NR 6 - PAŹDZIERNIK 2020

NEWSLETTER

IT-TECH

W NUMERZE:

- Dekompilacja programu komputerowego przed TSUE (sprawa C-13/20)
- Ograniczenie możliwości wyboru prawa obcego dla umów licencyjnych
- Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa
- Projekt nowej przesłanki wykluczenia z postępowania o udzielenie zamówienia związanej z cyberbezpieczeństwem (Nowe PZP)
- Dopuszczalność uchylenia tajemnicy telekomunikacyjnej na potrzeby dochodzenia ochrony dóbr osobistych (uchwała SN III CZP 78/19)
- MF ogłosił interpretację ogólną ws. 50% kosztów
- Propozycja nowej ulgi na robotyzację

Traple Konarski Podrecki & Wspólnicy

TKP

Dekompilacja programu komputerowego przed TSUE (sprawa C-13/20)

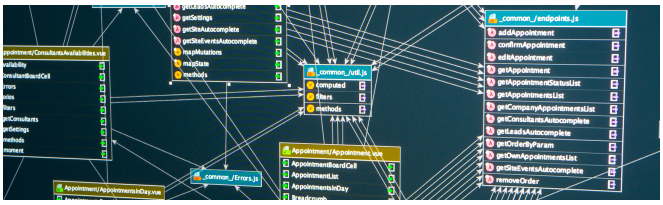
r.pr. Agnieszka Wachowska

Już wkrótce Trybunału Sprawiedliwości UE (”TS UE”) będzie musiał pochylić się nad zakresem uprawnień tzw. legalnego dysponenta (użytkownika) programu komputerowego. Do rozpoznania trafiła bowiem sprawa ciekawa sprawa[2] dotycząca zagadnienia zakresu dozwolonej legalnej dekompilacji programu komputerowego na gruncie przepisów dyrektywy ws. programów komputerowych („dyrektywa 2009/24/WE”)[2].

Tło i okoliczności faktyczne sprawy C-13/20

Sprawa dotyczy sporu między zamawiającym system, a wykonawcą dostarczającym jego komponenty. Służba ds. doboru i dysponowania kadrami administracji publicznej (dalej „Selorem”) używa systemu umożliwiającego rejestrację kandydatur zgłoszonych za pośrednictwem Internetu. Spółka Top System (dalej „Top System”) rozwija natomiast oprogramowanie komputerowe i w ramach działalności opracowała ona swój własny „Top System Framework” (zwany dalej „TSF”). Następnie, aby zapewnić Selorowi dostęp do kandydatur składanych za pośrednictwem Internetu, Top System opracował na jego zamówienie różnego rodzaju nowe aplikacje (zwane dalej „aplikacjami Seloru”), w tym „Selor Web Access” (SWA). Aplikacje Seloru składają się, z jednej strony, z komponentów zaprojektowanych „na miarę”, w odpowiedzi na potrzeby i wymagania Seloru, a, z drugiej strony, z komponentów pozyskanych z TSF.

Współpraca pomiędzy Top System i Selorem trwała przez wiele lat. Jednakże z powodu braku usunięcia wielu usterek, Selor zaczął samodzielnie poszukiwać rozwiązania problemu. Z analizy powołanego w sprawie biegłego wynika, że Selor dokonał dekompilacji bibliotek wynikowych Top System, zmierzając do odtworzenia ich kodów źródłowych. Selor przyznaje, że dokonał dekompilacji części TSF, której funkcje zostały zintegrowane z aplikacjami Seloru, aby wyłączyć jedną z jego funkcji, która okazała się wadliwa.



Kluczowe kwestie sporne

W wyniku powyższych działań Selor Top System wystąpił przeciwko Królestwu Belgii z powództwem mającym na celu w szczególności:

- stwierdzenie, że dokonana przez Selor dekompilacja TSF wiąże się z naruszeniem przysługujących Top System praw wyłącznych do utworu, a także
- zobowiązanie Królestwa Belgii do naprawienia szkody poniesionej przez Top System w wyniku dekompilacji i powielenia kodów źródłowych TSF.

Sąd apelacyjny wskazał, że Top System nie dostarczył całości kodów źródłowych dla aplikacji Seloru. W konsekwencji, zdaniem sądu, wobec niewywiązywania się z umowy, Selor powinien był jednak wezwać Top System do przekazania kodów źródłowych, a nie – dokonywać samodzielnej dekompilacji kodu wynikowego.

Zaniechawszy wezwania Top System do dostarczenia kodów źródłowych na podstawie umowy, Selor umyślnie wyszedł poza sferę stosunków umownych. Selor powinien zatem wykazać, że był uprawniony do dokonania dekompilacji przez obowiązujące przepisy prawa. W związku z tym, zdaniem sądu apelacyjnego, dla prawidłowego rozstrzygnię-cia sprawy **kluczowe jest ustalenie, czy dekompilacja całości lub części programu komputerowego stanowi jed-ną z czynności przewidzianych w art. 4 lit. a) i b) dyrekty-wy 91/250, których uprawniony użytkownik programu może dokonać w celu poprawienia występujących w nim błędów**.

[1] Sprawa zarejestrowana pod sygnaturą C-13/20 gdzie stroną wnosząca środek odwoławczy jest Top System SA przeciwko Królestwu Belgii, http://curia.europa.eu/juris/documents.jsf?oqp=&for=&mat=or&lgrec=en&jge=&td=%3BALL&jur=C%2CT%2CF&num=C13%252F20&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&1, dostęp: 5.09.2020 r.

[2] Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych (Dz.U.UE.L. 2009.111.16 z dnia 5 maja 2009 r.), dalej jako „dyrektywa 2009/24/WE”.

Mając to na uwadze, sąd apelacyjny zadał TS UE pytania:

- czy artykuł 5 ust. 1 dyrektywy 2009/24/WE należy interpretować w ten sposób, że zezwala on uprawnionemu nabywcy programu komputerowego na dokonanie dekompilacji całości lub części tego programu, jeżeli dekompilacja ta jest konieczna, aby pozwolić mu na poprawienie błędów mających wpływ na funkcjonowanie tego programu, również w przypadku, gdy poprawka ta polega na wyłączeniu funkcji mającej wpływ na poprawne funkcjonowanie aplikacji, której program ten jest częścią?
- jeśli odpowiedź na powyższe jest twierdząca - czy muszą zostać spełnione warunki określone w art. 6 dyrektywy lub jakieś inne warunki celem zapewnienia, że dekompilacja będzie zgodna z prawem?

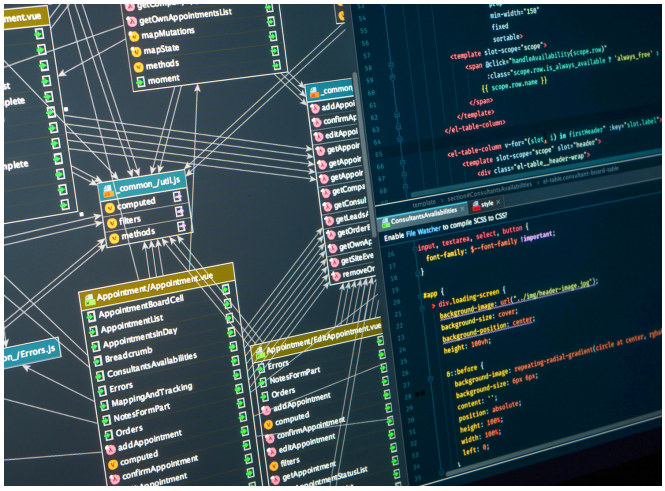
Praktyczne znaczenie rozstrzygnięcia

Mając na uwadze stan faktyczny sporu i zadane pytania, TS UE będzie musiał przesądzić niezwykle ciekawe kwestie, aby rozpoznać sprawę – a zwłaszcza określić:

- czym jest dekompilacja programu komputerowego na gruncie dyrektywy 2009/24/WE,
- jak należy rozumieć pojęcie tłumaczenia i zmiany oprogramowania w rozumieniu art. 4 ust. 1 lit b dyrektywy 2009/24/WE,
- jak należy rozumieć użyte w art. 5 dyrektywy 2009/24/WE sformułowanie *„konieczność użycia programu przez uprawnionego nabywcę”*.

Kluczową kwestią będzie jednak określenie relacji art. 5 i 6 dyrektywy 2009/24/WE, a konkretnie przesądzenie tego, czy dozwolona dekompilacja oprogramowania możliwa jest jedynie na podstawie i w warunkach przewidzianych w art. 6 dyrektywy 2009/24/WE (czyli na potrzeby otrzymania informacji koniecznych do osiągnięcia interoperacyjności niezależnie stworzonego programu komputerowego z innymi programami), czy też dekompilacja taka możliwa jest również na podstawie art. 5 ust. 1 dyrektywy 2009/24/WE, czyli w sytuacji, kiedy jej dokonanie byłoby konieczne do użycia programu przez uprawnionego nabywcę zgodnie z zamierzonym celem, włącznie z poprawianiem błędów.

Rozstrzygnięcie sporu będzie miało praktyczne znaczenie dla wszystkich nabywców systemów informatycznych, których elementy nie zostały dostarczone w formie kodu źródłowego oraz co do których nie zapewniono szerokich uprawnień pozwalających na ingerencję w oprogramowanie. W takich wypadkach, zamawiający zwykle korzystają z usług wykonawców zapewniających usługi serwisowe czy utrzymaniowe.



Rozstrzygnięcie TS UE powinno przesądzić, czy usuwanie błędów w oprogramowaniu wraz z towarzyszącą mu uprzednią dekompilacją może być dokonane samodzielnie przez zamawiającego, bez zgody wykonawcy – twórcy takiego oprogramowania.

Warto przy tym również podkreślić, że będzie to pierwszy wyrok Trybunału w przedmiocie zakresu uprawnień legalnego użytkownika oprogramowania. W zależności od rozstrzygnięcia Trybunału wyrok ten może częściowo przyczynić się do szerszego lub węższego korzystania z tych uprawnień, a przynajmniej weryfikacji obecnego podejścia do utrzymania systemów posiadanych przez zamawiających. Na sam wyrok przyjdzie jeszcze poczekać – sprawa trafiła do TSUE w styczniu 2020 r., a średni czas trwania postępowania wynosi ok. 15 miesięcy[3]. Zaznaczyć przy tym należy, że wydaje się, że wyrok ten nie będzie miał jednocześnie praktycznego przełożenia na rosnący dynamicznie sposób udostępniania programów komputerowych w modelu SaaS, czyli w chmurze obliczeniowej – w takim bowiem przypadku użytkownik nie otrzymuje kopii kodu wynikowego, na której mógłby dokonać dekompilacji. Powyższe pokazuje jednocześnie, jak regulacje dyrektywy 2009/24/WE, tworzone na przełomie lat 80 i 90 XX w. są przestarzałe i nieodpowiadające potrzebom oraz wyzwaniom współczesnego obrotu oprogramowania i jak bardzo przydałyby nowa, dopasowana do współczesnych potrzeb – regulacja w tym zakresie.

Zainteresowanych szerszą analizą prawną kwestii dekompilacji zapraszamy do lektury artykułu mec. Wachowskiej pt. *„Dekompilacja programu komputerowego na potrzeby dokonania jego niezbędnej modyfikacji – rozważania przed wyrokiem TSUE w sprawie C-13/20”*, który ukaże się w najbliższym Dodatku do Monitora Prawniczego – Prawo nowych technologii - a po publikacji będzie również dostępny w systemie informacji prawnej Legalis.

[3] W 2019 r. średni czas trwania postępowania przed TS UE wyniósł 14,4 miesiąca - https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/qdaq20001pln_002.pdf

Ograniczenie możliwości wyboru prawa obcego dla umów licencyjnych

Aleksander Elmerych

Spółki działające w ramach jednej grupy kapitałowej często dążą do jak największego ujednolicenia zasad prowadzenia działalności w różnych państwach. Jest to podejście jak najbardziej uzasadnione i racjonalne, ponieważ pozwala na redukcję kosztów i zapewnia dobrą organizację oraz możliwość przepływu informacji pomiędzy poszczególnymi spółkami.

W branży IT dobrym przykładem ujednolicania działalności poszczególnych spółek wchodzących w skład grupy kapitałowej są umowy licencyjne na korzystanie z tego samego produktu. Aby zminimalizować rozbieżności dotyczące zakresu udzielanych licencji oraz zasad wykonywania uprawnień z tytułu licencji, które mogą wynikać z różnic w ustawodawstwach poszczególnych państw, umowy licencyjne zawierane przez te spółki poddawane są zazwyczaj prawu jednego, wybranego wcześniej kraju. Dzięki temu ważność oraz skutki zastosowania postanowień tych umów oceniane są według takich samych przepisów i nie wymagają każdorazowego dostosowania w zależności od kraju, w którym licencja jest udzielana. Warto jednak mieć na uwadze to, że nie zawsze wybór prawa dokonany w umowie będzie w pełni skuteczny.

Możliwość wyboru prawa dla umów, w tym umów licencyjnych, wynika z postanowień art. 3 unijnego rozporządzenia Rzym I[1], które zastępuje w tym zakresie polską ustawę Prawo prywatne międzynarodowe[2]. Zgodnie z wyrażoną w nim zasadą swobody wyboru prawa, strony umowy mogą wybrać jako prawo właściwe dla umowy prawo dowolnego państwa, niezależnie od tego, czy jest ono członkiem Unii Europejskiej. W takim przypadku całość umowy licencyjnej, w tym skuteczność poszczególnych jej postanowień dotyczących zakresu licencji, okresu, na który została udzielona, możliwości wypowiedzenia czy zasad odpowiedzialności stron, należy oceniać z perspektywy prawa państwa, które strony wskazały jako właściwe. Co istotne, wybór prawa nie musi zostać dokonany w żadnej szczególnej formie – nie ma zatem przeszkód, by zawrzeć taką klauzulę w umowie zawieranej na odległość, na przykład przez Internet.

Ze szczególną sytuacją będziemy mieli jednak do czynienia w przypadku, gdy zarówno podmiot udzielający licencji jak i klient, który nabywa prawo do korzystania z produktu, mają swoją siedzibę w Polsce i nie zachodzą żadne inne okoliczności sprawy związane z państwem obcym. W takiej sytuacji wybór prawa dokonany przez strony zostanie na mocy art. 3 ust. 3 rozporządzenia Rzym I istotnie ograniczony i nie będzie mógł wyłączyć zastosowania przepisów bezwzględnie obowiązujących prawa polskiego. Nawet zatem w przypadku ustanowienia umowy licencyjnej na prawie obcym (dla przykładu na prawie niemieckim), postanowienia tej umowy będą musiały być w pierwszej kolejności zgodne z polskimi przepisami bezwzględnie obowiązującymi, a dopiero następnie będą oceniane z perspektywy prawa niemieckiego pod kątem skuteczności, ważności oraz sposobu wykładni.

W praktyce problematyczne może okazać się ustalenie, które przepisy polskiego porządku prawnego należy uznać za bezwzględnie obowiązujące, a które za względnie obowiązujące. Ustawodawca nie zawsze bowiem przesądza wprost o bezwzględnie obowiązującym charakterze poszczególnych norm, co potwierdził Sąd Najwyższy w wyroku z dnia 20 marca 2014 r., sygn. II CSK 290/13, wskazując, że: „*Jako ius cogens należy traktować nie tylko te przepisy, z których redakcji wyraźnie wynika ich bezwzględnie obowiązujący charakter, lecz także te, których treść jest wyrazem zasady moralnej, wyraża intencję ochrony porządku publicznego lub odzwierciedla istotny cel społeczno-gospodarczy*.” Wydaje się, że w przypadku umów.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 593/2008 z dnia 17 czerwca 2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I) (Dz. U. UE. L. z 2008 r. Nr 177, str. 6 z późn. zm.).
[2] Ustawa z dnia 4 lutego 2011 r. - Prawo prywatne międzynarodowe (t.j. Dz. U. z 2015 r. poz. 1792).

licencyjnych jako ograniczające możliwość wyboru prawa na gruncie art. 3 ust. 3 rozporządzenia Rzym I należy uznać m.in. polskie przepisy dotyczące wiążącego charakteru wzorców umownych (art. 384 k.c.), zakresu dopuszczalnego ograniczenia odpowiedzialności stron (art. 473 §2 k.c.), możliwości wypowiedzenia zobowiązań bezterminowych o charakterze ciągłym (art. 365(1) k.c.), czy wymogu formy pisemnej dla licencji wyłącznych (art. 67 ust. 5 pr. aut.). Mimo zatem wybrania prawa obcego jako prawa właściwego dla umowy licencyjnej, jej postanowienia będą musiały być zgodne z polskimi przepisami bezwzględnie obowiązującymi których przykłady wskazano powyżej. Przykładowo - nie będą skuteczne postanowienia:

- wyłączające odpowiedzialność jednej ze stron za szkody wyrządzone drugiej stronie umowy umyślnie,
- przyznające moc wiążącą wzorcowi umownemu, który nie został drugiej stronie doręczony lub udostępniony w formie elektronicznej, przed zawarciem umowy.

Nieważna będzie również umowa licencji wyłącznej zawarta bez zachowania formy pisemnej.

Podsumowując, strony umowy licencyjnej mogą co do zasady zlokalizować ją na prawie dowolnie wybranego przez siebie państwa. Należy mieć jednak na względzie, że w przypadku, gdy oba podmioty mają swoją siedzibę na terytorium Polski i w sprawie nie występuje żaden inny element zagraniczny, mimo dokonanego wyboru prawa umowa będzie musiała być zgodna z polskimi przepisami bezwzględnie obowiązującymi. Dlatego też niezwykle istotne jest zweryfikowanie wykorzystywanych wzorów umów pod tym kątem – może się bowiem okazać, że w przypadku ewentualnego sporu sądowego część ich postanowień zostanie uznana za nieważne.

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa

r.pr. Joanna Jastrząb

Zapowiadana od dłuższego czasu nowelizacja Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: „ustawa o KSC") niedługo stanie się faktem – 7 września 2020 r. do konsultacji publicznych przekazano jej projekt. Chociaż projekt przepisów nie zmienia podstawowych zagadnień regulowanych ustawą (np. obowiązków operatorów usług kluczowych czy dostawców usług cyfrowych), to propozycja nowelizacji spotkała się z dużym zainteresowaniem przedsiębiorców – na prośbę zrzeszających ich organizacji branżowych Ministerstwo Cyfryzacji przedłużyło termin konsultacji publicznych do 6 października 2020 r.

Najważniejsze proponowane zmiany

Poniżej znajduje się podsumowanie najważniejszych zmian przedstawionych w ramach projektu nowelizacji.

1. Objęcie regulacją ustawy o KSC także przedsiębiorców komunikacji elektronicznej.

Obecnie art. 1 ust. 2 pkt 1 ustawy o KSC wprost wyłącza jej zastosowanie wobec przedsiębiorców telekomunikacyjnych w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów.

Projektowana regulacja przewiduje natomiast uchylenie tego przepisu i włączenie w krajowy system cyberbezpieczeństwa przedsiębiorców komunikacji elektronicznej. Wyjaśnienia wymaga, że ta propozycja powiązana jest z projektem regulacji Prawa komunikacji elektronicznej – ustawy implementującej Europejski Kodeks Łączności Elektronicznej, która ma zastąpić obecną regulację Prawa telekomunikacyjnego. Więcej na ten temat pisaliśmy w poprzednim wydaniu newslettera, dostępnym pod tym linkiem (s. 2 newslettera).

Nowelizacja ustawy o KSC zakłada dodanie nowego rozdziału 4a, który ma określać obowiązki przedsiębiorców komunikacji elektronicznej, również w zakresie obsługi incydentów telekomunikacyjnych. Warto podkreślić, że obowiązki zostały przewidziane w sposób jednolity dla wszystkich przedsiębiorców komunikacji elektronicznej, niezależnie od tego, jakie usługi świadczą (dotyczy to więc zarówno przedsiębiorców telekomunikacyjnych, jak i podmiotów świadczących usługę komunikacji interpersonalnej niewykorzystującej numerów – np. usługi poczty elektronicznej).

Nowelizacja ustawy o KSC zakłada dodanie nowego rozdziału 4a, który ma określać obowiązki przedsiębiorców komunikacji elektronicznej, również w zakresie obsługi incydentów telekomunikacyjnych. Warto podkreślić, że obowiązki zostały przewidziane w sposób jednolity dla wszystkich przedsiębiorców komunikacji elektronicznej, niezależnie od tego, jakie usługi świadczą (dotyczy to więc zarówno przedsiębiorców telekomunikacyjnych, jak i podmiotów świadczących usługę komunikacji interpersonalnej niewykorzystującej numerów – np. usługi poczty elektronicznej).

2. Nadanie Kolegium kompetencji w sprawie oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa (art. 66a ustawy o KSC).

Na mocy nowelizacji istotne kompetencje ma otrzymać Kolegium ds. cyberbezpieczeństwa, czyli organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa, działający przy Radzie Ministrów (art. 64 ustawy o KSC). Kolegium uprawnione będzie do przeprowadzania oceny ryzyka dostawców sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa.

Kompetencja ta stanowi implementację unijnego Toolboxa 5G, dokumentu wydanego w styczniu 2020 r. przez NIS Cooperation Group, zawierającego zalecenia skierowane do państw członkowskich w zakresie przeciwdziałania ryzykom dla integralności i bezpieczeństwa sieci nowej generacji w Europie. Warto jednak podkreślić, że projektowany przepis przyznający tę kompetencję nie odnosi się wyłącznie do sprzętu lub oprogramowania w zakresie 5G.

Zgodnie z art. 66a ust. 5 ustawy o KSC ocena Kolegium może stwierdzać:

- wysokie ryzyko – jeżeli dostawca sprzętu lub oprogramowania stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa i zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe;
- umiarkowane ryzyko – jeżeli dostawca sprzętu lub oprogramowania stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa, a zmniejszenie poziomu tego ryzyka możliwe jest przez wdrożenie środków technicznych lub organizacyjnych;
- niskie ryzyko – jeżeli dostawca sprzętu lub oprogramowania stanowi niewielkie zagrożenie dla cyberbezpieczeństwa państwa;
- brak zidentyfikowanego poziomu ryzyka – jeżeli nie stwierdzono zagrożenia dla cyberbezpieczeństwa państwa lub poziom tego zagrożenia jest znikomy.

Ocena Kolegium przekłada się na możliwość wykorzystania sprzętu lub oprogramowania przez podmioty krajowego systemu cyberbezpieczeństwa (art. 66b ustawy o KSC):

- w przypadku umiarkowanego ryzyka podmioty te nie wprowadzają do użytkowania sprzętu, oprogramowania ani usług określonych w ocenie danego dostawcy, mogą jednak kontynuować dotychczasowe użytkowanie posiadanego już sprzętu i oprogramowania lub nadal korzystać z usług;
- w przypadku wysokiego ryzyka podmioty te nie tylko nie wprowadzają do użytkowania sprzętu, oprogramowania ani usług określonych w ocenie danego dostawcy, lecz także wycofują z użytkowania sprzęt, oprogramowanie i usługi nie później niż w ciągu 5 lat od dnia ogłoszenia komunikatu o ocenie.

Warto też podkreślić, że powyższe przepisy mogą istotnie wpłynąć na rynek zamówień publicznych – o czym piszemy w artykule pt. *Projekt nowej przesłanki wykluczenia z postępowania o udzielenie zamówienia związanej z cyberbezpieczeństwem do Nowego PZP*.

3. Uregulowanie w ramach ustawy ISAC – centrum wymiany i analizy informacji (art. 4a ustawy o KSC).
Nowelizacja zakłada uregulowanie funkcjonowania ISAC – specjalistycznych organizacji zapewniających współpracę i wymianę informacji w zakresie incydentów, zagrożeń, podatności oraz dobrych praktyk w zakresie ochrony cyberbezpieczeństwa. Organizacje takie z powodzeniem funkcjonują na świecie i w Europie, dotychczas nie utworzono natomiast żadnej takiej polskiej organizacji, wskazując brak przepisów w tym zakresie jako jedną z barier. Temat ISAC przybliżaliśmy już na blogu: artykuł dostępny pod tym linkiem.

4. Uregulowanie w ustawie wprost zasad funkcjonowania SOC (zespołu pełniącego funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie) – art. 14 ustawy o KSC.
Na mocy nowelizacji uszczegółowione mają zostać przepisy dot. realizacji obowiązków przez operatorów usług kluczowych. Dotychczas art. 14 zakładał ich realizację przez podmiot wyspecjalizowany w drodze outsourcingu lub przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo. Nowelizacja precyzuje tę zasadę, podkreślając, że obowiązki ma realizować SOC, czyli operacyjne centrum bezpieczeństwa – wewnętrzne lub zapewnione przez podmiot świadczący usługi z zakresu cyberbezpieczeństwa.

Nowelizacja zakłada także stworzenie wykazu SOC, który będzie m.in. wskazywał podmioty prowadzące SOC oraz podmioty, na rzecz których SOC realizuje zadania. Wykaz ten nie będzie ogólnodostępny – wgląd do niego otrzymają jedynie podmioty wskazane w ustawie.

5. Uszczegółowienie przepisów dot. CSIRT sektorowych (art. 44 ustawy o KSC).
Nowelizacja zakłada także zmiany umożliwiające zwiększenie roli CSIRT sektorowych – i motywujące organy właściwe do ich utworzenia. Dotychczas powołano jeden taki zespół: Sektorowy Zespół Cyberbezpieczeństwa dla Sektora Bankowości i Infrastruktury Rynków Finansowych (CSIRT KNF). Zespół został zresztą powołany w lipcu 2020 r., a więc stosunkowo niedawno.

Podsumowanie

Opublikowany projekt nowelizacji wzbudził kontrowersje zwłaszcza z uwagi na:

1. Włączenie przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa – dotychczas regulacje dot. bezpieczeństwa zostały ujęte w projekcie ustawy Prawo komunikacji elektronicznej, przedsiębiorcy obawiają się więc braku spójności między przepisami i szerokim zakresem regulacji, obejmującym wszystkich przedsiębiorców komunikacji elektronicznej.
2. Kompetencję Kolegium do oceny ryzyka dostawców – wskazuje się, że regulacja może prowadzić do jednostronnej i subiektywnej oceny z powodu nieprecyzyjności i lakoniczności przepisów. Kontrowersje budzi także ograniczony zakres możliwości odwołania się od dokonanej oceny (tylko dostawcy, którzy uzyskali ocenę „wysokie ryzyko") i organ rozpatrujący odwołanie – organem tym ma być Kolegium, które samo dokonało oceny.

Pozostałe zmiany odpowiadają natomiast na potrzeby zgłaszane przez podmioty krajowego systemu cyberbezpieczeństwa i mają stymulować tworzenie branżowych, wyspecjalizowanych organizacji, mających wspierać te podmioty w ochronie cyberbezpieczeństwa.

Można się spodziewać, że przedstawiony projekt ulegnie zmianie ze względu na wiele uwag, które planują zgłosić branżowe organizacje. Ostateczny kształt przepisów poznamy jednak zapewne niedługo – projektodawcy zakładali, że nowelizacja wejdzie w życie, z pewnymi wyjątkami, 21 grudnia 2020 r.

Projekt nowej przesłanki wykluczenia z postępowania o udzielenie zamówienia związanej z cyberbezpieczeństwem (Nowe PZP)

r.pr. Tomasz Krzyżanowski

W dniu 7 września 2020 r. do konsultacji publicznych przekazano projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych (dalej: „Projekt" lub „Nowelizacja"). Projekt przewiduje między innymi zmianę w Ustawie z dnia 11 września 2019 r. – Prawo zamówień publicznych[1] (dalej: „Nowe PZP"), która może mieć doniosłe znaczenie dla rynku sprzętu i oprogramowania.

Zmiana w zakresie PZP polega na wprowadzeniu możliwości oceny przez zamawiających ryzyka dostawców sprzętu i oprogramowania i ich wykluczenia z postępowania o udzielenie zamówienia w przypadku stwierdzenia wysokiego poziomu ryzyka dotyczącego cyberbezpieczeństwa państwa.

Zmiana nr 1 – ocena poziomu ryzyka dostawcy sprzętu lub oprogramowania

Zmiana polega na uzupełnieniu treści art. 96 Nowego PZP poprzez dodanie art. 96 ust. 2 pkt 3 PZP. Przepis art. 96 dotyczy wymagań, jakie zamawiający mogą stawiać w dokumentacji przetargowej, związanych z realizacją zamówienia, tj.: „wymagania związane z realizacją zamówienia, które mogą obejmować aspekty gospodarcze, środowiskowe, społeczne, związane z innowacyjnością, zatrudnieniem lub zachowaniem poufnego charakteru informacji przekazanych wykonawcy w toku realizacji zamówienia". Wymagania mogą dotyczyć w szczególności aspektów określonych w ust. 2 pkt 1–2 tego przepisu. Nowelizacja dodaje pkt 3.

Wymagania, o których mowa w ust. 1, mogą dotyczyć w szczególności: „[...] 3) poziomu ryzyka, jaki stanowi dostawca sprzętu lub oprogramowania, stwierdzonego oceną, o której mowa w art. 66a ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369)".

Zamawiający będzie zatem uprawniony do stawiania wymagań w odniesieniu do dopuszczalnego ryzyka w zakresie cyberbezpieczeństwa dostawcy sprzętu lub oprogramowania. Należy przy tym podkreślić, że oceny nie dokonuje zamawiający, lecz tzw. Kolegium do Spraw Cyberbezpieczeństwa (dalej: „Kolegium") uregulowane w Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: „ustawa o KSC"). Z treści proponowanego przepisu wynika zatem, że zamawiający publiczny będzie mógł wyma-gać np. braku zidentyfikowanych poziomów ryzyk (Kolegium może stwierdzić ryzyko na poziomie: wysokim, umiarkowa-nym, niskim), eliminując tym samym z postępowania o udzielenie zamówienia dostawcę sprzętu i oprogramowania, w odniesieniu do którego Kolegium stwierdziło jakikolwiek poziom ryzyka zgodnie z projektowanymi przepisami ustawy o KSC.

Zmiana nr 2 – dodanie w Nowym PZP dodatkowej przesłanki wykluczenia z postępowania (fakultatywnej)

Dopuszczenie wymagania przez zamawiających publicznych oceny poziomu ryzyka w postępowaniu o udzielenie zamówienia powoduje konieczność określenia skutków niespełnienia tego wymagania przez wykonawcę. Nowe PZP ustanawia w art. 109 ust. 1 fakultatywne przesłanki wykluczenia z postępowania. Ich fakultatywność oznacza, że aby zamawiający mógł taką przesłankę zastosować, wszczynając postępowanie, musi wskazać tę podstawę wykluczenia w ogłoszeniu o zamówieniu lub w dokumentach zamówienia. W nowelizacji ustawodawca proponuje dodać nową przesłankę wykluczenia art. 109 ust. 1 pkt 11 Nowego PZP.

Z postępowania o udzielenie zamówienia zamawiający może wykluczyć wykonawcę: „[...] 11) który jest dostawcą sprzętu lub oprogramowania, wobec którego stwierdzono wysokie ryzyko, w ramach oceny, o której mowa w art. 66a ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa".

[1] Wejdzie w życie w dniu 1 stycznia 2021 r.

Z ww. przepisu wynika, że wykonawca, który jest dostawcą sprzętu lub oprogramowania, wobec którego zostanie stwierdzone wysokie ryzyko dla cyberbezpieczeństwa państwa zgodnie z projektowanym przepisem art. 66a ustawy o KSC, zostanie wykluczony z postępowania o udzielenie zamówienia publicznego, pod warunkiem że zamawiający przewidzi taką przesłankę w ogłoszeniu o zamówieniu lub w dokumentacji postępowania. Warto zatem zauważyć, że wykluczenie nie będzie mogło nastąpić (pomimo stwierdzenia wysokiego ryzyka przez Kolegium), jeżeli zamawiający nie przewidzi odpowiedniej przesłanki, wszczynając postępowanie o udzielenie zamówienia. Wykluczenie nie będzie też dotyczyło stwierdzenia ryzyka na poziomie umiarkowanym oraz niskim. W tym przypadku można rozważyć odrzucenie oferty na podstawie art. 226 ust. 1 pkt 16 lub 17 Nowego PZP, choć Projekt w tym zakresie milczy.

Nowelizacja przewiduje również zmianę w art. 110 ust. 2 w taki sposób, że „pkt 2–10" zastępuje się „pkt 2–11". Przepis ten dotyczy tzw. self-cleaningu. Oznacza to, że w przypadku nowej przesłanki wykluczenia wykonawca będzie mógł zastosować procedurę samooczyszczenia.

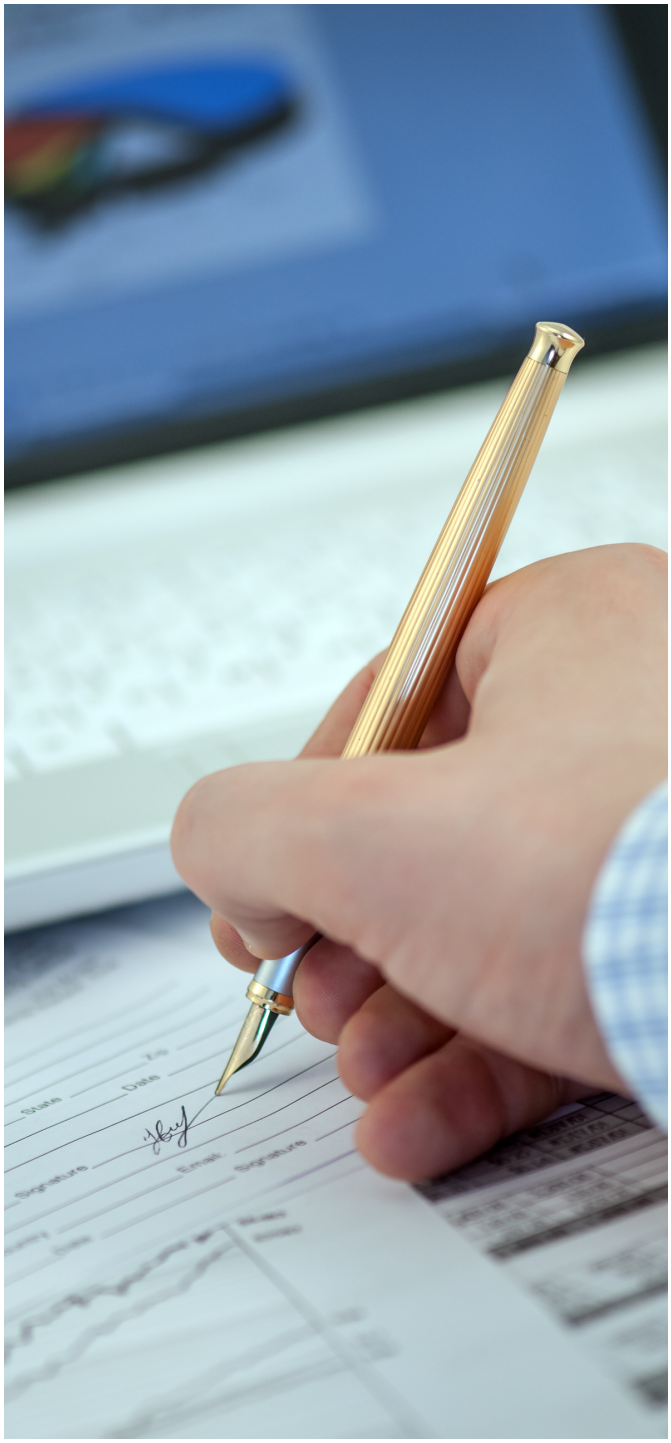
Ocena proponowanej zmiany i wątpliwości interpretacyjne

Projektowana zmiana Nowego PZP oraz ustawy o KSC może mieć znaczący wpływ na rynek ICT. Co do zasady należy tę zmianę ocenić pozytywnie, gdyż pozwoli ona wyeliminować z rynku zamówień publicznych wykonawców, którzy stanowią zagrożenie dla bezpieczeństwa państwa. W 2017 r. rząd Stanów Zjednoczonych zakazał wszystkim instytucjom rządowym korzystania z oprogramowania antywirusowego Kaspersky, stwierdzając, że może ono służyć rosyjskim służbom wywiadowczym. W Polsce instytucje publiczne, zwłaszcza opierające swe zakupy na procedurze ustawy – Prawo zamówień publicznych, nie mają bezpośrednich podstaw do wykluczania wykonawców w takich przypadkach lub do odrzucania ich ofert. Nowe przepisy mają tę lukę usunąć.

Konieczna będzie jednak duża ostrożność i rozwaga w stosowaniu nowych przepisów. Negatywna ocena Kolegium może bowiem spowodować wyeliminowanie z rynku określonego producenta lub znaczne utrudnienie mu działalności w związku ze spadkiem zaufania do jego produktów (nawet tych nieobjętych bezpośrednio oceną Kolegium).

Wejście w życie nowych przepisów

Zgodnie z Projektem zmiany dotyczące Nowego PZP wchodzą w życie z dniem 1 stycznia 2021 r.(tj. wraz z wejściem w życie ustawy PZP, którą zmieniają). Reszta ustawy wchodzi w życie wcześniej, tj. z dniem 21 grudnia 2020 r.
Szersza analiza wkrótce na blogu TKP.



Dopuszczalność uchylenia tajemnicy telekomunikacyjnej na potrzeby dochodzenia ochrony dóbr osobistych (uchwała SN III CZP 78/19)

r.pr. Magdalena Gąsowska-Paprota

Zgodnie z uchwałą Sądu Najwyższego (dalej: „SN") III CZP 78/19 z dnia 6 sierpnia 2020 r., w składzie trzech sędziów, sąd jest uprawniony – na podstawie art. 159 ust. 2 pkt 4 Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (dalej: „p.t.") – do zażądania od podmiotu związanego tajemnicą telekomunikacyjną informacji pozwalających zweryfikować twierdzenie powoda, że czynu naruszającego dobra osobiste dopuścił się pozwany w sprawie.

SN opowiedział się zatem za dopuszczalnością uchylenia tajemnicy telekomunikacyjnej na potrzeby toczącego się postępowania cywilnego. W postępowaniach związanych z ochroną dóbr osobistych, naruszanych poprzez treści zamieszczane w Internecie, dochodzenie roszczeń wymaga uzyskania odpowiednich danych o naruszeniu od operatora, chronionych tajemnicą telekomunikacyjną.

Zgodnie z art. 159 ust. 2 pkt 4 p.t. jedną z przesłanek dopuszczalności ujawnienia danych objętych tajemnicą telekomunikacyjną jest sytuacja, w której „będzie to konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi". Co również istotne, przepis art. 159 ust. 4 p.t. w brzmieniu wprowadzonym nowelizacją z 16 listopada 2012 r. tylko w postępowaniu karnym zezwala wprost na ujawnienie danych objętych tajemnicą telekomunikacyjną, ale już nie w postępowaniu cywilnym – ta regulacja miała na celu ograniczyć wykorzystanie przepisów o retencji danych do rozstrzygania spraw cywilnych.

Dotychczas w orzecznictwie Naczelnego Sądu Administracyjnego (dalej: „NSA") oraz sądów powszechnych prezentowane były rozbieżne poglądy dotyczące możliwości uchylenia tajemnicy telekomunikacyjnej na potrzeby toczącego się postępowania cywilnego. Za taką możliwością opowiadał się NSA w wyroku z dnia 21 lutego 2014 r. (I OSK 2324/12), wskazując, że „tajemnica telekomunikacyjna nie jest nieograniczona. Nie sięga przede wszystkim takich działań w sieci, które naruszają obowiązujący porządek prawny. Umożliwienie zatem podejmowania działań zmierzających do naprawy tej sytuacji, w tym też ścigania, i to nie tylko z urzędu, ale i w drodze prywatnego aktu oskarżenia czy domaganie się ochrony dóbr osobistych na drodze cywilnej, jest działaniem w granicach prawa, pozwalającym na zwolnienie z tej ochrony". Jednocześnie w wyrokach z 13 grudnia 2011 r. (I OSK 834/11, I OSK 1137/11) NSA stwierdził, że „w systemie prawa polskiego brakuje przepisu przyznającego osobie, której prawa autorskie zostały naruszone, prawa żądania od dostawcy usług internetowych udostępnienia danych osobowych użytkownika w celu skorzystania ze środka prawnego, mającego na celu ochronę tych praw w ramach postępowania cywilnego".

W przeciwną stronę zmierzało zaś podejście wyrażone w postanowieniu Sądu Apelacyjnego w Białymstoku z dnia 6 kwietnia 2011 r. (I ACz 279/11), który wskazał, że: „Ani prawo telekomunikacyjne, ani przepisy Kodeksu postępowania cywilnego nie stwarzają podstawy uzasadniającej wydanie przez sąd w sprawie cywilnej postanowienia dowodowego obligującego operatora do przetworzenia i przekazania temu sądowi danych objętych tajemnicą telekomu

Do postępowania w sprawie III CZP 78/19 przyłączył się Rzecznik Praw Obywatelskich, który wnosił, aby SN uznał ujawnienie tajemnicy telekomunikacyjnej w postępowaniu cywilnym za dopuszczalne, jeśli to właśnie treści z Internetu były podstawą naruszenia dóbr osobistych.

Uchwała SN w sprawie III CZP 78/19 jest istotnym krokiem w stronę przyznania prymatu możliwości dochodzenia ochrony dóbr osobistych nad ochroną prywatności m.in. w sieci. Uchwała zapewne wzbudzi kontrowersje na tle prezentowanego często przez operatorów telekomunikacyjnych poglądu o możliwości odmowy udzielenia przez informacji objętych tajemnicą telekomunikacyjną, których żąda sąd cywilny. Wskazuje się również, że może ona być w kontrze do założeń przyjmowanych przez Komisję Europejską, która potrzebę retencji danych telekomunikacyjnych wiąże przede wszystkim ze ściganiem przestępstw, w tym przeciwdziałaniem terroryzmowi.

Co istotne, w udostępnionym przez Ministerstwo Cyfryzacji 29 lipca 2020 r. projekcie ustawy Prawo komunikacji elektronicznej (dalej: „PKE"), która ma zastąpić p.t., nie przewidziano zasadniczych zmian w zakresie przepisów dotyczących tajemnicy telekomunikacyjnej, a treść obecnego art. 159 ust. 2 pkt 4 p.t. znaleźć się ma w formie niezmienionej w projektowanym art. 348 ust. 2 pkt 4 PKE.

Na moment publikacji tekstu, nie jest jeszcze dostępne uzasadnienie uchwały III CZP 78/19.

Interpretacja ogólna ws. 50% kosztów uzyskania przychodów

r.pr. Agnieszka Wachowska, r.pr. Joanna Jastrząb, Aleksander Elmerych

Ministerstwo Finansów 18 września 2020 r. opublikowało ogólną interpretację podatkową dotyczącą stosowania 50% kosztów uzyskania przychodów (nr DD3.8201.1.2018; dostępna: tutaj). Stało się to po ponad półtora roku oczekiwania – w styczniu 2019 r. ukazał się bowiem jej projekt (omówiony na naszym blogu: tutaj). W stosunku do tego projektu, wersja finalna została rozbudowana i poszerzona – a wnioski z niej płynące są w przeważającej mierze korzystne dla tych, którzy chcą stosować lub stosują już tę preferencję. Warto jednak, aby pracodawcy (płatnicy) oraz rozliczający dla podatników tą preferencję przeprowadzili weryfikację wewnętrznych procedur (w tym regulaminów i umów o pracę), aby zapewnić zgodność rozliczania 50% kosztów z wydaną interpretacją.

Kto jest beneficjentem 50% kosztów?

Krótko przypominając – 50% koszty uzyskania przychodu to preferencja podatkowa dla twórców, której zastosowanie zmniejsza podstawę opodatkowania, a tym samym – należny podatek dochodowy. W przypadku twórców – pracowników, do wynagrodzenia należnego za przeniesienie autorskich praw majątkowych bądź udzielenie licencji można bowiem zastosować nie „standardowe" pracownicze koszty uzyskania przychodu (obecnie 250 / 300 złotych[1]), ale koszty w wysokości 50% kwoty przychodu za przeniesienie praw lub udzielenie licencji. Zatem im większy przychód z tego tytułu (nazywany honorarium autorskim), tym większe koszty – a tym samym mniejsza zaliczka na podatek dochodowy i wyższe wynagrodzenia netto otrzymywane przez pracownika.

Od 2018 r. jedną z przesłanek warunkujących możliwość rozliczania 50% kosztów uzyskania przychodu jest podejmowanie działalności mieszczącej się w katalogu wskazanym w art. 22 ust. 9b ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych[2] (dalej: „PIT"). Wskazana została w nim m.in. działalność twórcza w zakresie programów lub gier komputerowych, co powoduje, że branża IT chętnie korzysta z tej preferencji podatkowej. Świadczy o tym chociażby fakt, że dotąd zdecydowana większość wydawanych indywidualnych interpretacji podatkowych dotyczyła pracodawców z tej branży.

Kluczowe kwestie wynikające z interpretacji ogólnej

Interpretacja ogólna, oprócz wyjaśnienia podstawowych kwestii dotyczących rozliczania 50% kosztów, w tym podstaw prawnych, **stawia na praktyczne wnioski dla pracodawców i pracowników**. W tym kontekście, warto wskazać zwłaszcza na następujące zagadnienia poruszone w interpretacji ogólnej:

- **wyjaśnienie, do których wybranych składników wynagrodzenia można stosować 50% koszty** (choć MF nie odniósł się do kwestii stosowania 50% kosztów do premii, co często kwestionowały organy skarbowe),
- **wskazanie dopuszczalnych sposobów dokumentowania wysokości honorarium autorskiego pracownika** – a zwłaszcza podkreślenie, że można w tym zakresie opierać się na oświadczeniu stron stosunku pracy, że dany utwór powstał (co z kolei powoduje, że w razie kontroli skarbowej nie powinno być wymagane przedstawienie konkretnych stworzonych utworów),
- **omówienie szczególnych regulacji dot. rozliczania 50% kosztów dla nauczycieli akademickich czy pracowników naukowych**.

[1] Zależnie od tego, czy pracownik dojeżdża do zakładu pracy w innej miejscowości (300 złotych) czy też nie (250 złotych).
[2] t.j. Dz. U. z 2020 r. poz. 1426 z późn. zm.

Najważniejszym jednak wnioskiem płynącym z interpretacji ogólnej wydaje się być stwierdzenie, że to w **gestii stron stosunku pracy jest określenie, jak będzie wyliczany przychód z tytułu korzystania z praw autorskich/ rozporządzania prawami autorskimi, czyli honorarium autorskie**. Minister Finansów oparł się w tym zakresie na orzeczeniach sądów administracyjnych, które podkreślały, że skoro przepisy prawa tej kwestii nie regulują, to pracownik i pracodawca mogą przyjąć w zasadzie dowolną zasadę ustalania wysokości honorarium – a więc w szczególności:

- metodę opartą o wyliczenie czasu pracy poświęconego na stworzenie utworów,
- metodę opartą na parametrze procentowym (% całości wynagrodzenia pracownika), czy też
- metodę kwotową (konkretnie określona kwota honorarium autorskiego).

Kwestia ta jest o tyle ważna, że powyżej zaprezentowane stanowisko sądów administracyjnych nie było podzielane przez Dyrektora Krajowej Informacji Skarbowej, który wydaje indywidualne interpretacje podatkowe. W wielu przypadkach stanowiska pracodawców przedstawiane w składanych wnioskach o interpretację uznawane były za nieprawidłowe właśnie z uwagi na zaprezentowaną metodę wyliczenia honorarium autorskiego. Znamienne było to, że Dyrektor Krajowej Informacji Skarbowej nie przedstawiał przy tym konkretnych wytycznych co do właściwego (w jego ocenie) sposobu obliczenia honorarium autorskiego.

Czego brakuje w interpretacji ogólnej?

Mimo tego, że wydana interpretacja ogólna podchodzi do tematu 50% kosztów w sposób kompleksowy, nie porusza wszystkich zagadnień, które budziły dotąd wątpliwości, zwłaszcza w branży IT. W dokumencie nie został bowiem skomentowany ani wyjaśniony w żaden sposób przepis art. 22 ust. 9b PIT, który określa rodzaje działalności uprawniające do zastosowania 50% kosztów.

Ma to znaczenie zwłaszcza dla utworów tworzonych w ramach branży IT – art. 22 ust. 9b PIT odwołuje się bowiem do „*działalności twórczej w zakresie programów komputerowych*". Biorąc pod uwagę, że pojęcie to nie sprowadza się wyłącznie do tworzenia programów komputerowych (programowania, tworzenia skryptów i kodów źródłowych), ale do prowadzenia „działalności twórczej" w ich zakresie, płatnicy skłaniali się do przyjęcia szerokiej wykładni, zgodnie z którą utworami tworzonymi w ramach działalności twórczej w zakresie programów komputerowych będą także wszelkiego rodzaju user stories, scenariusze testowe, dokumentacja funkcjonalna czy prezentacje multimedialne, o ile są wytwarzane w procesie wytwórczym oprogramowania. Takie stanowisko potwierdzał też Dyrektor Krajowej Informacji Skarbowej w indywidualnych interpretacjach podatkowych. Minister Finansów zdecydował się jednak nie zaadresować tej kwestii w interpretacji ogólnej.

Na co muszą uważać płatnicy?

Pozytywna ocena interpretacji ogólnej nie oznacza, że wszystkie zagadnienia w niej poruszone są korzystne dla płatników i podatników. Minister Finansów zwrócił bowiem uwagę na kwestię dotąd niekiedy pomijaną, czyli odpowiednie uregulowanie w umowie o pracę zasad nabycia praw autorskich przez pracodawcę. Interpretacja ogólna potwierdza, że pracownik musi wtórnie, w wyraźny sposób przenieść autorskie prawa majątkowe na pracodawcę, aby 50% koszty mogły zostać zastosowane. Natomiast na podstawie zasad ogólnych prawa autorskiego, mających zastosowanie dla stosunku pracy, w przypadku programów komputerowych pracodawca nabywa majątkowe prawa autorskie w sposób pierwotny, z mocy prawa. O ile więc umowa nie stanowi inaczej, w takim przypadku pracodawca nie ma podstaw do stosowania 50% kosztów uzyskania przychodu. Kwestia ta powinna zostać dokładnie zweryfikowana przez płatników pod kątem przyjętych regulacji, a w razie potrzeby zmieniona w zawartych umowach o pracę – tak aby zapewnić że pracownik przenosi autorskie prawa majątkowe na pracodawcę, również w przypadku programów komputerowych.

Znaczenie ogólnej interpretacji dla branży IT

Mając na uwadze, że interpretacja ogólna potwierdza kluczową dla rozliczania 50% kosztów kwestię, czyli swobodę w ustaleniu metody wyliczenia honorarium autorskiego, należy ją ocenić pozytywnie. Dotychczas była to główna przyczyna kwestionowania prawidłowości rozliczeń przez organy skarbowe, często w sposób niejednolity. Jednoznaczne stanowisko przedstawione przez Ministra Finansów w interpretacji ogólnej pozwoli rozstrzygnąć spór w tym zakresie i to w sposób korzystny dla płatników i podatników.

Co jest również istotne, interpretacja ogólna nie tylko przyczynia się do zapewnienia jednolitości stosowania prawa przez organy skarbowe, ale ma także walor ochronny – zgodnie z przepisami ordynacji podatkowej, zastosowanie się do interpretacji ogólnej nie może bowiem szkodzić temu, kto się do niej stosuje. Tym samym podatnicy i płatnicy nie mogą odnieść niekorzystnych skutków, jeśli postępują zgodnie z wytycznymi Ministra Finansów, mającymi walor interpretacji ogólnej. W tym zakresie, interpretacja ogólna zwiększy pewność prawa i stabilność jego stosowania.

Niemniej jednak, biorąc pod uwagę kompleksowy charakter interpretacji, powinna ona stać się impulsem do zweryfikowania dokonywanych przez pracodawcę rozliczeń 50% kosztów oraz sprawdzenia wewnętrznych procedur i dokumentów określających zasady tych rozliczeń – tak, aby zapewnić ich zgodność ze stanowiskiem Ministra Finansów.

Ulga na robotyzację

r.pr. Joanna Stecyk, r.pr. Joanna Jastrząb

W 2021 r. ma zostać wprowadzona ulga podatkowa na robotyzację. Ministerstwo Finansów i Ministerstwo Rozwoju zapowiedziały, że projekt zmian w Ustawie z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych i Ustawie z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych zostanie opublikowany jesienią.

Celem wprowadzenia ulgi jest zwiększenie poziomu robotyzacji polskiej gospodarki. Ma się to przyczynić do jej modernizacji, a także do polepszenia jakości i elastyczności produkcji oraz komfortu pracy. Zwiększenie produkcji przemysłowej za pomocą robotów ma podnieść wydajność i zyskowność, a tym samym konkurencyjność firm.

W momencie publikacji artykułu nie zostały przedstawione konkretne projekty przepisów, ale jedynie ich założenia. Zgodnie z nimi nowa ulga podatkowa zakłada możliwość odliczenia 50% kosztów kwalifikowanych poniesionych na inwestycje w robotyzację, niezależnie od wielkości i rodzaju branży. Nowa ulga jest więc wzorowana na obecnie funkcjonującej uldze B+R.

Zgodnie z przedstawionymi planami ulga ma być czasowa i obowiązywać przez 5 lat – do końca 2025 r.

Projektowana ulga trafiła do prekonsultacji branżowych, w ramach których zgłoszono uwagi dotyczące zwłaszcza jej zakresu. Dostrzeżono między innymi, że definicja robota nie obejmuje robotów software'owych, czyli symulujących pracę człowieka. Tymczasem oprogramowanie tego rodzaju może w pełnoprawny sposób być nazywane robotem, ponieważ wykonuje w sposób mechaniczny zadania, które w praktyce wykonywali dotąd pracownicy. Ulga zatem, w ocenie przedstawicieli branży, powinna obejmować również takie oprogramowanie.

Projektowana ulga niewątpliwie jest dobrym pomysłem. Aby jednak ją w pełni ocenić, pozostaje poczekać na przedstawienie konkretnych przepisów, które będą podstawą jej stosowania, a także wytycznych Ministerstwa Finansów w tym przedmiocie (np. objaśnień podatkowych lub ogólnych interpretacji podatkowych). Praktyka pokazuje bowiem, że stosowanie innych preferencji podatkowych, jak 50 proc. kosztów uzyskania przychodów dla pracowników branży IT, jest utrudnione, np. przez rozbieżności interpretacyjne organów podatkowych i brak jednolitości w rozumieniu ustawowych warunków zastosowania preferencji[1]. To z kolei wprost potwierdza, jak ważne w praktyce podatkowej są jednoznaczne przepisy ustaw oraz oficjalna wykładnia prezentowana przez Ministra Finansów.

W przypadku 50% kosztów jednolitość może zapewnić wydana niedawno ogólna interpretacja indywidualna, o której piszemy w artykule na str. 14

NADCHODZĄCE WYDARZENIA

13.10.2020

"Niewykonanie lub nienależyte wykonanie umowy IT - co zrobić aby uniknąć sporu i jak się zachować w sytuacjach kolizyjnych pomiędzy Wykonawcą i Zamawiającym?"

r. pr. Agnieszka Wachowska

Więcej informacji >>

3.11.2020

"Zwinne wdrożenia w umowach IT (AGILE, PRINCE2 AGILE) - przygotowanie i negocjowanie umów w projektach IT przy zwinnym podejściu"

r. pr. Agnieszka Wachowska

Więcej informacji >>

ARTYKUŁY

W październiku opublikowany zostanie specjalny dodatek do Monitora Prawniczego pt. ”Prawo nowych technologii” pod redakcją mec. Xawerego Konarskiego. Będzie to numer rekordowy, a znajdzie się w nim 26 artykułów. Wśród nich pojawią się artykuły naszych ekspertów:

Dostawcy usług internetowych – najnowsze zmiany w prawie UE i w prawie polskim
- artykuł mec. Xawerego Konarskiego

Dekompilacja programu komputerowego na potrzeby dokonania jego niezbędnej modyfikacji – rozważania przed wyrokiem TSUE w sprawie C-13/20
- artykuł mec. Agnieszki Wachowskiej

Konsekwencje istnienia wad oprogramowania przy odbiorach wdrożenia systemu IT
- artykuł mec. Agnieszki Wachowskiej i Aleksandra Elmerycha

Prawo komunikacji elektronicznej – wybrane zagadnienia
- artykuł mec. Magdaleny Gąsowskiej-Paproty

ZESPÓŁ IT-TELCO

Xawery Konarski
Adwokat, Senior Partner
xawery.konarski@traple.pl

Agnieszka Wachowska
Radca prawny, Partner
agnieszka.wachowska@traple.pl

Piotr Nepelski
Radca prawny, Senior Associate
piotr.nepelski@traple.pl

Tomasz Krzyżanowski
Radca prawny, Senior Associate
tomasz.krzyżanowski@traple.pl

Joanna Dworak
Radca prawny, Senior Associate
joanna.dworak@traple.pl

Joanna Jastrząb
Radca prawny, Senior Associate
joanna.jastrzab@traple.pl

Magdalena Gąsowska-Paprota
Radca prawny, Senior Associate
magdalena.gasowska@traple.pl

Karolina Grochecka-Goljan
Adwokat, Associate
karolina.grochecka@traple.pl

Wojciech Karwacki
Aplikant radcowski, Associate
wojciech.karwacki@traple.pl

Aleksander Elmerych
Junior Associate
aleksander.elmerych@traple.pl

Pytania prosimy kierować na adres:
it-telco@traple.pl

Redaktor newslettera:
r.pr. Joanna Jastrząb