. Urbanek, Dochodzenie odszkodowania za korzystanie z torrentów. Omówienie wyroku TS z dnia 17 czerwca 2021 r., C-597/19 (CNIL), LEX/el. 2021. <https://sip.lex.pl/#/publication/151389357/sztobryn-karolina-urbanek-anna-dochodzenie-odszkodowania-za-korzystanie-z-torrentow-omowienie...?cm=URELATIONS> [dostęp: 24.10.2021 r.].
- ³² D. Lubasz, W. Chomiczewski [w:] RODO. Ogólne rozporządzenie..., str. 396.
- ³³ Arkadiusz Sobczyk Processing employee data under art. 6 paragraph 1 point f) GDPR (Przetwarzanie danych pracowniczych na podstawie art. 6 ust. 1 lit. f RODO), Praca i zabezpieczenie społeczne 12/2018, https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/70259/sobczyk_processing_employee_data_under_art_6_paragraph_1_point_6_gdpr_2018.pdf?sequence=2&isAllowed=y [dostęp: 25.10.2021 r.].
- ³⁴ <https://sip.legalis.pl/document-full.seam?documentId=mjuwelrsgydygmryhe3to> [dostęp: 25.10.2021 r.].
- ³⁵ Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2020 poz. 1320).
- ³⁶ prof. UAM dr hab. Anna Musiała, Władza publiczna „rozproszona” w prawie pracy – dylematów systemowych w prawie ciąg dalszy, 2020, MOPR 2020, Nr 8, str. 9. <https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi3damrwwgq3temq#tab-metrical-info> [dostęp: 25.10.2021 r.].
- ³⁷ Wyrok WSA w Warszawie z 3.02.2010 r. sygn. akt II SA/Wa 1598/09 <https://orzeczenia.nsa.gov.pl/doc/AD6FF02867>.
- ³⁸ wyrok Sądu Najwyższego z 19.11.2003 r. sygn. akt I PK 590/02 <http://www.sn.pl/sites/orzecznictwo/orzeczenia/1%20pk%20590-02-1.pdf>.
- ³⁹ https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/70259/sobczyk_processing_employee_data_under_art_6_paragraph_1_point_6_gdpr_2018.pdf?sequence=2&isAllowed=y [dostęp: 25.10.2021 r.].
- ⁴⁰ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 20.11.2019 r. sygn. ZKE.440.54.2019, Pismo z dnia 20.11.2019 r., <https://uodo.gov.pl/decyzje/ZKE.440.54.2019>
- ⁴¹ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 27 maja 2020 r. sygn. ZKE.440.66.2019, <https://uodo.gov.pl/decyzje/ZKE.440.66.2019>
- ⁴² Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2020 poz. 1740).
- ⁴³ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 30 kwietnia 2020 r. sygn. ZKE.440.5.2019, <https://uodo.gov.pl/decyzje/ZKE.440.5.2019>
- ⁴⁴ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 23.04.2020 r. sygn. ZKE.440.22.2019, <https://uodo.gov.pl/decyzje/ZKE.440.22.2019>
- ⁴⁵ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 24.12.2019 r. sygn. ZKE.440.57.2019, <https://uodo.gov.pl/decyzje/ZKE.440.57.2019>
- ⁴⁶ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 23.12.2019 r. sygn. ZKE.440.70.2019, <https://uodo.gov.pl/decyzje/ZKE.440.70.2019>
- ⁴⁷ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 23.12.2019 r. sygn. ZKE.440.17.2019, <https://uodo.gov.pl/decyzje/ZKE.440.17.2019>
- ⁴⁸ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 6.11.2019 r. sygn. ZKE.440.44.2019, <https://uodo.gov.pl/decyzje/ZKE.440.44.2019>
- ⁴⁹ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 18.10.2019 r. sygn. ZSPR.440.998.2018, <https://uodo.gov.pl/decyzje/ZSPR.440.998.2018>
- ⁵⁰ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 25.04.2019 r., sygn. ZSPU.440.469.2018, <https://uodo.gov.pl/decyzje/ZSPU.440.469.2018>
- ⁵¹ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 9.08.2019 r., sygn. ZSOŚS.440.157.2018, <https://uodo.gov.pl/decyzje/ZSO%20C5%9AS.440.157.2018>
- ⁵² Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 5.06.2020 r. sygn. ZKE.440.52.2019, <https://uodo.gov.pl/decyzje/ZKE.440.52.2019>
- ⁵³ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 20.12.2018 r. sygn. ZSPR.440.370.2018, <https://uodo.gov.pl/decyzje/ZSPR.440.370.2018>
- ⁵⁴ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 19.02.2019 r. sygn. ZSZS.440.658.2018, <https://uodo.gov.pl/decyzje/ZSZS.440.658.2018>
- ⁵⁵ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 21.03.2019 r. sygn. ZSPR.440.195.2019, <https://uodo.gov.pl/decyzje/ZSPR.440.195.2019>
- ⁵⁶ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 11 kwietnia 2019 r. sygn. ZSPU.440.840.2018, <https://uodo.gov.pl/decyzje/ZSPU.440.840.2018>
- ⁵⁷ Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 15.05.2019 r. sygn. ZSPU.440.423.2018, <https://uodo.gov.pl/decyzje/ZSPU.440.423.2018>
- ⁵⁸ Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za złamanie inteligencję (2020/2014(INL)).
- ⁵⁹ Projekt rozporządzenia stanowi załącznik do wspomnianej Rezolucji Parlamentu Europejskiego; pełny tytuł projektu: *Rozporządzenie Parlamentu Europejskiego i Rady w sprawie odpowiedzialności za działanie systemów sztucznej inteligencji.*
- ⁶⁰ Projekt z dnia 21 kwietnia 2021 r., COM(2021) 206 final, 2021/0106(COD); pełny tytuł projektu: *Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie Sztucznej Inteligencji) i zmieniające niektóre akty ustawodawcze Unii.*



Outsourcing pracowników

Na co powinien zwrócić uwagę pracodawca

Jakub Kowal

W miarę rozwoju przedsiębiorstwa, a w konsekwencji zwiększania zatrudnienia, pracodawcy stają przed różnymi możliwościami optymalizacji kosztów prowadzonej działalności. Jedną z takich możliwości jest wydzielenie procesów realizowanych wewnątrz organizacji na zewnątrz przedsiębiorstwa, czyli tzw. outsourcing. Stosowanie outsourcingu w zakresie kadr i płac, księgowości czy IT może przyczynić się nie tylko do ograniczania kosztów, ale także do poprawy jakości realizowanych procesów przez powierzenie ich podmiotom doświadczonym i wykwalifikowanym w danej dziedzinie. Niemniej, outsourcing wiąże się również z ryzykami prawnymi dla pracodawcy. Ryzyka te, przy zastosowaniu odpowiednich mechanizmów prawnych, mogą być jednak zminimalizowane.

W niniejszym artykule autor porusza problematykę outsourcingu pracowników z perspektywy prawa pracy. Wskazuje na cechy charakterystyczne outsourcingu w kontekście innych konstrukcji opierających się na korzystaniu przez przedsiębiorcę z pracy pracowników zewnętrznych. Określa również prawne konsekwencje stosowania outsourcingu na gruncie prawa pracy, w tym ryzyka prawne dla pracodawców. Wskazuje także, jakie praktyczne działania może podjąć pracodawca, żeby zminimalizować te ryzyka.

Czym jest outsourcing?

Aby poprawnie zidentyfikować ryzyka prawne związane z outsourcingiem, należy w pierwszej kolejności ustalić znaczenie outsourcingu z prawnego punktu widzenia. Przepisy prawa, w tym prawa pracy, nie zawierają definicji legalnej outsourcingu. Zgodnie z orzecznictwem Sądu Najwyższego, outsourcing można zdefiniować jako przedsięwzięcie polegające na wydzieleniu ze struktury

organizacyjnej przedsiębiorstwa macierzystego realizowanych przez nie funkcji i przekazanie ich do realizacji innym podmiotom gospodarczym. Jest to jednak definicja outsourcingu w ujęciu ekonomicznym, szerszym od ujęcia prawnego. Z perspektywy prawa pracy taki outsourcing staje się prawnie relevantny dopiero w momencie, w którym wiąże się on z korzystaniem z pracowników podmiotu zewnętrznego, któremu przekazano do realizacji określone funkcje. Dopiero wtedy można mówić o tzw. outsourcingu pracowniczym. Zjawisko to wywołuje skutki m.in. na gruncie prawa pracy oraz ubezpieczeń społecznych, szerzej opisane w dalszej części artykułu.

Pojęcie outsourcingu pracowniczego jest czasami stosowane zamiennie z takimi pojęciami jak *bodyleasing*, leasing pracowników czy praca tymczasowa. Rzeczywiście, pojęcia te są częściowo zbliżone – wszystkich bowiem używa się do opisanego zjawiska sprowadzające się do korzystania przez pracodawcę z pracowników lub współpracowników podmiotu zewnętrznego. W istocie pomiędzy tymi pojęciami istnieją jednak znaczące różnice.

Outsourcing a praca tymczasowa

Stosunkowo łatwe jest odróżnienie outsourcing'u od pracy tymczasowej. Ta ostatnia została bowiem wprost zdefiniowana w ustawie z dnia 9 lipca 2003 r. o zatrudnianiu pracowników tymczasowych (dalej: „**UPT**”). Oznacza ona wykonywanie przez pracownika zatrudnionego przez agencję pracy tymczasowej na rzecz tzw. pracodawcy użytkownika, zadań:

- 1) o charakterze sezonowym, okresowym, doraźnym lub
- 2) których terminowe wykonanie przez pracowników zatrudnionych przez

pracodawcę użytkownika nie byłoby możliwe, lub

- 3) których wykonanie należy do obowiązków nieobecnego pracownika zatrudnionego przez pracodawcę użytkownika.

Zgodnie z ugruntowanym orzecznictwem sądów, cechą odróżniającą outsourcing pracowniczy od pracy tymczasowej jest brak bezpośredniego i stałego podporządkowania (zarówno prawnego i faktycznego) wykonawców w stosunku do podmiotu korzystającego z ich pracy (insourcer'a). Podporządkowanie takie występuje natomiast w przypadku pracy tymczasowej, gdzie pracownicy tymczasowi świadczą pracę na rzecz i pod kierownictwem pracodawcy użytkownika.

Outsourcing a *bodyleasing* lub leasing pracowniczy

Nieco bardziej problematyczne jest ustalenie granic pomiędzy outsourcingiem oraz *bodyleasingiem*/leasingiem pracowników. Problemy te wynikają z tego faktu, iż dwa ostatnie pojęcia – w przeciwieństwie do pracy tymczasowej – nie doczekały się ani definicji legalnej, ani nie były definiowane przez sądy. *Bodyleasing* to pojęcie rozpowszechnione przede wszystkim w branży IT, oznaczające krótkoterminowy „wynajem” specjalistów w danej dziedzinie do realizacji konkretnego projektu (np. wdrożenia systemu informatycznego u klienta przedsiębiorcy, który korzysta z „wynajmowanych” specjalistów). W przypadku outsourcingu świadczenie insourcer'a (podmiotu, któremu zadania są przekazywane do wykonywania), polega na realizacji danego procesu na rzecz insourcer'a w sposób kompleksowy przy pomocy zatrudnionego przez siebie personelu. *Bodyleasing* zakłada natomiast, że zasadniczo realizacja

funkcji lub procesów pozostaje w gestii pracodawcy, który jedynie tymczasowo (krótkoterminowo) korzysta z „siły roboczej” dostarczanej przez podmiot zewnętrzny w celu realizacji konkretnych zadań (często w charakterze wsparcia zatrudnianego przez siebie zespołu).

W tym zakresie do *bodyleasingu* podobne jest pojęcie leasingu pracowniczego, szerzej rozpowszechnione w sektorze produkcyjnym. Granice między tymi pojęciami są płynne, a w niektórych przypadkach zakres ich zastosowania może się częściowo pokrywać, co potwierdza fakt, iż nawet sądy stosują je niekiedy zamiennie. Z perspektywy pracodawców najistotniejszy jest jednak fakt, że orzecznictwo sądowe jednoznacznie uznaje dopuszczalność stosowania outsourcingu pracowniczego przez przedsiębiorców.

Umowy outsourcingu w praktyce

Zasadniczo, outsourcing może być realizowany zarówno na podstawie „typowych” umów scharakteryzowanych w Kodeksie cywilnym (tzw. umów nazwanych), np. umowy o świadczenie usług czy umowy o dzieło, jak i tzw. umów nienazwanych, zawieranych w ramach ogólnej zasady swobody kontraktowania. Decydująca będzie tutaj treść umowy, czyli w praktyce zawarcie w niej

elementów charakterystycznych dla outsourcingu pracowniczego. Umowa outsourcingu pracowniczego powinna wyraźnie przewidywać, iż insourcer nie sprawuje kontroli nad osobami, które świadczą na jego rzecz usługi. Ten element pozwoli odróżnić outsourcing od pracy tymczasowej czy *bodyleasingu* (leasingu pracowniczego). Rozróżnienie takie – zarówno na gruncie postanowień umowy, jak i faktycznego sposobu działania stron – jest konieczne, aby outsourcer i insourcer nie zostali uznani za funkcjonujących w reżimie UPT. Konsekwencją takiej kwalifikacji byłoby bowiem objęcie zarówno outsourcer’a, jak i insourcer’a restrykcyjnymi ograniczeniami przewidzianymi w tej ustawie (np. obowiązkiem prowadzenia ewidencji pracowników tymczasowych czy limitami czasowymi co do możliwości korzystania z pracy danego pracownika). Zamiast sprawowania kontroli nad pracownikami, nadzór insourcer’a powinien sprowadzać się do weryfikacji jakości świadczonych przez outsourcer’a usług. Przykładowo, sklep internetowy (insourcer), który outsource’uje obsługę procesu reklamacji produktów, zamiast weryfikować efektywność konkretnych pracowników, powinien ustalić ogólne wskaźniki, za pomocą których zmierzy jakość świadczonych przez outsourcer’a usług (np. czas reakcji na reklamację, liczbę zamkniętych procesów reklamacyjnych w danym okresie lub poziom satysfakcji klienta z obsługi reklamacyjnej) i przy ich pomocy dokonywać oceny działań outsourcer’a.

Prawidłowo skonstruowana umowa outsourcing’u powinna zatem określać przede wszystkim:

- 1) jakie procesy/funkcje ma realizować outsourcer na rzecz insourcera,
- 2) czy powierzone procesy / funkcje outsourcer realizuje za pomocą własnych pracowników, czy za pomocą pracowników insourcera,
- 3) przewidywać sposób weryfikacji jakości usług świadczonych przez outsourcera.

Outsourcing a przejście zakładu pracy

Trzeba też zauważyć, iż zdaniem Sądu Najwyższego, jeżeli konsekwencją umowy outsourcingu ma być przejście zakładu pracy na outsourcer’a, należy dochować formy pisemnej umowy. Przejście zakładu pracy jest jednym z najistotniejszych potencjalnych skutków prawnych zawarcia umowy outsourcingu pracowniczego. Mechanizm przejścia zakładu pracy ma swoje źródło w postanowieniach art. 231 Kodeksu pracy, zgodnie z którym w razie przejścia zakładu pracy lub jego części na innego pracodawcę, taki pracodawca staje się z mocy prawa stroną w dotychczasowych stosunkach pracy. W przypadku przejścia (części) zakładu pracy z mocy samego prawa, tj. bez konieczności zawierania w tym zakresie dodatkowych porozumień z pracownikami, dochodzi do zmiany pracodawcy



z insourcer'a na outsourcer'a z zachowaniem ciągłości zatrudnienia pracownika (np. w zakresie uprawnień wynikających ze stażu pracy, takich jak długość okresu wypowiedzenia).

Zgodnie z orzecznictwem sądowym omawiana konstrukcja znajduje zastosowanie nie tylko w przypadku przeniesienia z jednego przedsiębiorstwa na drugie materialnych składników biznesu, takich jak nieruchomości, maszyny, urządzenia czy flota pojazdów. Będzie miała ona zastosowanie również w sytuacji przejścia zadań, których wykonywanie stanowi treść stosunku pracy pracowników podlegających przejściu. Przejmowanie zadań (funkcji) jest nieodłącznym elementem outsourcing'u. W efekcie konsekwencją zawarcia umowy outsourcingu pracowniczego może być przejście zakładu pracy lub jego części. Warto zaznaczyć, iż przejście pracowników w trybie art. 231 Kodeksu pracy następuje niezależnie od woli pracodawców – stron umowy outsourcingu. W rezultacie w przypadku zawarcia umowy outsourcing'u części działalności pracodawcy, pracownicy związani z wydzielaną częścią działalności insourcer'a mogą stać się z mocy prawa pracownikami outsourcer'a nawet wtedy, jeżeli strony nie będą miały intencji wywołania takiego skutku prawnego.

Z tego względu istotne jest uprzednie dokonanie przez strony transakcji oceny, czy w konkretnej sytuacji dojdzie do przejścia zakładu pracy lub jego części. Ocena taka może w praktyce nastrożać trudności. Przy jej dokonywaniu należy bowiem uwzględnić szereg złożonych okoliczności. Sądy stoją na stanowisku, iż konieczne jest wzięcie pod uwagę w szczególności:

- 1) czy doszło do przejścia składników majątkowych (materialnych i niematerialnych) przedsiębiorstwa,
- 2) czy „nowy” pracodawca przejmuje klientów poprzedniego pracodawcy,
- 3) czy i w jakim stopniu pracownicy, którzy mają podlegać przejściu, są związani z przyjmowanymi procesami, zadaniami lub funkcjami,
- 4) czy i w jakim stopniu działalność „nowego” i poprzedniego pracodawcy jest podobna,
- 5) który podmiot sprawuje faktyczne kierownictwo nad przejętymi pracownikami.



Trzeba jednocześnie podkreślić, że rodzaj i waga czynników kluczowych dla oceny czy doszło do przejścia zakładu pracy, są w dużym stopniu zależne od profilu działalności obu pracodawców oraz charakteru transakcji.

Przykładowo, inne czynniki będą brane pod uwagę w ocenie, czy wydzierżawienie linii produkcyjnej przedsiębiorstwa produkującego opakowania spowoduje przejście pracowników zatrudnionych przy produkcji, a inne dla ustalenia, czy doszło do przejścia części zakładu pracy w wyniku wydzielenia zadań realizowanych przez zespół obsługujący rozliczenia wynagrodzeń w dużej korporacji do nowoutworzonego centrum usług wspólnych.

Każdorazowo zatem w przypadku outsourcingu procesów na zewnątrz organizacji i związanego z tym potencjalnego transferu pracowników, zarówno outsourcer, jak i insourcer powinni dokonać kompleksowej analizy wszystkich okoliczności towarzyszących transakcji aby ustalić, czy konsekwencją transakcji będzie przejście zakładu pracy lub jego części.

Jeśli taka analiza doprowadzi do wniosku, że doszło do przejścia pracowników w drodze przejścia zakładu pracy lub jego części, to jakie będą tego praktyczne skutki? Oprócz podstawowej, wspomnianej już wyżej konsekwencji w postaci zmiany pracodawcy przyjmowanego pracownika z zachowaniem ciągłości zatrudnienia, należy wskazać przede wszystkim na obowiązki informacyjne obu pracodawców. Zgodnie z art. 231 Kodeksu pracy dotychczasowy i nowy pracodawca zobowiązani są do poinformowania pracowników lub działających u nich organizacji związkowych o przewidywanym terminie przejścia zakładu pracy lub jego części na innego pracodawcę, jego przyczynach, prawnych, ekonomicznych oraz socjalnych skutkach dla pracowników, a także zamierzonych działaniach dotyczących warunków zatrudnienia pracowników, w szczególności warunków pracy, płacy i przekwalifikowania.

Przekazanie informacji powinno nastąpić co najmniej na 30 dni przed przewidywanym terminem przejścia zakładu pracy lub jego części na innego pracodawcę. W praktyce przejście

zakładu pracy nastąpi w momencie, w którym nowy pracodawca – outsourcer – obejmie faktyczne władztwo nad przejętą częścią zakładu pracy. Ten moment może być w praktyce dość trudny do precyzyjnego wskazania. Jeżeli więc dynamika transakcji outsourcing'u unieemożliwia ustalenie konkretnej daty, w której outsourcer przejmie realizację powierzonych mu procesów, dobrą praktyką jest przekazanie pracownikom wymaganych prawem informacji z odpowiednim wyprzedzeniem.

Do innych istotnych konsekwencji prawnych przejścia zakładu pracy w kontekście outsourcing'u trzeba zaliczyć również uprawnienie przejętych pracowników do rozwiązania stosunku pracy za 7-dniowym uprzedzeniem w terminie 2 miesięcy od przejścia zakładu pracy. Nie jest możliwe wyłączenie skorzystania przez pracownika z tego uprawnienia. Generuje ono zatem ryzyko odpływu kluczowych dla organizacji osób praktycznie z dnia na dzień, co znacząco utrudnia zarządzanie zmianą zwłaszcza przy złożonych procesach outsourcing'owych. Szczególne znaczenie ma to w przypadkach, w których transakcja outsourcing'u przewiduje wydzielenie zadań i funkcji realizowanych przez wysoko wykwalifikowanych specjalistów, których pozyskanie oraz wyszkolenie jest czasochłonne i kosztowne. Pracodawca nie jest jednak całkowicie pozbawiony możliwości ochrony przed odpływem kluczowego personelu. Formą zabezpieczenia przed takimi sytuacjami jest zaproponowanie pracownikom premii retencyjnych, dodatkowego wynagrodzenia, którego przyznanie jest uzależnione od pozostania przez pracownika w zatrudnieniu przez określony czas po transakcji, np. wskazane wyżej 2 miesięcy od dnia przejścia zakładu pracy.

Kolejną praktyczną konsekwencją przejścia zakładu pracy lub jego części na innego pracodawcę jest zakaz traktowania tego zdarzenia (przejścia) jako przyczyny uzasadniającej wypowiedzenie przez pracodawcę stosunku pracy. Sam outsourcing nie może więc posłużyć jako uzasadnienie dla restrukturyzacji zatrudnienia przez outsourcer'a. Takim uzasadnieniem mogą być jednak zmiany organizacyjne będące konsekwencją outsourcing'u. Przykładowo, przeniesienie obsługi procesów rozliczeń kosztów

w grupie spółek do dedykowanego centrum usług wspólnych nie powinno stanowić podstawy do rozwiązania stosunków pracy z osobami zatrudnionymi w dziale odpowiedzialnym za te rozliczenia. Przeprowadzana przez outsourcer'a optymalizacja procesów i związana z tym likwidacja stanowisk pracy w ramach działu rozliczeń, może jednak takie działania uzasadniać.

Dla outsourcer'a przejmującego pracowników skutkiem przejścia zakładu pracy lub jego części jest również konieczność dokonania szeregu czynności o charakterze organizacyjnym, takich jak zgłoszenie przejścia pracowników do Zakładu Ubezpieczeń Społecznych, włączenie ich do PPK czy odebranie akt osobowych od insourcer'a. W zależności od okoliczności, niezbędne może być także przekazanie outsourcer'owi środków z zakładowego funduszu świadczeń socjalnych insourcer'a.

Porozumienie trójstronne jako sposób outsource'owania pracowników

Nie w każdym jednak przypadku outsourcer i insourcer staną przed koniecznością spełnienia wymogów związanych z przejściem zakładu pracy. Będzie tak w sytuacjach, w których transakcja outsourcingu nie wywoła skutku w postaci przejścia zakładu pracy. Aby w takich przypadkach umożliwić skuteczny transfer pracownika i w konsekwencji zapewnić outsourcer'owi zasoby kadrowe niezbędne do realizacji przejętych procesów, strony mogą się posłużyć konstrukcją porozumienia trójstronnego (pomiędzy outsourcer'em, insourcer'em i pracownikiem). Zawarcie takiego porozumienia nie jest co prawda regulowane wprost przez przepisy prawa pracy, tym niemniej należy je uznać za dopuszczalne, jeżeli nie jest ono niekorzystne dla pracownika.

Z prawnego punktu widzenia zawarcie porozumienia trójstronnego oznacza rozwiązanie stosunku pracy z insourcer'em za porozumieniem stron oraz zawarcie nowego stosunku pracy z outsourcer'em na dotychczasowych

warunkach (chyba, że co innego wynika z treści samego porozumienia). Aby uniknąć zarzutu o pogorszenie sytuacji prawnej pracownika i w konsekwencji narażenia się na nieważność porozumienia, dotychczasowy i nowy pracodawca powinni ustalić w nim zachowanie przez pracownika uprawnień wynikających ze stażu pracy u dotychczasowego pracodawcy, takich jak okres wypowiedzenia czy liczba dni urlopu przysługującego pracownikowi. Jeżeli porozumienie ma spowodować także przeniesienie na outsourcer'a praw i obowiązków wynikających z dodatkowych umów zawartych z pracownikiem, takich jak umowa o zakazie konkurencji, należy ten skutek wyraźnie przewidzieć w jego treści.

Podsumowanie

Podsumowując, outsourcing pracowników jest dopuszczalny prawnie. Może on jednak nastroczać trudności dla pracodawców przede wszystkim na etapie ustalania, czy dokonanie określonej czynności prawnej (zawarcie umowy lub przeprowadzenie transakcji) w ogóle będzie miało charakter outsourcing'u pracowniczego, czy też będzie stanowiło *bodyleasing* lub powierzenie pracy tymczasowej. W tym zakresie kluczowe jest właściwe sformułowanie postanowień umowy. Jeżeli w danym przypadku taka czynność stanowi outsourcing, outsourcer i insourcer powinni przeanalizować możliwość wystąpienia skutku w postaci przejścia zakładu pracy lub jego części. W sytuacji, w której dojdą do wniosku, że taki skutek wystąpi, konieczne będzie podjęcie działań w celu spełnienia wymogów wynikających z przepisów dotyczących przejścia zakładu pracy. Jeżeli natomiast do przejścia zakładu pracy lub jego części nie dojdzie, a zamiarem stron będzie transfer pracowników na outsourcer'a, strony powinny zawrzeć odpowiednie porozumienia trójstronne, na podstawie których dojdzie do „przekazania” pracownika pomiędzy pracodawcami.

Jakub Kowal

radca prawny, Senior Associate
w Kancelarii Maruta Wachta

Odpowiedzialność za szkody wynikające z działania systemów sztucznej inteligencji

Proponowane rozwiązania legislacyjne

Łukasz Wieczorek

Uczestnicy konferencji w Dartmouth w 1956 r. prawdopodobnie nie zdawali sobie sprawy, jaką karierę zrobi ukułte wtedy pojęcie sztucznej inteligencji. Po upływie 65 lat na dobre wrosła ona w krajobraz współczesnego świata doby cyfrowej. Postępujący rozwój techniczny, wzrost mocy obliczeniowej komputerów, możliwość zapisywania i analizowania ogromnych zasobów danych z wykorzystaniem chmury obliczeniowej stworzyło warunki do tworzenia wysoce złożonego oprogramowania, pozwalającego generować określone sugestie wyników czy rekomendacje działań.

Sztuczna inteligencja pojawia się zawsze w kontekście określonego oprogramowania. Mówi się więc często o systemach sztucznej inteligencji (SI), które są „wbudowane” w określone produkty czy usługi. Rosnący stopień złożoności i skomplikowania systemów sztucznej inteligencji zaczął jednocześnie uwytkuć problemy immanentne w nich tkwiące, a polegające przede wszystkim na trudności w przesłedzeniu procesu decyzyjnego danego systemu SI. Produkt lub usługa oparta o system SI może więc nie działać „prawidłowo”, a w skrajnym wypadku może wręcz wyrządzić szkodę.

Ta konstatacja stała się przyczynkiem do dyskusji na temat prawnego uregulowania sztucznej inteligencji. Jednym z aspektów regulacji problematyki sztucznej inteligencji jest kwestia odpowiedzialności za szkody, które zostały wyrządzone przez sztuczna inteligencję, a precyzyjnie – przez produkty lub usługi inkorporujące systemy SI. Konkretną propozycję takiej regulacji przedstawił Parlament Europejski w ramach swojej rezolucji z 2020 r.¹ Zaproponowane przez Parlament Europejski rozporządzenie w sprawie odpowiedzialności za działanie systemów sztucznej inteligencji² (dalej: „Projektowane Rozporządzenie”)

nie stało się jeszcze obowiązującym prawem, lecz stanowi ciekawy materiał dla poznania i zrozumienia podejścia Unii Europejskiej do kwestii odpowiedzialności za sztuczna inteligencję. W ramach niniejszego artykułu przeanalizowany zostanie projekt ww. rozporządzenia.

Geneza regulacji

UE już od kilku lat podejmuje problematykę regulacji sztucznej inteligencji. Rezolucja Parlamentu Europejskiego i Projektowane Rozporządzenie nie są jedynymi propozycjami ustawodawczymi dotyczącymi sztucznej inteligencji, jakie ujrzały światło dzienne w ostatnim czasie. W szczególności warto podkreślić, że w kwietniu 2021 r. Komisja Europejska opublikowała pierwszy na świecie, tak kompleksowy projekt aktu prawnego dotyczący wprowadzania do obrotu systemów sztucznej inteligencji (tzw. Akt w sprawie Sztucznej Inteligencji)³.

Choć Projektowane Rozporządzenie i Akt w sprawie Sztucznej Inteligencji nie zawsze pozostają względem siebie spójne, we wszystkich ww. dokumentach UE konsekwentnie prezentuje podejście do sztucznej inteligencji oparte na humanocentryzmie. Z jednej strony jest zatem człowiek (użytkownik), który korzysta z możliwości, jakie oferują systemy SI. Człowiek jest również pierwotnym twórcą systemów SI – projektuje je, rozwija, utrzymuje, itd. Jednocześnie systemy SI wkomponowane w określone produkty czy usługi stwarzają ryzyka i zagrożenia dla użytkowników – dla ich praw i wolności, np. dla prywatności, ale też mogą godzić w życie, zdrowie czy majątek. Humanocentryczne podejście UE ma na celu zadbanie, by obywatele UE posiadali adekwatną ochronę w kontekście korzystania z produktów i usług opartych na sztucznej inteligencji, na wzór chociażby regulacji

dotyczących obrotu produktami niebezpiecznymi.

Przyjęcie uregulowań dotyczących różnych aspektów korzystania z rozwiązań opartych na sztucznej inteligencji wynika z przekonania, że regulacja przyczyni się do podniesienia standardów produktów i usług bazujących na sztucznej inteligencji oraz zapewni ochronę praw i wolności obywateli UE. Można ponadto wyrazić opinię, że odważna postawa UE w zakresie regulacji dotyczących systemów SI ma również inspirować inne państwa świata do podjęcia trudu unormowania przedmiotowej problematyki.

Specyfika systemów SI

Podejście do regulacji sztucznej inteligencji jest zakotwiczone w ryzykach i zagrożeniach płynących z korzystania z produktów i usług bazujących na sztucznej inteligencji. Te ryzyka wynikają ze specyfiki systemów SI. W motywach uzasadniających potrzebę regulacji odpowiedzialności za systemy SI Parlament Europejski wskazuje, że systemy SI są złożone, nieprzejrzyste („czarna skrzynka” – trudność lub niemożność przesłedzenia procesu decyzyjnego), coraz bardziej autonomiczne ze względu na postępujące uczenie się maszyn (*deep machine learning*), a także podatne na zagrożenia (np. naruszenia cyberbezpieczeństwa).

Ponadto wiele podmiotów (przedsiębiorców) jest zwykle zaangażowanych lub w inny sposób ingeruje w cykl życia systemów SI. Dany system SI może być tylko częścią większego systemu informatycznego, różne podmioty mogą być dostawcami komponentów czy funkcjonalności składających się na gotowy produkt. W konsekwencji rozmywa to odpowiedzialność poszczególnych podmiotów za negatywne skutki działania systemu SI.

Do argumentacji zawartej w Rezolucji Parlamentu Europejskiego można jeszcze dodać, że na systemach SI ciąży ryzyko tzw. przechyłu algorytmicznego (*algorithmic bias*), czyli swego rodzaju stronniczości systemu SI w zwracanych wynikach czy rekomendacjach działań. Skutkiem przechyłu algorytmicznego jest zwykle dyskryminacja (ze względu na określone cechy) i w efekcie nierzetelność lub nieprawidłowość wyniku. Ze względu na często towarzyszącą systemom SI nieprzejrzystość, zwykle trudno ustalić co konkretnie było przyczyną wygenerowania dyskryminującego wyniku.

W ramach Projektowanego Rozporządzenia Parlament Europejski nie dąży do rozwiązania wspomnianych wyżej problemów. Istotą projektu jest stworzenie ram prawnych dla obywateli UE (użytkowników) dotkniętych negatywnymi skutkami działania systemów SI. Mając na uwadze omówioną wyżej specyfikę systemów SI, w tym w szczególności brak przejrzystości systemów SI, z perspektywy osoby poszkodowanej w praktyce bardzo trudne może być ustalenie:

- kto kontroluje ryzyko związane z korzystaniem z danego systemu SI,
- który kod (źródłowy) lub które dane wejściowe wywołały szkodę,
- czy istnieje związek przyczynowy między szkodą a powodującym ją zachowaniem.

Dodatkowo, ustalenie tych elementów może być bardzo kosztowne.

W rezultacie osoba, która doznała szkody w następstwie korzystania z produktu lub usługi inkorporującej system SI, mogłaby nigdy nie uzyskać odszkodowania albo zostać istotnie zniechęcona do podjęcia trudu dochodzenia należnej rekompensaty. Konieczne zatem są regulacje prawne, które pozwolą na efektywne dochodzenie odpowiedzialności odszkodowawczej, ustalą reżim tej odpowiedzialności, a także zidentyfikują podmiot odpowiedzialny za wyrządzoną szkodę.

Status projektowanej regulacji

Publikacja Rezolucji Parlamentu Europejskiego stanowi impuls dla Komisji Europejskiej do podjęcia dalszych szczegółowych prac nad regulacją problematyki poruszonej w Projektowanym Rozporządzeniu. Jak dotąd, kwestia odpowiedzialności cywilnej za szkody wynikające z działania systemów SI nie doczekała się dalej idących kroków ustawodawczych. Projekt aktu prawnego przygotowany przez Parlament Europejski pozostaje zatem wyłącznie niewiążącą propozycją.

Co znamienne, Parlament Europejski proponuje, by regulacja odpowiedzialności cywilnej za sztuczną inteligencję przyjęła formę rozporządzenia unijnego. Rozporządzenie jest aktem prawnym wywierającym bezpośredni skutek w Państwach Członkowskich UE.

Oznacza to, że materia regulowana rozporządzeniem jest w pełni samodzielna i nie wymaga implementacji do krajowego porządku prawnego (w przeciwieństwie np. do dyrektyw). Ewentualna rozbieżność regulacyjna w poszczególnych Państwach Członkowskich UE utrudniłaby rozwój jednolitego rynku cyfrowego.

Podmiot odpowiedzialny za szkodę

Jak wskazano w Rezolucji Parlamentu Europejskiego, „wszystkie działania fizyczne czy wirtualne opierające się na systemach SI, urządzenia czy procesy, w których korzysta się z tych systemów, mogą zasadniczo być bezpośrednią lub pośrednią przyczyną szkody, a jednocześnie są one niemal zawsze wynikiem tego, że ktoś skonstruował lub wdrożył taki system albo ingerował w niego”. Odpowiedzialność za szkodę wyrządzoną działaniem systemu SI powinien więc zawsze ponosić człowiek. W konsekwencji nie jest konieczne przydawanie systemom SI odrębnej osobowości prawnej, by wprzęgnąć je w system efektywnej odpowiedzialności cywilnej.

W Projektowanym Rozporządzeniu osobą odpowiedzialną za system SI jest „operator”, to jest osoba fizyczna lub prawna, która:

- 1) do pewnego stopnia kontroluje ryzyko związane z działaniem systemu SI i czerpie korzyści z jego działania



- („operator front-end”; np. firma pożyczkowa) lub
- 2) w sposób ciągły określa cechy technologii, dostarcza dane i podstawowe usługi wsparcia, a zatem też sprawuje pewną kontrolę nad ryzykiem związanym z działaniem systemu SI („operator back-end”; np. firma dostarczająca system do oceny wiarygodności kredytowej).

Projektowane Rozporządzenie pozwala więc poszkodowanemu dość łatwo ustalić adresata ewentualnych roszczeń odszkodowawczych. Jednocześnie przedsiębiorcy zaangażowani w oferowanie systemów SI otrzymują jasną informację, na kim będzie ciążyło ryzyko odpowiedzialności odszkodowawczej. Usuwa to więc niepewność prawną co do tego, który z przedsiębiorców jest eksponowany na ryzyko roszczeń. Można też założyć, że przedsiębiorcy, którzy rozpoznają swój status operatora systemu SI, będą mieć większą motywację do podjęcia starań minimalizujących ryzyka wynikające z działania systemu SI.

Odpowiedzialność za system SI

Warto podkreślić, że regulowana w Projektowanym Rozporządzeniu odpowiedzialność operatorów dotyczy szkód wyrządzonych przez system SI. Jak wskazano na początku artykułu, sztuczna inteligencja wkomponowana w produkty czy usługi to nic innego jak określone oprogramowanie. Nie może więc dziwić, że Projektowane Rozporządzenie nie definiuje sztucznej inteligencji jako takiej (co zresztą byłoby zadaniem co najmniej trudnym), lecz posługuje się pojęciem „systemu sztucznej inteligencji”. Zgodnie z zaproponowaną definicją, system SI to „system, który opiera się na oprogramowaniu albo jest wbudowany w urządzenia, wykazuje się zachowaniem symulującym inteligencję m.in. w oparciu o gromadzenie i przetwarzanie danych, analizowanie i wyciąganie wniosków dotyczących otoczenia oraz podejmuje działania w pewnym stopniu autonomicznie, aby osiągnąć konkretne cele”.

Na marginesie, odmienną, aczkolwiek wydaje się doskonalszą, definicję

„systemu sztucznej inteligencji” sformułowano w Akcie w sprawie Sztucznej Inteligencji. Zgodnie z jego treścią jest nią „oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I [np. mechanizmy uczenia maszynowego – przyp. aut.], które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję”. Tego rodzaju rozbieżności w projektowanych aktach prawnych dotyczących sztucznej inteligencji unaocniają, jak wiele pracy legislacyjnej należy jeszcze włożyć w wypracowanie koherentnych, wzajemnie uzupełniających się regulacji prawnych.

Zasady odpowiedzialności

Odpowiedzialność operatorów systemów SI zaktualizuje się wtedy, gdy na terenie UE poszkodowany poniesie szkodę wskutek działania systemu SI. Oznacza to, że nie ma znaczenia, skąd pochodzi operator systemu SI. Strony danego kontraktu nie mogą przy tym tej odpowiedzialności umownie wyłączyć ani zmienić.

W aspekcie dochodzenia odpowiedzialności za szkody wyrządzone działaniem systemu SI Parlament Europejski opowiedział się za skorzystaniem z dostępnych zasad odpowiedzialności wypracowanych w prawie cywilnym opartych na zasadzie ryzyka i na zasadzie winy.

Odpowiedzialność oparta na zasadzie ryzyka charakteryzuje się tym, że podmiot odpowiedzialny nie może zwolnić się z odpowiedzialności za wyrządzoną szkodę wskazując, że nie ponosi winy. Okolicznością wyłączającą odpowiedzialność jest wyłącznie siła wyższa, własne postępowanie poszkodowanego lub osoby trzeciej. Przykładem zastosowania takiego reżimu odpowiedzialności jest odpowiedzialność za szkody wyrządzone działalnością kopalni czy elektrowni. W Projektowanym Rozporządzeniu odpowiedzialność na zasadzie ryzyka dotyczy funkcjonowania tych systemów SI, które ze swej natury wiążą się ze znacznym ryzykiem i autonomicznością, zagrażając ogółowi społeczeństwa w znacznie większym stopniu

– np. pojazdy autonomiczne, drony itp. Parlament Europejski proponuje, by systemy SI wysokiego ryzyka zostały skatalogowane w załączniku do Projektowanego Rozporządzenia.

Z kolei odpowiedzialność na zasadzie winy oznacza, że podmiot odpowiedzialny ponosi winę w wystąpieniu zdarzenia wywołującego szkodę. W Projektowanym Rozporządzeniu ten rodzaj odpowiedzialności miałby obowiązywać w zakresie szkód wyrządzonych działaniem systemów SI innych niż systemy SI wysokiego ryzyka. Operator takiego systemu uwolni się od odpowiedzialności, jeżeli szkoda jest następstwem działania siły wyższej lub własnego postępowania poszkodowanego bądź osoby trzeciej, jak również wtedy, gdy wykaże, że system SI został uruchomiony bez jego zgody pomimo podjęcia rozsądnych środków zapobiegawczych lub dochował należytej staranności „dobierając odpowiedni system sztucznej inteligencji do danego zadania i umiejętności, uruchamiając go odpowiednio, nadzorując działanie i utrzymując go w dobrym stanie poprzez regularną instalację dostępnych aktualizacji”.

Jeżeli za szkodę odpowiedzialnych jest dwóch lub więcej operatorów, ich odpowiedzialność jest solidarna. Poszkodowany może wtedy żądać odszkodowania od dowolnego operatora. Podmiot, który zaspokoi roszczenie poszkodowanego, może następnie regresowo dochodzić zwrotu części wypłaconej kwoty od pozostałych zobowiązanych operatorów, zależnie od stopnia kontroli operatorów nad ryzykiem związanym z działaniem systemu SI. W tym kontekście można się spodziewać, że we wzajemnych relacjach przedsiębiorcy kwalifikowani jako operatorzy front-end lub back-end będą dążyli do umownego określania stopnia kontroli nad ww. ryzykiem i w ten sposób zarządzać ryzykiem roszczeń regresowych.

Ubezpieczenie OC i przedawnienie

Projektowane Rozporządzenie określa górne limity odpowiedzialności operatora systemu SI wysokiego ryzyka. Jest to kwota do 2 milionów euro w przypadku



szkody na osobie oraz do 1 miliona euro w razie szkody niematerialnej skutkującej możliwą do zweryfikowania stratą ekonomiczną lub szkody majątkowej. Jednocześnie Parlament Europejski proponuje, by operatorzy systemów SI wysokiego ryzyka podlegali obowiązkowemu ubezpieczeniu od odpowiedzialności cywilnej w granicach wspomnianych kwot. Powyższe będzie zmuszało przedsiębiorców do przeprowadzenia dokładnej analizy, czy są operatorami systemu SI wysokiego ryzyka, by w razie ustalenia takiego statusu nabyć potrzebną polisę ubezpieczeniową.

Parlament Europejski ponadto proponuje, by roszczenia odszkodowawcze z tytułu szkód wyrządzonych działaniem systemów SI wysokiego ryzyka podlegały szczególnym zasadom przedawnienia. Roszczenia dotyczące śmierci, uszczerbku na zdrowiu lub kalectwa przedawniałyby się po 30 latach od daty powstania szkody. Z kolei roszczenia dotyczące szkód majątkowych lub poważnych szkód niematerialnych skutkujących stratą ekonomiczną przedawniałyby się:

1) po 10 latach od daty powstania szkody albo

2) po 30 latach od daty „przeprowadzenia operacji z wykorzystaniem systemu sztucznej inteligencji obciążonego wysokim ryzykiem, która doprowadziła do zniszczenia własności poszkodowanego lub do poważnej szkody niematerialnej” (przy czym zastosowanie ma ten termin, który upłynie szybciej).

W przypadku szkód wyrządzonych wskutek działania systemów SI innych niż systemy wysokiego ryzyka, obowiązywałby okres przedawnienia określony w przepisach Państwa Członkowskiego, w którym powstała szkoda.

Podsumowanie

Projektowane Rozporządzenie jest niewątpliwie interesującą propozycją ustawodawczą, której potrzeba istnienia wpisuje się w plany kompleksowej regulacji problematyki sztucznej inteligencji w UE. Cele przyświecające regulacji odpowiedzialności za działania systemów SI są jasno zarysowane i konsekwentnie realizowane przez ustawodawcę unijnego.

Proponowane przez Parlament Europejski rozwiązania w zakresie ukształtowania reżimu odpowiedzialności za szkody wyrządzone działaniem systemów SI nie są rewolucyjne, dzięki czemu mogą spotkać się z łatwiejszą absorpcją ze strony przedsiębiorców oferujących produkty lub usługi oparte o sztuczną inteligencję.

Warto też podkreślić, że Projektowane Rozporządzenie wymusi na przedsiębiorcach z wielu różnych gałęzi biznesu konieczność wdrożenia mechanizmów zapewniających zgodność z projektowanymi regulacjami. Z jednej strony, przedsiębiorca będzie musiał na bieżąco monitorować i weryfikować, czy jest adresatem regulacji (operatorem), a z drugiej strony – podejmować działania minimalizujące ryzyka wynikające z korzystania z danego produktu lub usługi inkorporującej system SI. Omawiane regulacje wciąż pozostają pionierskie w swej naturze, toteż dopiero przyszłość pokaże, czy i jak dodatkowe obowiązki wpłyną na konkurencyjność przedsiębiorców i rzeczywiste osiągnięcie zakładanych celów.

Łukasz Wieczorek

radca prawny, absolwent studiów prawniczych i doktoranckich na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego, partner w Konieczny Wierzbicki Kancelaria Radców Prawnych, gdzie kieruje zespołem TMT; specjalizuje się w prawie nowych technologii/IT, prawie własności intelektualnej i prawie zwalczania nieuczciwej konkurencji, koordynując w Kancelarii sprawy o charakterze międzynarodowym (International Desk) w zakresie ww. obszarów prawnych

- 1 Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję (2020/2014(INL)).
- 2 Projekt rozporządzenia stanowi załącznik do wspomnianej Rezolucji Parlamentu Europejskiego; pełny tytuł projektu: *Rozporządzenie Parlamentu Europejskiego i Rady w sprawie odpowiedzialności za działanie systemów sztucznej inteligencji*.
- 3 Projekt z dnia 21 kwietnia 2021 r., COM(2021) 206 final, 2021/0106(COD); pełny tytuł projektu: *Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie Sztucznej Inteligencji) i zmieniające niektóre akty ustawodawcze Unii*.



Rejestracja znaku towarowego a prawo autorskie

Konsekwencje braku uregulowania kwestii praw autorskich do znaku towarowego

Marta Lampart

Oznaczenie odróżniające może podlegać ochronie jako znak towarowy zarówno na gruncie polskich, jak i unijnych przepisów prawa. Takim oznaczeniem odróżniającym, objętym ochroną prawnoznakową może być m.in. wyraz, nazwisko, rysunek, litera, forma przestrzenna lub dźwięk. Możliwe także, że dane oznaczenie objęte jest ochroną wynikającą z prawa autorskiego, o ile spełnia przesłanki do uznania go za utwór w rozumieniu prawa autorskiego. Co do zasady dopuszczalna jest kumulatywna ochrona znaku towarowego na gruncie odpowiednich przepisów prawa własności przemysłowej oraz przepisów prawa autorskiego. Problematyczna może być jednak sytuacja, w której uprawnionym z prawa ochronnego na znak towarowy i uprawnionym do praw autorskich są dwa różne podmioty. Planując uzyskanie rejestracji znaku towarowego dla przedsiębiorstwa warto rozważyć zagadnienia związane z ochroną oznaczenia odróżniającego jako znaku towarowego oraz utworu w świetle prawa autorskiego. Jest to ważne w kontekście możliwości rejestracji oznaczenia odróżniającego w charakterze znaku towarowego.

Znak towarowy jako utwór

Ustawa z dnia 30 czerwca 2000 r. Prawo własności przemysłowej¹, która reguluje między innymi zasady uzyskania i utrzymania ochrony znaków towarowych w Polsce, przewiduje, że przepisy tej ustawy nie uchybiają ochronie znaków towarowych określonej w innych ustawach. Jest to ogólna zasada wprowadzona przez ustawodawcę umożliwiająca kumulatywną ochronę dóbr własności przemysłowej². Mogą one podlegać również ochronie na gruncie przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych³. Przedmiotem prawa autorskiego jest z kolei każdy przejaw działalności

twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia, tj. utwór. Takim może być również w pewnych przypadkach oznaczenie odróżniające.

W przeciwieństwie do zasad ochrony dóbr własności przemysłowej na gruncie p.w.p., prawo autorskie nie wymaga uzyskania rejestracji, utwór jest przedmiotem prawa autorskiego od chwili ustalenia, chociażby miał postać nieukończoną, a ochrona przysługuje twórcy niezależnie od spełnienia jakichkolwiek formalności. Do utworu twórcy przysługują osobiste oraz majątkowe prawa autorskie. W orzecznictwie sądowym znajdujemy stanowisko, które przewiduje, iż podmiot autorskich praw majątkowych do znaku graficznego ma prawo decydowania o wykorzystaniu tego znaku⁴.

Rejestracji w charakterze znaku towarowego podlegają nierzadko m.in. słowno-graficzne lub graficzne oznaczenia odróżniające. Przykładowo takie oznaczenia mogą podlegać kumulatywnej ochronie – zarówno jako znak towarowy, jak i utwór. W literaturze prawniczej przyjmuje się, że ochrona prawnoautorska możliwa jest zwłaszcza w odniesieniu do znaku słowno-graficznego⁵. Nie jest wykluczone, że nowe typy znaków towarowych, uwzględniające najnowsze trendy, mogą również być objęte ochroną wynikającą z prawa autorskiego.

Przedsiębiorcy używają w swojej działalności logo, które najczęściej zamawiają u grafika, a następnie rejestrują jako znak towarowy. Wielu przedsiębiorców nie jest świadomych, że dla zgodnego z prawem i nienaruszającego praw autorskich twórcy korzystania z oznaczenia wykonanego przez grafika niezbędne jest odpowiednie uregulowanie kwestii autorskich praw, w tym majątkowych i wymienienie w umowie właściwych

pól eksploatacji. Może być to umowa licencyjna lub umowa przenosząca prawa majątkowe autorskie, w zależności od ustaleń w danej sprawie. Wynika to z tego, że to twórcy przysługuje wyłączne prawo do korzystania z utworu i rozporządzania nim na wszystkich polach eksploatacji oraz do wynagrodzenia za korzystanie z utworu. Są to prawa majątkowe autorskie do utworu, które są zbywalne i podlegają dziedziczeniu. W umowie powinny znaleźć się również postanowienia dotyczące autorskich praw osobistych.

Jeżeli dane oznaczenie odróżniające spełnia przesłanki do uznania go za utwór w rozumieniu prawa autorskiego, to korzystanie z tego oznaczenia w działalności przedsiębiorcy bez odpowiedniego uregulowania kwestii praw autorskich prowadzić będzie do naruszenia praw twórcy oznaczenia lub podmiotu, któremu przysługują prawa majątkowe autorskie. Ma to znaczenie nie tylko dla skutecznego zgłoszenia oznaczenia odróżniającego w charakterze znaku towarowego do Urzędu Patentowego Rzeczypospolitej Polskiej (UPRP), ale także dla nienaruszającego praw autorskich korzystania z tego oznaczenia na potrzeby przedsiębiorstwa. Niezależnie bowiem od tego, czy dane oznaczenie podlegać będzie zgłoszeniu do UPRP, jego używanie w obrocie wymaga także uregulowania możliwości korzystania z tego oznaczenia w działalności przedsiębiorstwa.

Coraz częściej przedsiębiorcy sami tworzą swój znak towarowy w oparciu o gotowe grafiki czy symbole dostępne w popularnych programach graficznych. Również tworząc samemu oznaczenie trzeba zwracać uwagę na postanowienia licencji przewidzianych w tym programach, zwłaszcza w zakresie możliwości zgłoszenia tak stworzonego oznaczenia do ochrony w charakterze znaku towarowego⁶.



Brak uregulowania kwestii praw autorskich do znaku towarowego a rejestracja znaku towarowego

Zgłoszenie znaku towarowego w UPRP rozpoczyna procedurę rejestracji oznaczenia odróżniającego w tym urzędzie, która może zakończyć się decyzją przyznającą prawo ochronne na znak towarowy albo decyzją odmawiającą przyznania takiego prawa zgłaszającemu. W przypadku uzyskania prawa ochronnego na znak towarowy przez UPRP nabywa się prawo wyłącznego używania znaku towarowego w sposób zarobkowy lub zawodowy na całym obszarze Rzeczypospolitej Polskiej, przez okres 10 lat liczonych od daty zgłoszenia, a udzielone prawo ochronne podlega wpisowi do rejestru znaków towarowych. Wydanie pozytywnej decyzji przez UPRP oznacza jedynie przyznanie ochrony prawnoznakowej. Znak towarowy, jeśli spełnia przesłanki do uznania go za utwór w rozumieniu prawa autorskiego, chroniony jest także jako dzieło. Jego ochrona jako utworu nie wymaga spełnienia żadnych formalności.

Procedura rejestracji znaku towarowego, obecnie analogicznie jak w przepisach unijnych, podzielona jest niejako na dwa etapy – najpierw UPRP bada istnienie bezwzględnych przeszkód rejestracji, a po tym etapie następuje okres, w którym możliwe jest złożenie sprzeciwu wobec zgłoszenia znaku towarowego. Ta zmiana została wprowadzona w polskich przepisach w 2016 r., wcześniej UPRP z urzędu brał pod uwagę zarówno bezwzględne, jak i względne przeszkody rejestracji. Obecnie twórcom lub uprawnionym do wcześniejszych praw osobistych lub majątkowych pozostaje monitorowanie zgłoszeń znaków towarowych i reagowanie na te zgłoszenia w odpowiednim terminie.

W sprzeciwie można podnosić istnienie względnych przeszkód rejestracji określonych m.in. w art. 1321 p.w.p. W terminie 3 miesięcy od daty ogłoszenia o zgłoszeniu znaku towarowego uprawniony do wcześniejszego znaku towarowego, uprawniony z wcześniejszego prawa

osobistego lub majątkowego, a także osoba uprawniona do wykonywania praw wynikających z chronionej nazwy pochodzenia lub chronionego oznaczenia geograficznego może wnieść sprzeciw wobec zgłoszenia znaku towarowego z przyczyn, o których mowa m.in. w art. 1291 ust. 4 lub w art. 1321 ust. 1-3. Po rozpatrzeniu sprzeciwu uznanego za zasadny nie udziela się prawa ochronnego na znak towarowy m.in. w przypadku znaku towarowego, którego używanie narusza prawa osobiste lub majątkowe osób trzecich. Tak będzie, gdy istnieje wcześniejsze prawo i możliwość jego naruszenia poprzez używanie znaku towarowego⁷. Słusznie podnosi się w literaturze i orzecznictwie, że UPRP ma wyłączną kognicję do dokonywania ustaleń w zakresie naruszenia praw osobistych lub majątkowych w toku rozpoznawanego sprzeciwu⁸. Nie ma tutaj znaczenia dla jakich towarów lub usług zostało dokonane zgłoszenie znaku towarowego, znamienne jest bowiem naruszenie prawa osobistego lub majątkowego, a takie może występować niezależnie od tego dla jakich towarów lub usług dokonano zgłoszenia znaku towarowego. Jak przyjmuje UPRP „podmiot wnoszący sprzeciw – domagający się ochrony praw autorskich majątkowych, jeśli sam nie jest autorem utworu, powinien przedstawić dowody na przeniesienie majątkowych praw autorskich w zakresie, w którym możliwe jest dochodzenie naruszenia w przypadku kolizji ze znakiem towarowym”⁹. Z kolei pisemna zgoda uprawnionego z wcześniejszego prawa osobistego lub majątkowego na udzielenie prawa ochronnego na późniejszy znak towarowy powoduje oddalenie sprzeciwu (przewiduje takie rozwiązanie art. 133 p.w.p.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) nr 2015/2436 z dnia 16 grudnia 2015 r. mająca na celu zbliżenie ustawodawstw państw członkowskich odnoszących się do znaków towarowych¹⁰ w art. 5 ust. 4 lit. b) wprowadziła fakultatywną możliwość postanowienia przez państwa członkowskie, że znaku towarowego nie rejestruje się, a w przypadku, gdy został już zarejestrowany, podlega on unieważnieniu, jeżeli i w zakresie, w jakim używanie znaku towarowego może być zabronione w związku z istnieniem wcześniejszego prawa innego niż

prawa, o których mowa w ust. 2 i w lit. a) ust. 4, a w szczególności prawa do nazwiska lub nazwy, prawa do osobistego wizerunku, prawa autorskiego lub prawa własności przemysłowej. W p.w.p. takie rozwiązanie zostało wprowadzone w art. 1321 ust. 1 pkt 1, nawet w szerszym zakresie. Dyrektywa w 36 motywie przewiduje także: „W celu usprawnienia i ułatwienia dostępu do ochrony znaków towarowych oraz zwiększenia pewności i przewidywalności prawa, procedura rejestracji znaków towarowych w państwach członkowskich powinna być efektywna i przejrzysta oraz oparta na przepisach zbliżonych do przepisów mających zastosowanie do unijnych znaków towarowych”.

O ile w przypadku bezwzględnych przeszkód rejestracji UPRP bierze je pod uwagę z urzędu, tak względne przeszkody rejestracji zgłaszane mogą być w sprzeciwie przez uprawnione do tego podmioty. Jeżeli sprzeciw nie wpłynie w ustawowo określonym terminie, to prawo ochronne na znak towarowy zostanie przyznane, o ile nie zachodzą żadne z innych przeszkód rejestracji i nie zostały zgłoszone inne sprzeciwy wobec zgłoszenia.

W sytuacji, gdy zgłaszający nie uregulował odpowiednio z twórcą oznaczenia odróżniającego kwestii praw autorskich do tego oznaczenia, a w szczególności autorskich praw majątkowych istnieje uzasadnione ryzyko, że twórca będzie mógł wnieść sprzeciw wobec zgłoszenia znaku towarowego, o ile oznaczenie to spełnia przesłanki do uznania go za utwór w rozumieniu prawa autorskiego i być może skutecznie zablokować możliwość uzyskania ochrony na zgłoszone oznaczenie. Na rynku istnieje wiele ofert dotyczących stworzenia oznaczenia dla przedsiębiorstwa, warto jednak pamiętać nie tylko o tym, aby zamówione oznaczenie spełniało podstawowe przesłanki przyznania ochrony jako znaku towarowego, ale także o tym, aby odpowiednio zagwarantować w umowie z twórcą korzystanie z takiego oznaczenia. Pozwoli to uniknąć tym samym ryzyka wniesienia sprzeciwu wobec zgłoszenia znaku towarowego w tym zakresie. Istotne jest tutaj przede wszystkim prawidłowe wymienienie w umowie przenoszącej prawa majątkowe autorskie lub umowie licencyjnej pól eksploatacji.



Brak uregulowania kwestii praw autorskich do znaku towarowego a możliwość unieważnienia prawa z rejestracji znaku towarowego

Ze względu na procedurę rejestracji znaku towarowego w UPRP możliwe jest, że oznaczenie odróżniające uzyska ochronę jako znak towarowy pomimo tego, że jego używanie narusza prawa osobiste lub majątkowe osób trzecich. Może dojść do udzielenia prawa ochronnego na znak towarowy w sytuacji, gdy uprawniony podmiot nie złoży w terminie sprzeciwu wobec znaku towarowego. Nie oznacza to jednak, że raz uzyskane prawo ochronne nie może zostać unieważnione. W ustawie przewidziane są pewne warunki, przy których spełnieniu możliwe jest podważenie ważności udzielonego prawa ochronnego.

Zgodnie z art. 164 p.w.p. prawo ochronne na znak towarowy może być unieważnione na wniosek, w całości lub części, jeżeli nie zostały spełnione warunki do uzyskania tego prawa z przyczyn, o których mowa w art. 1291, art. 1361 oraz art. 1363 i w przypadku istnienia wcześniejszego prawa, o którym mowa w art. 1321 ust. 1–3 p.w.p. Takim wcześniejszym prawem jest prawo osobiste lub majątkowe. Na to prawo może powoływać się tylko uprawniony z tego prawa oraz osoba uprawniona do wykonywania praw wynikających z tego prawa.

Istnieją pewne ograniczenia związane z możliwością występowania z wnioskiem o unieważnienie prawa ochronnego z powodu naruszenia praw osobistych lub majątkowych wnioskodawcy. Stanie się tak, gdy przez okres pięciu kolejnych lat używania zarejestrowanego znaku wnioskodawca, będąc świadomym jego używania, nie sprzeciwiał się temu. Wyłączenia to nie ma jednak zastosowania, jeżeli uprawniony uzyskał prawo ochronne działając w złej wierze. Nie można natomiast wystąpić z wnioskiem o unieważnienie, jeżeli sprzeciw oparty na tych samych prawach wcześniejszych i na tych samych podstawach prawnych został prawomocnie



oddalony. Nie ma więc sensu w tym przypadku składanie wniosku o unieważnienie udzielonego prawa ochronnego na znak towarowy, jeżeli wcześniej złożony sprzeciw został prawomocnie oddalony.

W przepisach p.w.p. znajduje się zatem również rozwiązanie umożliwiające unieważnienie udzielonego prawa ochronnego na znak towarowy, jeżeli mamy do czynienia z istnieniem wcześniejszych praw autorskich do znaku towarowego, a kwestia używania takiego znaku nie została odpowiednio uregulowana w umowie z jego twórcą lub podmiotem uprawnionym do autorskich praw majątkowych.

Podsumowanie

Przedsiębiorcy działający na polskim i unijnym rynku planujący dokonać zgłoszenia oznaczeń odróżniających do ochrony jako znaki towarowe powinni zwracać uwagę, czy używanie ich znaku narusza będzie prawa osobiste lub majątkowe osób trzecich. Kwestia ta ma znaczenie w przypadku oznaczeń, które stanowią utwór, a więc mogą być objęte ochroną wynikającą z prawa autorskiego. Szczególnie ważna jest tutaj treść umowy zawartej z grafikiem i odpowiednio uregulowanie w niej kwestii praw autorskich, w tym majątkowych praw autorskich. Popełnione błędy mogą skutkować uznaniem przez UPRP wniesionego sprzeciwu wobec zgłoszenia lub wniosku o unieważnienie udzielonego już prawa ochronnego za uzasadniony. Inwestycja w znaki towarowe przedsiębiorstwa wymaga więc zadbania również o właściwe uregulowanie

kwestii praw autorskich do oznaczenia, które ma podlegać zgłoszeniu w charakterze znaku towarowego.

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 ze zm; dalej jako: p.w.p.
- ² M. Poźniak-Niedzielska, *Ochrona kumulatywna wzorów przemysłowych*, STPP 2011, Nr 1, str. 287, § 1 (wersja elektroniczna, Legalis).
- ³ Tekst jednolity: Dz. U. z 2021 r. poz. 1062 ze zm.; dalej jako: p.a.p.p.
- ⁴ Wyrok Sądu Najwyższego – Izba Cywilna i Administracyjna z dnia 25 października 1988 r., sygn. akt: II CR 143/88, Legalis nr 26448.
- ⁵ M. Bohaczewski, Ł. Żelechowski, Art. 1321 [Skutki zasadnego sprzeciwu], [w:] K. Osajda, Ł. Żelechowski (red.), *Prawo własności przemysłowej*. Komentarz, Warszawa 2021, teza 49 (wersja elektroniczna, Legalis).
- ⁶ Przykładowo wskazać można popularny program Canva i jego warunki w omawianym zakresie: <https://www.canva.com/help/article/trademarks-logo> [dostęp: 7.11.2021 r.].
- ⁷ M. Witkowska, A. Michalak, *Znaki towarowe i oznaczenia geograficzne*, [w:] A. Michalak (red.), *Prawo własności przemysłowej*. Komentarz, Warszawa 2016, s. 419.
- ⁸ M. Bohaczewski, Ł. Żelechowski, Art. 1321 [Skutki zasadnego sprzeciwu], [w:] K. Osajda, Ł. Żelechowski (red.), *Prawo własności przemysłowej*. Komentarz, Warszawa 2021, teza 13 i 51 (wersja elektroniczna, Legalis).
- ⁹ *Wytyczne w zakresie znaków towarowych, Naruszenie praw osobistych lub majątkowych, Autorskie prawa osobiste i majątkowe*, UPRP, <https://uprp.gov.pl/pl/przedmioty-ochrony/ogolne-wytyczne-prezesa-uprp/wytyczne-w-zakresie-znakow-towarowych/-naruszenie-praw-osobistych-lub-majatkowych/autorskie-prawa-osobiste-i-majatkowe>, [dostęp: 7.11.2021 r.].
- ¹⁰ Dz. Urz. UE L Nr 336, s. 1; dalej jako: dyrektywa 2015/2436.



Tajemnica przedsiębiorcy i tajemnica przedsiębiorstwa, cz. II

Różnice i podobieństwa

Józef Edmund Nowicki

Wyjaśnienia składane w celu ustalenia, czy oferta zawiera rażąco niską cenę

Za tajemnicę przedsiębiorstwa mogą być również uznane wyjaśnienia wykonawcy składane w celu ustalenia, czy oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia. W wyroku z dnia 14 maja 2013 r., KIO 908/13 uznano, że wyjaśnienia złożone przez wykonawcę mogą być uznane za stanowiące tajemnicę przedsiębiorstwa, gdyż zarówno metoda kalkulacji ceny, jak i konkretne dane cenotwórcze ujawnione przez wykonawcę na żądanie zamawiającego dla sprawdzenia, czy cena oferty nie jest ceną rażąco niską, stanowią tajemnicę przedsiębiorstwa i mogą być przedmiotem ochrony przez ich utajnienie przed innymi podmiotami, również tymi uczestniczącymi w przetargu. Krajowa Izba Odwoławcza zwróciła uwagę, że informacje te powstają na potrzeby konkretnego postępowania o zamówienie publiczne więc mają wartość gospodarczą. Sposób budowania strategii cenowej w ofercie i elementy składowe tej strategii spełniają przesłanki uznania informacji tych za tajemnicę przedsiębiorstwa, stanowią jego *know-how*, jako posiadających wartość handlową i gospodarczą, obrazują bowiem rozwiązanie dotyczące kalkulacji ceny, która pozwoliła na wybór oferty tego wykonawcy jako najkorzystniejszej.

Faktury

Co do zasady treść faktur i potwierdzenia zapłaty nie stanowią tajemnicy przedsiębiorstwa (wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 25 listopada 2015 r., II SA/Wa 1266/15).

Treść faktur może stanowić tajemnicę przedsiębiorstwa, jeżeli ich ujawnienie mogłoby mieć wpływ na sytuację

ekonomiczną wykonawcy, jakkolwiek nie muszą mieć same w sobie wartości gospodarczej (zob. wyrok Wojewódzkiego Sądu Administracyjnego z dnia 26 października 2017 r., IV SA/Po 571/17). Warto zauważyć, że treść faktury obrazuje wielkość produkcji i sprzedaży, a także źródła zaopatrzenia i zbytu. W postanowieniu z dnia 30 października 1996 r., XVII Amz 3/96 Sąd Antymonopolowy uznał, że dane obrazujące wielkość produkcji i sprzedaży, a także źródła zaopatrzenia i zbytu mogą stanowić tajemnicę przedsiębiorstwa.

Jak wykonawca powinien dowodzić, że informacja stanowi tajemnicę przedsiębiorstwa?

To na wykonawcy, zastrzegającym taką informację, spoczywa obowiązek wykazania przesłanek skuteczności takiego zastrzeżenia. Wykonawca winien uczynić to jednocześnie z samym zastrzeżeniem, nie czekając na decyzję i ewentualne wezwania zamawiającego w tym zakresie" (zob. wyrok z dnia 8 czerwca 2015 r., KIO 997/15). W wyroku z dnia 4 lutego 2016 r., KIO 84/16 Krajowa Izba Odwoławcza nakazując odtajnienie koncepcji wykonawcy Z., z uwagi na brak wykazania zasadności zastrzeżenia tajemnicy przedsiębiorstwa, stwierdziła, że poprzestanie przez wykonawcę na wskazaniu informacji niepodlegających ujawnieniu, przy braku jednoczesnego wykazania, że stanowią one tajemnicę przedsiębiorstwa, powinno być poczytane przez zamawiającego, jako nieskuteczne zastrzeżenie tajemnicy przedsiębiorstwa. W takiej sytuacji zamawiający ma obowiązek udostępnienia zainteresowanym przekazanych informacji, niezależnie od tego, czy stanowiłyby one tajemnicę przedsiębiorstwa w rozumieniu art. 11

ust. 4 uznk, rozpatrywanego w oderwaniu od art. 8 ust. 3 Pzp. **Niewykazanie przez wykonawcę zasadności poczynionego zastrzeżenia oznacza bowiem, co najmniej, że w postępowaniu o udzielenie zamówienia nie podjął on niezbędnych działań w celu zachowania w poufności informacji mających dla niego wartość gospodarczą, które uprzednio nie były ujawnione do wiadomości publicznej.**

Ustawodawca pozostawił wykonawcy dowolność w doborze środków służących wykazaniu, że zastrzeżona informacja stanowi tajemnicę przedsiębiorstwa. Użyte w art. 18 ust. 3 Pzp wyrażenia „zastrzegł, że nie mogą być one udostępniane” oraz „wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa” oznaczają, iż w ramach wykazywania istnienia przesłanek określonych w art. 11 ust. 4 uznk, w odniesieniu do zastrzeganych informacji, wykonawca powinien przedłożyć określone dowody, nie zaś ograniczyć się do samego zastrzeżenia określonych informacji jako tajemnicy przedsiębiorstwa. Wykazanie przez wykonawcę, że zastrzeżone informacje posiadają walor tajemnicy przedsiębiorstwa, powinno polegać na złożeniu dowodów mających postać np. oświadczenia uzasadniającego, dlaczego określone informacje mają przymiot tajemnicy przedsiębiorstwa, np. wyciągu z umów z kontrahentami zawierających postanowienia o zachowaniu określonych okoliczności w poufności.

Wykonawca powinien wskazać konkretne okoliczności, czy chociażby działania które zostały podjęte przez wykonawcę, tj. np. wykazanie się wewnętrznymi regulaminami, wskazującymi iż zastrzeżona informacja nie może zostać w żaden sposób upubliczniona (wyrok z dnia 23 kwietnia 2010 r., KIO/UZP 528/10). **Dla wykazania wystąpienia przesłanek tajemnicy przedsiębiorstwa, o których mowa w art. 11**



ust. 4 uznk nie wystarczą same deklaracje. Wykonawca musi nie tylko wyjaśnić, ale także udowodnić ziszczenie się poszczególnych przesłanek warunkujących uznanie danej informacji za tajemnicę przedsiębiorstwa. Wykonawca musi wykazać, że informacja ma charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub inny posiadający wartość gospodarczą i nie została ujawniona do wiadomości publicznej oraz że podjęto w stosunku do niej niezbędne działania w celu zachowania poufności. Pod pojęciem „wykazania” należy rozumieć nie tylko złożenie oświadczenia, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa, ale również przedstawienie dowodów na jego potwierdzenie. W wyroku z dnia 16 lutego 2018 r., KIO 200/18, Krajowa Izba Odwoławcza w pełni podzieliła stanowisko prezentowane w uzasadnieniu do poselskiego projektu ustawy o zmianie ustawy – Prawo zamówień publicznych (Sejm RP VII kadencji, druk sejmowy nr 1653), w którym wskazano, że „mimo zasady jawności postępowania, informacje dotyczące przedsiębiorstwa nie są podawane do publicznej wiadomości. Jednakże, słuszny w swym założeniu przepis jest w praktyce patologicznie nadużywany przez wykonawców, którzy zastrzegając informacje będące podstawą do ich ocen, czynią to ze skutkiem naruszającym zasady uczciwej konkurencji, tj. wyłącznie w celu uniemożliwienia weryfikacji przez konkurentów wypełniania przez nich wymagań zamawiającego. Realizacja zadań publicznych wymaga faktycznej jawności wyboru wykonawcy. Stąd te dane, które są podstawą do dopuszczenia wykonawcy do udziału w postępowaniu powinny być w pełni jawne. Praktyka taka miała miejsce do 2005 r. i bez negatywnego skutku dla przedsiębiorców dane te były ujawniane. Poddanie ich regułom ochrony właściwym dla tajemnicy przedsiębiorstwa jest sprzeczne z jej istotą, a przede wszystkim sprzeczne z zasadą jawności realizacji zadań publicznych”. W ocenie Krajowej Izby odwoławczej **samo powoływanie się na klauzule poufności zawarte w umowie z kontraktem, bez udowodnienia że informacja ma charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub inny posiadający wartość gospodarczą i nie została ujawniona do wiadomości publicznej oraz**

że podjęto w stosunku do niej niezbędne działania w celu zachowania poufności, a nawet bez wykazania, że taka umowa została faktycznie zawarta, nie może uzasadniać uznania zastrzeżenia tajemnicy przedsiębiorstwa za skuteczne. W ocenie Krajowej Izby Odwoławczej nie wystarczą jedynie twierdzenia wykonawcy. W takim wypadku niezbędne jest przedłożenie konkretnych dowodów, a zatem umowy zawartej w konkretnej dacie z konkretnym podmiotem, zawierającej konkretne postanowienia, w ramach której wykonawca zobowiązany jest do zachowania w poufności wszelkich informacji. W przypadku gdy wykonawca powołuje się na kilka umów, powinien załączyć wszystkie. W sposób tożsamy należy ocenić powołanie się wykonawcy na wewnątrz procedury obowiązujące w jego przedsiębiorstwie. Skoro obowiązują u wykonawcy procedury narzucające pracownikom odpowiedni sposób gromadzenia, przetwarzania i przechowywania poufnych danych, specyficzny obieg dokumentów, a także poszczególne osoby zobowiązane są do zachowania poufności, to wykonawca powinien takie procedury przedstawić zamawiającemu, jako dowody na tę okoliczność. Przykładowo będą to zarządzenia w sprawie ochrony bezpieczeństwa informacji, regulacje związane z obiegiem dokumentów, dostępem do nich, utworzeniem kancelarii tajnej czy też postanowienia umowne zawierające klauzule poufności dotyczące pracowników.

Postępowanie zamawiającego w przypadku zastrzeżenia tajemnicy przedsiębiorstwa

Zamawiający powinien każdorazowo dokonać oceny, czy w stosunku do informacji, których poufność wykonawca zastrzegł, nastąpiło kumulatywne ziszczenie się przesłanek określonych w art. 11 ust. 4 uznk oraz 18 ust. 3 Pzp. Na zamawiającym spoczywa bowiem obowiązek należytego badania zastrzeżenia tajemnicy przedsiębiorstwa, a następnie podjęcia decyzji o odtajnieniu, bądź nie, informacji zawartych w ofercie wykonawcy. Zamawiający obligatoryjnie

w każdym przypadku powinien zbadać, czy faktycznie zaistniały przesłanki objęcia danych informacji tajemnicą przedsiębiorstwa. Nie może zatem bezkrytycznie akceptować zastrzeżenia tajemnicy przedsiębiorstwa poczynione go przez wykonawcę, lecz winien żądać od wykonawcy wykazania zastrzeżenia tajemnicy przedsiębiorstwa w sposób uprawniony (zob. wyrok z dnia 31 marca 2009 r., KIO/UZP/338/09).

W przypadku stwierdzenia, że tajemnicą objęte zostały informacje niespełniające przesłanek uznania, iż stanowią tajemnicę przedsiębiorstwa, zamawiający ma obowiązek odtajnienia treści ofert, stosownie do wskazań Sądu Najwyższego w uchwale z dnia 21 października 2005 r., III CZP 74/05, zgodnie z którymi w postępowaniu o udzielenie zamówienia publicznego zamawiający bada skuteczność dokonanego przez oferenta zastrzeżenia dotyczącego zakazu udostępniania informacji potwierdzających spełnienie wymagań wynikających ze specyfikacji istotnych warunków zamówienia.

Odwołujący uzasadniając postawiony zarzut wskazał, że z ochrony wynikającej z tajemnicy przedsiębiorstwa mogą korzystać jedynie informacje (a nie automatycznie całe dokumenty), które odpowiadają definicji ustawowej tajemnicy przedsiębiorstwa. W konsekwencji nie jest dopuszczalne objęcie tajemnicą przedsiębiorstwa całego dokumentu, a wyłącznie tych informacji, które w jego treści faktycznie stanowią tajemnicę przedsiębiorstwa.

Postępowanie zamawiającego, gdy wykonawca nie wykaże, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.

Jeżeli wykonawca poprzestanie na zastrzeżeniu w ofercie danych informacji jako tajemnicy przedsiębiorstwa, bez wykazania skuteczności ich utajnienia w świetle art. 11 ust. 4 uznk, zamawiający nie jest związany zakazem ujawniania tych informacji, wynikającym z art. 18 ust. 3 Pzp. Nie składając wyjaśnień wykonawca rezygnuje w postępowaniu z ochrony zastrzeżonych informacji, które nawet poza postępowaniem mogły spełniać przesłanki określone w art. 11 ust. 4 uznk (zob. wyrok z dnia 3 kwietnia 2015r., KIO 561/15 i wyrok



z dnia 28 sierpnia 2015 r., KIO 1730/15). W orzecznictwie podkreśla się, że obowiązek wykazania, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa są dodatkowym, ustawowym warunkiem koniecznym dla zachowania poufności informacji (zob. wyrok z dnia 5 maja 2015 r., KIO 761/15, KIO 764/15). Podkreśla się również to, że zastrzeżenie tajemnicy przedsiębiorstwa i wykazanie, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa musi nastąpić jednocześnie (zob. wyrok z dnia 2 marca 2015 r., KIO 279/15). W wyroku z dnia 3 kwietnia 2015 r., KIO 561/15 Krajowa Izba Odwoławcza uznała, że brak wykazania, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa rodzi po stronie zamawiającego obowiązek udostępnienia zainteresowanym informacji, niezależnie od tego, czy stanowiłyby one tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 uznk. Jeżeli w wyniku weryfikacji okaże się, że zastrzeżona informacja nie stanowi tajemnicy przedsiębiorstwa, to zadeklarowane zastrzeżenie staje się bezskuteczne (wyrok WSA w Warszawie z dnia 12 października 2012 r. sygn. akt II SA/Wa 1483/12, wyrok WSA w Warszawie z dnia 4 kwietnia 2014 r., sygn. akt II SA/Wa 2406/13).

Jaki jest termin na wniesienie odwołania na zaniechanie ujawnienia informacji zastrzeżonych w ofercie jako tajemnicy przedsiębiorstwa?

W wyroku z dnia 26 stycznia 2012 r., KIO 100/12, dotyczącym liczenia terminu na wniesienie odwołania na zaniechanie ujawnienia informacji zastrzeżonych w ofercie jako tajemnicy przedsiębiorstwa Krajowa Izba Odwoławcza zwróciła uwagę, że w przypadku odwołania wobec zaniechania ujawnienia informacji zastrzeżonych w ofercie, powstaje pytanie jaki dzień uznać należy za ten, w którym powzięto, lub przy zachowaniu należytej staranności można było powziąć, wiadomość o okolicznościach stanowiących podstawę do wniesienia odwołania na nieodtajnienie oferty. Problem z ustaleniem



początku biegu terminu na wniesienie odwołania w tej kwestii komplikuje również fakt, że ustawa Pzp nie przewiduje, w jakim terminie zamawiający musi przeprowadzić weryfikację ofert pod wyżej wskazanym kątem, jak również nie przewiduje obowiązku, ani trybu poinformowania wykonawców o zajęciu przez zamawiającego stanowisku i jego uzasadnieniu. W tym zakresie, wytycznych należy poszukiwać w licznych orzeczeniach sądów oraz Krajowej Izby Odwoławczej.

Niewątpliwym jest, że pierwszym terminem, kiedy wykonawca dowiaduje się lub może się dowiedzieć o samym fakcie zastrzeżenia tajemnicy w ofertach innych wykonawców, jest termin otwarcia ofert. Jednakże należy podkreślić, że w tym samym terminie również zamawiający dowiaduje się o fakcie, że w złożonych ofertach zostały zastrzeżone niektóre informacje czy dokumenty i musi on mieć stosowny okres czasu na podjęcie określonych badań, aby stwierdzić, czy zaistniały okoliczności odpowiadające warunkom określonym w art. 11 ust. 2 uznk. Rozpoczęcie badania zasadności zastrzeżenia tajemnicy przedsiębiorstwa w ofertach wykonawców, zgodnie z orzecznictwem Krajowej Izby Odwoławczej musi nastąpić niezwłocznie po terminie otwarcia (zob. wyrok KIO 183/11/).

Do etapu badania należy zaliczyć również potrzebę wystąpienia do wykonawcy o wskazanie i szczegółowe uzasadnienie podstaw zastrzeżenia określonych informacji jako tajemnica przedsiębiorstwa. Za zasadnością takiego wystąpienia przemawia przede wszystkim fakt, że przesłanka zachowania tajemnicy pewnych informacji dotyczy przedsiębiorstwa wykonawcy, a nie zamawiającego i dlatego też to wykonawca winien wykazać zamawiającemu potrzebę

tego zastrzeżenia. W sytuacji kiedy wykonawca wystąpi z wnioskiem do Zamawiającego o udostępnienie mu w całości oferty danego wykonawcy i Zamawiający poinformuje go o terminie, w którym podejmie decyzję, czy zastrzeżenie tajemnicy zostało dokonane prawidłowo, to termin na wniesienie odwołania biegnie dopiero od tego wskazanego terminu. Tym samym termin na wniesienie odwołania od zaniechania odtajnienia zastrzeżonych w ofercie informacji powinien być liczony od momentu uzyskania przez wykonawcę wiedzy o podjęciu przez zamawiającego decyzji odnośnie do skuteczności danego zastrzeżenia.

Zamawiający, przekazując informacje o odmowie udostępnienia wykonawcom oferty w pełnym zakresie, automatycznie uruchamia początek biegu terminu na wniesienie odwołania. Takim terminem, zdaniem tego składu orzekającego, nie jest termin otwarcia ofert, chyba że Zamawiający w tym dniu dokonałby również oceny zasadności zastrzeżenia tajemnicy przedsiębiorstwa, co w praktyce wydaje się działaniem niewykonalnym. Jednocześnie Krajowa Izba Odwoławcza uznała, że ostatecznym terminem, od którego biegnie termin na wniesienie odwołania w tym zakresie, jest decyzja zamawiającego dotycząca wyboru i oceny ofert, gdyż ta decyzja kończy etap oceny ofert, a tym samym również oceny zasadności zastrzeżenia informacji oferty jako tajemnicy przedsiębiorstwa. W ocenie Krajowej Izby Odwoławczej zasadnym jest stwierdzenie, że nie jest możliwe wskazanie dla wszystkich stanów faktycznych jednolitej zasady co do określenia terminu, od którego należy liczyć rozpoczęcie biegu terminu na wniesienie odwołania w omawianym zakresie, a kwestia ta winna każdorazowo podlegać indywidualnej ocenie.



Dyrektywa 2016/943 w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa)

W dniu 5 lipca 2016 r. weszła w życie dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskaniem, wykorzystywaniem. Celem dyrektywy 2016/943 jest harmonizacja przepisów państw członkowskich Unii Europejskiej poprzez wprowadzenie spójnej definicji *tajemnicy przedsiębiorstwa* oraz środków ochrony cywilnoprawnej w przypadku bezprawnego naruszenia prawa do tajemnicy przedsiębiorstwa. Z motywu 14 dyrektywy wynika obowiązek przyjęcia jednolitej definicji tajemnicy przedsiębiorstwa bez ograniczania zakresu ochrony przed przywłaszczeniem. Taka definicja powinna zatem być sformułowana w sposób uwzględniający *know-how*, informacje handlowe i informacje techniczne w przypadkach, w których istnieje zarówno uzasadniony interes w utrzymaniu poufności, jak i uzasadnione oczekiwanie, że taka poufność zostanie zachowana. Ponadto taki know-how lub informacje powinny mieć rzeczywistą lub potencjalną wartość handlową. Takie informacje lub know-how powinny być uważane za informacje o wartości handlowej wówczas, gdy przykładowo ich bezprawne pozyskiwanie, wykorzystywanie lub ujawnianie może spowodować szkody dla interesów osoby, która zgodnie z prawem sprawuje nad nimi kontrolę, szkodząc jej naukowemu lub technicznemu potencjałowi, interesom gospodarczym lub finansowym, pozycji strategicznej lub zdolności do konkurowania.

Definicja tajemnicy handlowej nie obejmuje nieistotnych informacji oraz doświadczeń i umiejętności, które zostały zdobyte przez pracowników w trakcie prowadzenia normalnej pracy, a także nie obejmuje informacji, które są powszechnie znane lub łatwo dostępne

osobom z kręgów zajmujących się zwykle tym rodzajem informacji.

Dyrektywa 2016/943 wprowadziła jednolitą definicję tajemnicy przedsiębiorstwa, czego potrzebę podkreślono także w jej preambule. Zgodnie z art. 2 pkt 1 dyrektywy „tajemnica przedsiębiorstwa” oznacza informacje, które spełniają wszystkie następujące wymogi:

- są poufne w tym sensie, że jako całość lub w szczególnym zestawie i zbiorze ich elementów nie są ogólnie znane lub łatwo dostępne dla osób z kręgów, które zwykle zajmują się tym rodzajem informacji;
- mają wartość handlową dlatego, że są objęte tajemnicą;
- poddane zostały przez osobę, która zgodnie z prawem sprawuje nad nimi kontrolę, rozsądnym, w danych okolicznościach, działaniom dla utrzymania ich w tajemnicy.

W art. 4 dyrektywy 2016/943 wyszczególniono, kiedy pozyskiwanie, wykorzystywanie i ujawnianie tajemnicy przedsiębiorstwa jest bezprawne.

Pozyskanie tajemnicy przedsiębiorstwa bez zgody posiadacza tajemnicy przedsiębiorstwa uznaje się za bezprawne zawsze wówczas, gdy wynika ono z nieuprawnionego dostępu, przywłaszczenia lub kopiowania wszelkich dokumentów, przedmiotów, materiałów, substancji lub plików elektronicznych, nad którymi zgodnie z prawem posiadacz tajemnicy przedsiębiorstwa sprawuje kontrolę, zawierających tajemnicę przedsiębiorstwa lub pozwalających na wywnioskowanie tajemnicy przedsiębiorstwa lub z każdego innego postępowania, które uznaje się w danych okolicznościach za sprzeczne z uczciwymi praktykami handlowymi (art. 4 ust. 2 dyrektywy 2016/943).

Zgodnie z art. 4 ust. 3 dyrektywy 2016/943 wykorzystanie lub ujawnienie tajemnicy przedsiębiorstwa uznaje się za bezprawne w każdym przypadku, gdy bez zgody posiadacza tajemnicy przedsiębiorstwa dokonuje go osoba, która spełnia którykolwiek z następujących warunków:

- pozyskała bezprawnie tajemnicę przedsiębiorstwa;
- naruszyła umowę o poufności lub inny obowiązek nieujawniania tajemnicy przedsiębiorstwa;

- naruszyła umowny lub inny obowiązek ograniczenia wykorzystywania tajemnicy przedsiębiorstwa.

Pozyskiwanie, wykorzystywanie lub ujawnianie tajemnicy przedsiębiorstwa uznaje się również za bezprawne zawsze wówczas, gdy w momencie pozyskiwania, wykorzystywania lub ujawniania osoba wie lub powinna w danych okolicznościach wiedzieć, że tajemnicę przedsiębiorstwa uzyskano bezpośrednio lub pośrednio od innej osoby wykorzystującej lub ujawniającej tajemnicę przedsiębiorstwa bezprawnie w rozumieniu art. 4 ust. 3 dyrektywy 2016/943.

Produkcję, oferowanie lub wprowadzanie do obrotu towarów stanowiących naruszenie oraz przywóz, wywóz bądź przechowywanie towarów stanowiących naruszenie do takich celów uznaje się również za bezprawne wykorzystywanie tajemnicy przedsiębiorstwa, jeżeli osoba dokonująca tych czynności wiedziała lub powinna była w danych okolicznościach wiedzieć o bezprawnym wykorzystywaniu w rozumieniu art. 4 ust. 3 dyrektywy 2016/943, tajemnicy przedsiębiorstwa.

Przepis art. 5 lit. b) dyrektywy 2016/943 zapewnia uchylenie zastosowania środków ogólnych w związku z naruszeniem tajemnicy przedsiębiorstwa, jeżeli zostało ono dokonane na skutek działalności sygnalizacyjnej („Państwa członkowskie zapewniają, by wniosek o zastosowanie środków ogólnych, procedur i środków prawnych przewidzianych w niniejszej dyrektywie został oddalony, jeżeli domniemane pozyskanie, wykorzystywanie lub ujawnienie tajemnicy przedsiębiorstwa miało miejsce dla ujawnienia nieprawidłowości, uchybienia lub działania z naruszeniem prawa, pod warunkiem że pozwany działał w celu ochrony ogólnego interesu publicznego.”).

Józef Edmund Nowicki

właściciel kancelarii CONEXIS
Zamówienia publiczne, wieloletni ekspert zewnętrzny w zakresie kontroli zamówień współfinansowanych z budżetu Unii Europejskiej. Autor komentarzy do ustawy – Prawo zamówień publicznych i ponad 500 publikacji z dziedziny prawa zamówień publicznych

Sprzedaż internetowa na nowych zasadach

Poradnik dla małych i średnich przedsiębiorców

Marta Czeladzka

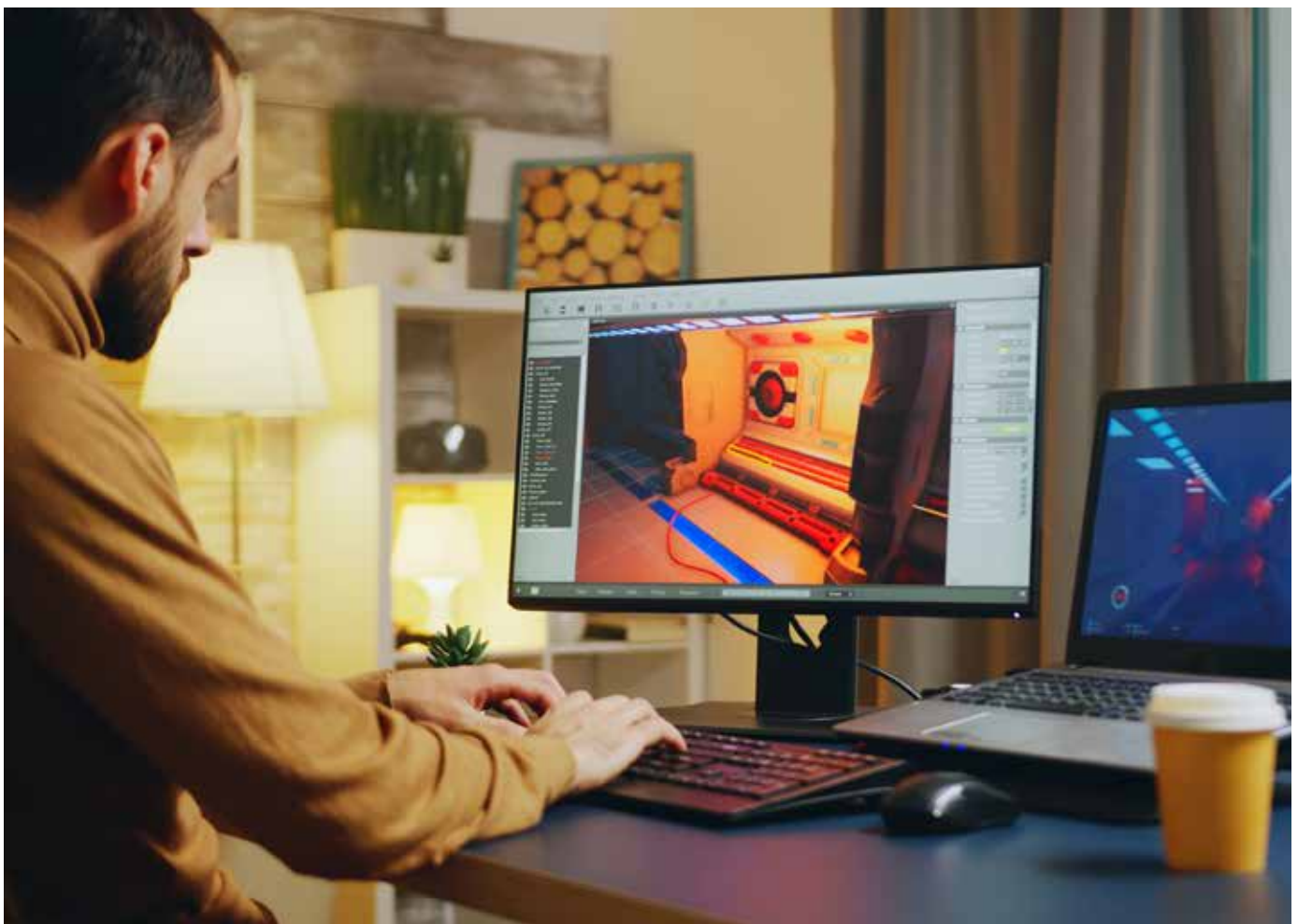
Sprzedaż internetowa to bardzo szerokie pojęcie. Uogólniając można przyjąć, że odnosi się ono do prowadzenia sklepu internetowego. Przedmiotem sprzedaży w sieci mogą być bardzo różnorodne produkty – zarówno tradycyjne towary, takie jak żywność, odzież, buty, kosmetyki, sprzęt elektroniczny czy sprzęt RTV/AGD, jak i mniej oczywiste dobra, np. treści cyfrowe (filmy czy muzyka). Jednocześnie część towarów jest wyjęta spod obrotu w internecie, np. alkohol, militaria czy konta mailowe. Przepisy prawa nie ustanawiają szczególnych, odrębnych zasad dla rozpoczęcia sprzedaży internetowej. Aby prowadzić sklep w internecie, nie są konieczne specjalne zezwolenia administracyjnoprawne czy wpisy do rejestru. Jednak ustawodawca, poza

ogólnymi przepisami ochronnymi, odnoszącymi się do umów zawieranych przez konsumenta z przedsiębiorcą w okolicznościach typowych (zwłaszcza w lokalu przedsiębiorstwa), ustanawia szczególny reżim prawny ochrony konsumenta, dotyczący umów zawieranych poza lokalem przedsiębiorstwa (np. w drodze akwizycji) lub na odległość, w szczególności za pośrednictwem internetu. Instrumenty ochronne, jakie przyznaje konsumentom w takich sytuacjach ustawodawstwo unijne, a w ślad za nim polska ustawa o prawach konsumenta¹ (dalej: „u.p.k.”), to głównie obowiązek dostarczenia konsumentowi przez przedsiębiorcę pewnych informacji na etapie przedkontraktowym (tzw. obowiązki informacyjne) oraz przyznanie konsumentowi

uprawnienia do rezygnacji z zawartej umowy (prawo odstąpienia od umowy, tzw. „prawo do namysłu”).

Planowane zmiany

W nadchodzącym czasie dojdzie do sporych zmian w obszarze ochrony praw konsumenta, które odczują zwłaszcza przedsiębiorcy trudniący się sprzedażą przez internet. W 2022 r. wejdą bowiem w życie planowane w obecnej chwili przepisy nowelizujące ustawy konsumenckie, w tym zwłaszcza u.p.k., wdrażające do polskiego porządku prawnego szereg konsumenckich dyrektyw unijnych uchwalonych w 2019 r.



Chodzi w szczególności o dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (tzw. „dyrektywa cyfrowa”)² oraz powiązaną z nią dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/771 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów sprzedaży towarów, zmieniającą rozporządzenie (UE) 2017/2394 oraz dyrektywę 2009/22/WE i uchylającą dyrektywę 1999/44/WE (tzw. „dyrektywa towarowa”)³. Dyrektywy są częścią Strategii jednolitego rynku cyfrowego dla Europy⁴, ogłoszonej przez Komisję Europejską w dniu 6 maja 2015 r., której fundamentalnym założeniem jest stworzenie wolnego, jednolitego rynku online dla towarów, osób, usług oraz kapitału w Europie⁵. Głównym celem obu dyrektyw jest wzmocnienie potencjału transgranicznego handlu elektronicznego w Unii Europejskiej przez umożliwienie konsumentom lepszego dostępu do treści cyfrowych i usług cyfrowych oraz ułatwienie przedsiębiorcom dostarczania tych treści i usług, przy jednoczesnym zapewnieniu wysokiego poziomu ochrony konsumentów. W założeniu ustawodawcy unijnego obie dyrektywy mają się przy tym wzajemnie uzupełniać. Dyrektywa 2019/770 (dyrektywa cyfrowa) znajduje zastosowanie do umów o dostarczanie treści cyfrowych lub usług cyfrowych. Z kolei dyrektywa 2019/771 (dyrektywa towarowa) ujednocila w ramach Unii Europejskiej regulację dotyczącą rękopisów konsumenckiej, która powiązana jest z umowami sprzedaży towarów, w tym towarów z elementami cyfrowymi⁶.

Od kiedy zmiany?

Dyrektywy cyfrowa i towarowa weszły w życie 11 czerwca 2019 r. Państwa członkowskie zostały zobowiązane do przyjęcia przepisów niezbędnych do wykonania dyrektyw do dnia 1 lipca 2021 r. oraz do stosowania tych przepisów począwszy od dnia 1 stycznia 2022 r. W Polsce projekt ustawy wdrażającej dyrektywy („ustawa o zmianie ustawy o prawach konsumenta oraz ustawy – Kodeks cywilny”) ukazał się w dniu 27 grudnia 2020 r., w którym został skierowany do uzgodnień międzyresortowych, konsultacji publicznych i opiniowania.

Na chwilę zakończenia prac nad niniejszą publikacją ustawa wdrażająca nie została jeszcze uchwalona. Dostępna jest natomiast wersja projektu ustawy nowelizującej datowana na dzień 2 listopada 2021 r., która została opublikowana na stronach Rządowego Centrum Legislacji w dniu 19 listopada 2021 r. Wersja ta uwzględnia szereg uwag zgłoszonych w trakcie konsultacji publicznych. Wszelkie spostrzeżenia na temat wdrożenia dyrektyw cyfrowej i towarowej w Polsce, jakie będą czynione w niniejszej publikacji, odnoszą się do wspomnianego, najnowszego projektu ustawy wdrażającej (...).

Zakres podmiotowy dwóch dyrektyw

Art. 1 dyrektywy cyfrowej, a także art. 1 dyrektywy towarowej, wskazują, że przepisy ustanowione w tych dyrektywach dotyczą umów zawartych pomiędzy konsumentem a przedsiębiorcą. Dyrektywom podlegają więc jedynie umowy zawierane w stosunkach *business-to-consumer* (B2C), przepisy dyrektyw nie obejmują natomiast relacji *business-to-business* (B2B), ani tym bardziej relacji *peer-to-peer* (P2P). Regulacja taka jest wynikiem przyjęcia w ramach konsultacji poprzedzających uchwalenie dyrektyw opinii, iż specyfika umów, w tym umów o dostarczanie treści lub usług cyfrowych, zawieranych między przedsiębiorcami (ani tym bardziej pomiędzy samymi konsumentami) nie prowadzi do zakłóceń w swobodnym przepływie towarów i usług na rynku wewnętrznym, wobec czego nie zdecydowano się objąć tych relacji dyrektywami 2019/770 oraz 2019/771⁷.

W związku z przyjętym przez ustawodawcę unijnego zakresem podmiotowym stosowania omawianych dyrektyw należy zadać pytanie o rozumienie pojęć konsumenta i przedsiębiorcy. Z pomocą przychodzi same omawiane akty prawne, które zawierają stosowne definicje w tym zakresie. Zgodnie z art. 2 pkt 6) dyrektywy cyfrowej jako **konsumenta** należy rozumieć osobę fizyczną, która w przypadku umów objętych tą dyrektywą (tj. umów o dostarczanie treści i usług cyfrowych) działa w celach niezwiązanych ze swoją działalnością

handlową, gospodarczą, rzemieślniczą ani wykonywaniem wolnego zawodu. Definicja o analogicznej treści znajduje się w art. 2 pkt 2) dyrektywy towarowej. Z kolei **przedsiębiorcę** obie dyrektywy definiują jako osobę fizyczną lub prawną, niezależnie od tego, czy jest to podmiot publiczny, czy prywatny, która w przypadku umów objętych dyrektywą działa – w tym również za pośrednictwem innej osoby działającej w imieniu tej osoby fizycznej lub prawnej lub na rzecz tej osoby – w celach związanych z działalnością handlową, gospodarczą, rzemieślniczą tej osoby lub wykonywaniem wolnego zawodu przez tę osobę (art. 2 pkt 5) dyrektywy cyfrowej oraz art. 2 pkt 3) dyrektywy towarowej, przy czym ten ostatni posługuje się terminem „sprzedawca”. Warto dodać, że definicje konsumenta i przedsiębiorcy zawarte w dyrektywach 2019/770 oraz 2019/771 są tożsame z definicją tych pojęć zawartych w dyrektywie 2011/83/UE (odpowiednio art. 2 pkt 1) oraz art. 2 pkt 2) tej dyrektywy).

Zakres przedmiotowy dyrektywy cyfrowej

Zgodnie z art. 3 ust. 1 dyrektywy cyfrowej jej przepisy stosuje się do umów, na podstawie których przedsiębiorca dostarcza lub zobowiązuje się dostarczyć konsumentowi treści cyfrowe lub usługę cyfrową, a konsument płaci cenę lub zobowiązuje się do jej zapłaty. Zgodnie z art. 3 ust. 2 dyrektywy obejmuje ona także sytuacje, gdy umowa dotyczy treści cyfrowych lub usługi cyfrowej tworzonej zgodnie ze wskazówkami klienta, w tym oprogramowania dostosowanego do potrzeb konsumenta (motyw 26 dyrektywy). Ponadto dyrektywa stosuje się do nośników materialnych, które służą wyłącznie jako nośnik treści cyfrowych (art. 3 ust. 3 dyrektywy).

Jak podano w motywie 19 dyrektywy, w celu uwzględnienia szybkiego rozwoju technologicznego oraz zachowania nieulegającego dezaktualizacji charakteru pojęcia treści cyfrowych lub usługi cyfrowej, dyrektywa obejmuje swoim zakresem m.in. programy komputerowe, aplikacje, pliki wideo,

pliki audio, pliki muzyczne, gry elektroniczne, e-booki lub inne publikacje elektroniczne, w tym np. pliki elektroniczne potrzebne do drukowania towarów w 3D⁸, a także usługi cyfrowe pozwalające na tworzenie, przetwarzanie lub przechowywanie danych w postaci cyfrowej bądź dostęp do nich, w tym usługi typu „oprogramowanie jako usługa”, takie jak udostępnianie treści wideo i audio (np. YouTube) oraz innego rodzaju hosting plików, edycja tekstu lub gry oferowane w chmurze obliczeniowej i w mediach społecznościowych (np. Facebook). Z uwagi na to, że treści cyfrowe lub usługa cyfrowa mogą być dostarczane na różne sposoby, tj. przekazywane na nośniku materialnym, pobierane przez konsumentów na ich własne urządzenia, przesyłane strumieniowo, w formie dostępu do treści cyfrowych przechowywanych w chmurze obliczeniowej lub dostępu do mediów społecznościowych, dyrektywa ma zastosowanie **niezależnie od nośnika** użytego

do przekazania bądź do udostępnienia treści cyfrowych lub usługi cyfrowej.

Przepisy dyrektywy stosuje się również wtedy, gdy przedsiębiorca dostarcza lub zobowiązuje się dostarczyć konsumentowi treści cyfrowe lub usługę cyfrową, a konsument dostarcza lub zobowiązuje się dostarczyć przedsiębiorcy **dane osobowe**, z wyjątkiem przypadków, gdy dane osobowe dostarczone przez konsumenta są przetwarzane przez przedsiębiorcę wyłącznie w celu dostarczenia treści cyfrowych lub usługi cyfrowej zgodnie z dyrektywą lub w celu umożliwienia przedsiębiorcy spełnienia wymogów prawnych, którym on podlega, a przedsiębiorca nie przetwarza tych danych do żadnych innych celów. Rozwiązanie to zostało uwzględnione także w przepisach dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/2161 z dnia 27 listopada 2019 r. zmieniającej dyrektywę Rady 93/13/EWG i dyrektywę Parlamentu Europejskiego i Rady 98/6/WE, 2005/29/WE oraz 2011/83/UE

w odniesieniu do lepszego egzekwowania i unowocześnienia unijnych przepisów dotyczących ochrony konsumenta (dalej: „dyrektywa Omnibus” lub „dyrektywa 2019/2161), gdzie dostarczanie danych osobowych przez konsumenta jest traktowane jako środek płatności (...)”⁹.

Zakres przedmiotowy dyrektywy towarowej

Art. 3 ust. 1 dyrektywy towarowej stanowi, że dyrektywę tę stosuje się do umów sprzedaży pomiędzy konsumentem a sprzedawcą¹⁰. Art. 3 ust. 2 precyzuje, że dotyczy to także umów pomiędzy sprzedawcą a konsumentem dotyczących dostarczania towarów, które mają zostać wytworzone lub wyprodukowane w przyszłości.

Dyrektywa 2019/771 na potrzeby związane z jej stosowaniem wprowadza



definicję pojęć „umowa sprzedaży” oraz „towar”. Zgodnie z art. 2 pkt 1) dyrektywy umową sprzedaży w jej rozumieniu jest umowa, na podstawie której sprzedawca (przedsiębiorca) przenosi lub zobowiązuje się do przeniesienia na konsumenta własności towarów, a konsument płaci lub zobowiązuje się do zapłacenia ich ceny. Towary w rozumieniu dyrektywy (art. 2 pkt 5) dyrektywy) oznaczają:

- a) materialne rzeczy ruchome; wodę, gaz i energię elektryczną należy uznać za towary w rozumieniu niniejszej dyrektywy, w przypadku gdy są oferowane do sprzedaży w ograniczonej objętości lub w określonej ilości;
- b) materialne rzeczy ruchome, które zawierają w sobie treści cyfrowe lub usługę cyfrową lub są z takimi treściami lub usługą wzajemnie połączone w taki sposób, że brak tych treści cyfrowych lub usługi cyfrowej uniemożliwiłby tym towarom pełnienie ich funkcji (zwane dalej „**towarami z elementami cyfrowymi**”).

Należy odnotować, że tożsama definicja towaru z elementami cyfrowymi została zamieszczona w art. 2 pkt 3) dyrektywy cyfrowej.

Podobnie jak dyrektywa cyfrowa, dyrektywa towarowa reguluje jedynie niektóre aspekty umów sprzedaży towarów. W założeniu ustawodawcy europejskiego dyrektywa 2019/771 rozszerza przy tym ochronę konsumenta wynikającą z dyrektywy 2011/83/UE. Podczas gdy dyrektywa 2011/83/UE ustanawia przede wszystkim przepisy dotyczące wymogów w zakresie informacji przed zawarciem umowy, prawa odstąpienia od umowy w przypadku umów zawieranych na odległość lub umów zawieranych poza lokalem przedsiębiorstwa oraz warunków dostarczenia towarów oraz przenoszenia ryzyka, dyrektywa towarowa ustanawia dodatkowo zharmonizowane przepisy dotyczące zgodności towarów z umową, środki ochrony prawnej w przypadku braku zgodności z umową oraz zasady korzystania z tych środków.

Analogicznie jak ma to miejsce w przypadku dyrektywy cyfrowej, także dyrektywa towarowa wyłącza spod swojego zakresu kwestie dotyczące aspektów ogólnego prawa umów, takie jak przepisy dotyczące zawierania, skuteczności,

nieważności lub skutków umów, w tym konsekwencji rozwiązania umów oraz określonych aspektów dotyczących naprawy i wymiany w zakresie, w jakim kwestie te nie są regulowane w dyrektywie. Ponadto dyrektywa towarowa nie wpływa na swobodę pozostawienia konsumentom przez państwa członkowskie wyboru konkretnego środka ochrony prawnej, jeżeli brak zgodności towaru z umową ujawni się po jego dostarczeniu, w okresie nieprzekraczającym 30 dni, oraz na przepisy krajowe niespecyficzne dla umów konsumentskich przewidujące szczególne środki ochrony prawnej w przypadku pewnych rodzajów wad, które nie były widoczne w momencie zawierania umowy sprzedaży. Podobnie państwa członkowskie zachowują swobodę co do sposobu uregulowania prawa stron umowy do wstrzymania się z wykonywaniem swoich zobowiązań lub ich części do czasu wywiązania się przez drugą stronę z jej zobowiązań, w tym warunków i zasad wstrzymania się z zapłatą ceny przez konsumenta, a ponadto prawa konsumenta do odszkodowania za szkody poniesione w wyniku naruszenia dyrektywy przez sprzedawcę (...).

Zmiany w UPK

Projekt ustawy implementującej dyrektywy cyfrową i towarową do polskiego prawa wprowadza do u.p.k. definicję umowy o dostarczenie treści cyfrowej lub usługi cyfrowej (planowany art. 2 pkt 2 a) u.p.k.). Definicja ta miałaby brzmieć następująco: umowa o dostarczenie treści cyfrowej lub usługi cyfrowej – umowa, na podstawie której przedsiębiorca zobowiązuje się dostarczyć konsumentowi treść cyfrową lub usługę cyfrową, w tym również wykonaną według wskazówek konsumenta, a konsument zobowiązuje się zapłacić cenę lub dostarczyć dane osobowe, chyba że dane osobowe dostarczone przez konsumenta są przetwarzane przez przedsiębiorcę wyłącznie w celu:

- a) dostarczenia treści cyfrowej lub usługi cyfrowej,
- b) poprawy bezpieczeństwa, kompatybilności lub interoperacyjności oprogramowania oferowanego na podstawie wolnej i otwartej licencji,
- c) wykonania obowiązku ustawowego. Jest to jednocześnie jedyny przepis

ustawy implementującej odnoszący się bezpośrednio do kwestii umów o dostarczanie treści cyfrowych i usług cyfrowych dostarczanych konsumentowi w zamian za dane osobowe.

W ramach konsultacji publicznych projektu ustawy zwrócono uwagę, że planowany sposób wdrożenia przepisów dyrektywy cyfrowej dotyczących umowy o dostarczanie treści cyfrowej lub usługi cyfrowej w zamian za dane osobowe może być niezgodny z dyrektywą 2019/770. Jak wskazano w uwagach Prezesa Urzędu Ochrony Konkurencji i Konsumentów¹¹ projekt zmian przedstawionych przez ustawodawcę właściwie nie reguluje w ogóle możliwości stosowania przepisów u.p.k. do treści cyfrowych i usług cyfrowych dostarczanych w zamian za dane osobowe, czyli nie realizuje jednego z głównych rozwiązań dyrektywy cyfrowej. Zamieszczenie w słowniczku ustawy definicji umowy o dostarczanie treści cyfrowej lub usługi cyfrowej nie może być bowiem traktowane jako przepis merytoryczny regulujący zakres stosowania norm ustawy (...).

Obowiązki w zakresie integracji treści cyfrowych lub usługi cyfrowej

Dyrektywa cyfrowa wprowadza obowiązki przedsiębiorcy związane z integracją treści cyfrowych lub usługi cyfrowej ze sprzętem komputerowym i oprogramowaniem konsumenta. Integracja, zgodnie z art. 2 pkt 4) dyrektywy 2019/770 oznacza połączenie treści cyfrowych lub usługi cyfrowej z elementami środowiska cyfrowego konsumenta i włączanie ich do tych elementów, tak aby możliwe było korzystanie z treści cyfrowych lub usługi cyfrowej zgodnie z wymogami zgodności z umową przewidzianymi w dyrektywie. Niewłaściwa integracja może stać się podstawą odpowiedzialności przedsiębiorcy za brak zgodności z umową. Zgodnie z art. 9 dyrektywy może to mieć miejsce w sytuacji, gdy niewłaściwa integracja treści cyfrowych lub usługi cyfrowej została przeprowadzona przez przedsiębiorcę lub na jego odpowiedzialność. Ponadto przedsiębiorca może być odpowiedzialny, kiedy niewłaściwa integracja jest

Konsument to osoba fizyczna, która w przypadku umów objętych dyrektywą działa w celach niezwiązanych ze swoją działalnością handlową, gospodarczą, rzemieślniczą ani wykonywaniem wolnego zawodu.

wynikiem działań samego konsumenta, jednak przyczyną takiej niewłaściwej integracji są błędy w instrukcji integracji dostarczonej przez przedsiębiorcę. Jak wskazuje motyw 52 dyrektywy cyfrowej, za takie błędy można uznać niekompletność lub niejasność instrukcji, które sprawiły, że przeciętny konsument nie był w stanie dokonać integracji w sposób prawidłowy (...).

Obowiązek dokonywania zmian treści lub usług cyfrowych

Art. 8 ust. 4 dyrektywy cyfrowej wskazuje, że w przypadku, gdy umowa przewiduje dostarczanie treści cyfrowych lub usługi cyfrowej w sposób ciągły przez określony czas, treści cyfrowe lub usługi cyfrowe muszą pozostawać zgodne z umową przez cały ten czas. Oznacza to, że przedsiębiorca ma obowiązek dokonywać zmian tych treści lub usług cyfrowych w zakresie koniecznym do utrzymania zgodności z umową. Jednak przedsiębiorca może dokonywać – jednostronnie – zmian treści cyfrowych lub usługi cyfrowej także w zakresie wykraczającym ponad to, co jest niezbędne do zachowania zgodności tych treści lub usługi z umową, o ile są spełnione następujące warunki, wskazane w art. 19 dyrektywy. Po pierwsze, umowa o dostarczanie treści cyfrowych lub usługi cyfrowej musi przewidywać taką możliwość i określać uzasadnioną przyczynę do dokonania takiej zmiany. Oznacza to, że ewentualna zmiana nie może być podyktowana wyłącznie wolą przedsiębiorcy, musi zaistnieć dla niej pewien obiektywny powód. Motyw 75 dyrektywy wyjaśnia, że takim uzasadnionym powodem mogą być sytuacje, w których zmiana jest niezbędna

do dostosowania treści cyfrowych lub usługi cyfrowej do nowego środowiska technicznego lub do wzrostu liczby użytkowników lub z innych istotnych względów eksploatacyjnych. Takie zmiany są zresztą często korzystne dla konsumenta, ponieważ stanowią ulepszenie treści cyfrowych lub usługi cyfrowej. Drugim warunkiem do dokonania przez przedsiębiorcę jednostronnej, pozytywnej dla konsumenta zmiany treści cyfrowych lub usługi cyfrowej, jest to, aby zmiana nie obciążała konsumenta dodatkowymi kosztami oraz, aby konsument został poinformowany o zmianie w sposób jasny i zrozumiały.

Może zdarzyć się również tak, że planowana przez przedsiębiorcę zmiana treści lub usługi cyfrowej ma potencjał, aby wpłynąć na korzystanie z tych treści lub usługi przez konsumenta lub dostęp do treści lub usługi negatywnie, w sposób bardziej niż tylko nieistotny. Dla oceny, czy planowana przez przedsiębiorcę zmiana dotycząca treści lub usługi cyfrowej ma charakter pozytywny czy negatywny dla konsumenta, powinno się brać pod uwagę zobiektywizowane kryteria uwzględniające charakter i przeznaczenie treści cyfrowych lub usługi cyfrowej oraz jakość, funkcjonalność, kompatybilność i inne podstawowe cechy, których oczekuje się od treści cyfrowych lub usług cyfrowych tego samego rodzaju (motyw 75 dyrektywy cyfrowej). Jako przykład można podać sytuację, w której konsument ma zawartą z przedsiębiorcą umowę zapewniającą mu dostęp do platformy z grami komputerowymi, w trakcie trwania której przedsiębiorca znacznie ogranicza ilość dostępnych do wykorzystania gier. W takim przypadku przedsiębiorca zobowiązany jest do przekazania konsumentowi informacji, które umożliwią mu podjęcie decyzji co do dalszego trwania umowy. Informacje te muszą zostać przekazane konsumentowi z odpowiednim wyprzedzeniem, na trwałym nośniku (tj. np. na płycie CD czy DVD, ale także pocztą elektroniczną bądź tradycyjną – chodzi o to, by konsument mógł w każdej chwili odtworzyć treść otrzymanych informacji) i obejmować wiadomości o właściwościach i terminie dokonania zmiany, a także o prawie do rozwiązania umowy lub o możliwości zachowania treści cyfrowych lub usługi cyfrowej bez planowanej przez przedsiębiorcę zmiany.

Zakres informacji, do przekazania których jest zobowiązany przedsiębiorca, wskazuje jednocześnie, jakie prawa przysługują konsumentowi na wypadek planowanych przez przedsiębiorcę zmian treści lub usługi cyfrowej o charakterze negatywnym. Konsument ma tutaj dwie możliwości. Po pierwsze, może on zachować się biernie i zgodzić w ten sposób na planowaną przez przedsiębiorcę zmianę oraz dalsze trwanie umowy. Po drugie, konsument może zachować się aktywnie i rozwiązać umowę – w takim wypadku konsument jest zobowiązany do złożenia oświadczenia o rozwiązaniu umowy w terminie 30 dni od dnia otrzymania informacji lub od momentu zmiany przez przedsiębiorcę treści cyfrowych lub usługi cyfrowej, w zależności od tego, które z tych zdarzeń nastąpiło później. Należy mieć jednak na uwadze, że konsument nie będzie miał prawa do rozwiązania umowy, jeżeli przedsiębiorca umożliwi mu, bez obciążania go dodatkowymi kosztami, zachowanie treści cyfrowych lub usługi cyfrowej bez zmiany, a treści cyfrowe lub usługa cyfrowa pozostają zgodne z umową.

Należy ocenić, że rozwiązanie zaproponowane przez ustawodawcę europejskiego w art. 19 dyrektywy jest racjonalne i służy zapewnieniu elastyczności dla stron umowy o dostarczanie treści lub usług cyfrowych w obliczu nieustannych zmian zachodzących na rynku cyfrowym, przy jednoczesnym zachowaniu równowagi kontraktowej stron. Z jednej strony bowiem przedsiębiorca ma możliwość dokonywania modyfikacji treści lub usług w czasie trwania umowy z konsumentem, co w założeniu ma służyć dalszemu rozwojowi tych treści i usług, z drugiej strony zaś konsument ma zapewnione prawo zakończenia stosunku umownego w sytuacji, gdyby nie akceptował zaproponowanych przez przedsiębiorcę zmian.

Omawiane zmiany do polskiego prawodawstwa wdrażane są planowanymi przepisami art. 43m oraz art. 43n u.p.k. Przepisy te w zasadzie skrupulatnie oddają tekst art. 19 dyrektywy 2019/770, z uwzględnieniem dostosowanego do polskich instytucji prawa cywilnego nazewnictwa w postaci prawa wypowiedzenia umowy przysługującego konsumentowi na wypadek braku akceptacji

zaproponowanych przez przedsiębiorcę zmian w dostarczanej treści lub usłudze cyfrowej (...).

Środki ochrony prawnej w przypadku niedostarczenia treści cyfrowych lub usługi cyfrowej

Jak wskazuje art. 11 ust. 1 dyrektywy 2019/770 przedsiębiorca odpowiada za niedostarczenie konsumentowi treści lub usługi cyfrowej zgodnie z art. 5 dyrektywy. Środki prawne przysługujące konsumentowi w przypadku niedostarczenia przez przedsiębiorcę treści cyfrowych lub usługi cyfrowej opisuje art. 13 dyrektywy. Zgodnie z jego treścią konsumentowi, który nie otrzymał od przedsiębiorcy treści lub usług cyfrowych niezwłocznie po zawarciu umowy lub w terminie określonym przez strony w umowie, przysługuje prawo do rozwiązania umowy po uprzednim wezwaniu przedsiębiorcy do spełnienia świadczenia (art. 13 ust. 1 dyrektywy). Zasadą jest zatem, że konsument wzywa

przedsiębiorcę do dostarczenia treści lub usług, uzgadniając z nim ewentualnie w wyraźny sposób dodatkowy termin zrealizowania świadczenia.

Od powyższej reguły dyrektywa przewiduje dwa wyjątki, umożliwiając konsumentowi natychmiastowe rozwiązanie umowy. Są to przypadki, gdy, po pierwsze, przedsiębiorca oświadczył bądź też z okoliczności jasno wynika, iż nie dostarczy treści cyfrowej lub usługi cyfrowej, i po drugie – gdy konsument i przedsiębiorca uzgodnili lub z okoliczności zawarcia umowy jasno wynika, że określony termin dostarczenia treści lub usługi cyfrowej ma dla konsumenta istotne znaczenie, a przedsiębiorca nie dostarczył treści lub usługi cyfrowej przed upływem tego terminu lub w tym terminie. Jedynie zatem w tych dwóch wskazanych sytuacjach konsument jest zwolniony z obowiązku dania przedsiębiorcy „drugiej szansy” i wzywania go do spełnienia świadczenia (...).

Marta Czeladzka

radca prawny, specjalizuje się w prawie własności intelektualnej, w tym zwłaszcza w prawie autorskim

oraz prawie nowych technologii; absolwentka studiów doktoranckich na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego oraz studiów LL.M w zakresie prawa porównawczego, europejskiego i międzynarodowego w Europejskim Instytucie Uniwersyteckim we Florencji; autorka publikacji z zakresu prawa autorskiego

Artykuł jest fragmentem publikacji pt. „Sprzedaż internetowa na nowych zasadach. Poradnik dla małych i średnich przedsiębiorców”, która została wydana przez ośrodek Enterprise Europe Network przy Polskiej Agencji Rozwoju Przedsiębiorczości

¹ Ustawa z dnia 30 maja 2014 r. o prawach konsumenta, Dz.U.2020.287 t.j. z dnia 2020.02.21.

² Dz.U.U.E.L.2019.136.1 z dnia 2019.05.22.

³ Dz.U.U.E.L.2019.136.28 z dnia 2019.05.22.

⁴ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Strategia jednolitego rynku cyfrowego dla Europy (COM(2015) 192 final. Strategia jednolitego rynku cyfrowego została przyjęta przez Komisję Europejską jako dokument prezentujący planowane prace Unii Europejskiej w obszarze cyfrowym do 2020 r. Ogólnym jej zamierzeniem jest wyeliminowanie barier, które utrudniają rozwój cyfrowy Europy. Strategia oparta została na trzech filarach, których celem jest utworzenie jednolitego rynku cyfrowego: zapewnienia konsumentom i przedsiębiorstwom łatwiejszego dostępu do towarów i usług cyfrowych w całej Europie, stworzenia odpowiednich i równych warunków funkcjonowania umożliwiających rozkwit sieci cyfrowych i innowacyjnych usług oraz maksymalizacji potencjału wzrostu gospodarki cyfrowej.

⁵ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: *Strategia jednolitego rynku cyfrowego dla Europy*, COM(2015) 192 final.

⁶ Pierwotnie projekt dyrektywy 2019/771 ograniczał zakres jej stosowania do umów sprzedaży towarów przez internet lub w inny sposób na odległość. Jednak w toku prac legislacyjnych zdecydowano się na ujednolicenie zakresu stosowania tego aktu prawnego do umów zawieranych online i offline. Było to rozwiązanie spójne z treścią projektu rozporządzenia Parlamentu i Rady w sprawie wspólnych europejskich przepisów dotyczących sprzedaży z 11 października 2011 r. (rozporządzenie CESL), które ostatecznie nie zostało przyjęte.

⁷ Wniosek Komisji Europejskiej *Dyrektywa Parlamentu Europejskiego i Rady w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych*, COM(2015) 634 final, oraz Wniosek Komisji Europejskiej *Dyrektywa Parlamentu Europejskiego i Rady w sprawie niektórych aspektów umów sprzedaży towarów zawieranych przez internet lub w inny sposób na odległość*, COM(2015) 635 final.

⁸ Dyrektywa cyfrowa nie ma jednak zastosowania do praw i obowiązków związanych z towarami wytworzonymi przy użyciu technologii drukowania 3D.

⁹ Por. szerzej rozdział III.

¹⁰ Por. uwagi wyżej co do pojęcia przedsiębiorcy.

¹¹ Uwagi Prezesa Urzędu Ochrony Konkurencji i Konsumentów do projektu ustawy o zmianie ustawy o prawach konsumenta oraz ustawy – Kodeks cywilny, datowane na dzień 26 listopada 2021 r., dostępne pod adresem: <https://legislacja.rcl.gov.pl/projekt/12341810/katalog/12752766#12752766>.



Oferty współpracy

Chiny

Firma będąca spółką zależną chińskiego producenta pociągów poszukuje dostawców powłok antykorozyjnych do stosowania na wewnętrznych powierzchniach zbiorników wody pitnej i zbiorników odpływowych w pociągach. Preferowana formą współpracy to umowa dostawy. Numer referencyjny BRCN20211125001

Francja

Francuski producent luksusowych dodatków skórzanych poszukuje dostawców alternatywnych surowców pochodzenia roślinnego. Oferowane produkty powinny być wytrzymałe i biodegradowalne, dostępne w rolkach w różnych kolorach. Dostawy będą realizowane bezpośrednio do warsztatu we Francji dwa razy w roku – w lutym i wrześniu.

Numer referencyjny BRFR20210916001
Doświadczona francuska firma oferuje pomoc w promocji i dystrybucji na tamtejszym rynku takich produktów, jak wyposażenie domu, produkty dla dzieci, sportowe i do ogrodu. Oferowane wyroby powinny być przyjazne dla środowiska i produkowane w zrównoważony sposób. Numer referencyjny BRFR20211118001

Grecja

Grecka firma logistyczna o zasięgu globalnym nawiąże współpracę z producentami kartonów i plastikowych kopert kurierskich. Kartony powinny spełniać następujące wymogi: konstrukcja z dwóch warstw, dostosowane do przewożenia dużych ciężarów i zgodne ze standardami FEFCO, w trzech wariantach rozmiarów (24,4 x 14,5 x 5 cm; 24,9 x 17,5 x 7,9 cm; 33,1 x 24,1 x 10,4 cm). Koperty kurierskie powinny mieć wymiary 35 x 24 cm. Numer referencyjny BRGR20211122001

Holandia

Holenderska hurtownia mebli biurowych jest zainteresowana nawiązaniem współpracy z producentami blatów

do biurek i stołów obiadowych. Przedsiębiorstwo oferuje zawarcie umów produkcyjnych oraz umów agencyjnych. Numer referencyjny BRNL20211202001

Niemcy

Niemiecka firma specjalizująca się w dystrybucji produktów fryzjerskich poszukuje producenta przyborów łazienkowych oraz akcesoriów do włosów i masażu. Firma w ciągu ostatnich 35 lat urosła do rangi wiodącego europejskiego dystrybutora artykułów do włosów. W celu poszerzenia swego asortymentu „Made in Europe”, poszukuje europejskich dostawców m.in. akcesoriów łazienkowych (dozowniki mydła, mydelniczki, kubki, lustra), szczotek i grzebieni do włosów, pędzli kosmetycznych i akcesoriów do masażu. Numer referencyjny BRDE20210823001

Rumunia

Rumuński startup poszukuje dostawców wysokiej jakości tkanin – bawełna i softshell – oraz dodatków wykorzystywanych przy produkcji odzieży – zamki błyskawiczne, sznurki, zatrzaski, gumki. Działalność firmy koncentruje się na produkcji odzieży casualowej i sportowej dla kobiet, mężczyzn i dzieci. Projekty produktów powstają we własnym dziale projektowym firmy. Numer referencyjny BRRO20211015001

Rumuńska firma zajmująca się projektowaniem architektury poszukuje partnerów specjalizujących się w planowaniu oraz projektowaniu budynków i domów. Firma ta jest aktywna na rynku krajowym od ponad 15 lat. Obecnie poszukuje partnerów, którzy zajmują się projektowaniem architektonicznym, w tym ekologicznych projektów budowlanych, aranżacją wnętrz, a także doradztwem w zakresie działalności architektonicznej, nadzorem budowlanym i wszystkimi procedurami dotyczącymi pozwoleń na budowę. Numer referencyjny BRRO20210622001

Słowacja

Firma ze Słowacji zajmująca się sprzedażą suplementów diety na bazie enzymu laktazy za pośrednictwem ponad 2.500 słowackich i czeskich aptek poszukuje dostawców enzymu laktazy w postaci tabletek lub kapsułek o zawartości 9 000 FCC/lu i więcej na tabletkę/kapsułkę. Firma poszukuje rzetelnego dostawcy i jest zainteresowana długoterminową współpracą. Numer referencyjny BRSK20211006001

Ukraina

Ukraiński producent weterynaryjnych dodatków do pasz oraz szerokiej gamy leków weterynaryjnych dla drobiu, bydła, koni i zwierząt domowych zainteresowany jest poszerzeniem asortymentu w ramach umowy o świadczenie usług dystrybucyjnych. Numer referencyjny BRUA20211103001

Wielka Brytania

Brytyjska firma działająca w obszarze ochrony zdrowia poszukuje dostawców/producentów małych połączanych magnesów ferrytowych i neodymowych, które mają na celu łagodzenie objawów menopauzy. Firma poszukuje w szczególności: połączanych magnesów neodymowych N35 – 3800 Gs lub połączanych magnesów ferrytowych 800 Gs. Wymiary: średnica 5mm, grubość 2 mm. Połączana warstwa musi być wykonana z hipoalergicznego 14-karatowego złota. Numer referencyjny BRUK20211105001

Brytyjska firma specjalizująca się w sprzedaży odzieży dla osób podnoszących ciężary poszukuje nowych doświadczonych producentów już oferowanych produktów oraz planowanych do wprowadzenia do oferty akcesoriów do CrossFit i sprzętu rehabilitacyjnego. Numer referencyjny BRUK20211018001

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

Zapraszamy do skorzystania z naszych usług

WWW.EEN.ORG.PL

Na naszym portalu znajdziecie informacje dotyczące takich zagadnień jak:

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