NR 1 - LUTY 2022

NEWSLETTER

IT-TECH

W NUMERZE M.IN.:

- UZP opublikowało finalna wersję Rekomendacji dotyczących zamówień publicznych na systemy informatyczne (tom II)
- Regulacyjne cybertsunami
- Exit plan – potężne narzędzie w rękach zamawiającego chmurę
- 50% koszty i IP Box, czyli ulgi podatkowe dla pracowników z branży IT
- Kara umowna za zwłokę bez określonego limitu

Traple
Konarski
Podrecki
& Wspólnicy

TKP

UZP opublikowało finalna wersję Rekomendacji dotyczących zamówień publicznych na systemy informatyczne (tom II) – jak przygotować OPZ na system IT?

Agnieszka Wachowska

W grudniu 2021 r., po wielu miesiącach przygotowań oraz prowadzonych konsultacji, UZP opublikował II tom rekomendacji dotyczących zamówień publicznych na systemy informatyczne (dalej: „Tom II Rekomendacji"). Jest on efektem prac zespołu roboczego przy UZP, w których z ramienia PIIT uczestniczyła mec. Agnieszka Wachowska. Tom II poświęcony jest kwestiom związanym z formułowaniem opisu przedmiotu zamówienia (OPZ) oraz zawiera praktyczne wskazówki na temat przygotowania postępowania o udzielenie zamówienia publicznego.

Tom II Rekomendacji stanowi kompendium wiedzy na temat OPZ na systemy IT w pigułce. Porusza zagadnienia istotne z punktu widzenia przygotowania opisu przedmiotu zamówienia, tj. kwestie związane z podziałem zamówienia na części, określonością przedmiotu zamówienia, zasadami konkurencyjnego i równego traktowania wykonawców z uwzględnieniem elementów typowych dla branży IT i specyfiki zamawiania systemów informatycznych. Dokument zwraca uwagę na prawidłowe stosowanie kryteriów w celu oceny równoważności, odpowiednie opisywanie wymaganych uprawnień do korzystania z systemów informatycznych (w tym kwestie prawnoautorskie), właściwe narzędzia przeciwdziałania *vendor lock-in*, a także na potrzebę opisywania wymogów związanych z cyberbezpieczeństwem dla zamawianych systemów IT.

Sposób ujęcia i konstrukcja Tomu II Rekomendacji

Dokument Tomu II Rekomendacji, przy założeniu, że poszczególne zagadnienia merytoryczne są omawiane w odrębnych blokach dotyczących kluczowych zagadnień wspólnych dla wszystkich rodzajów zamówień, podzielony został na **osiem głównych rozdziałów tematycznych**:

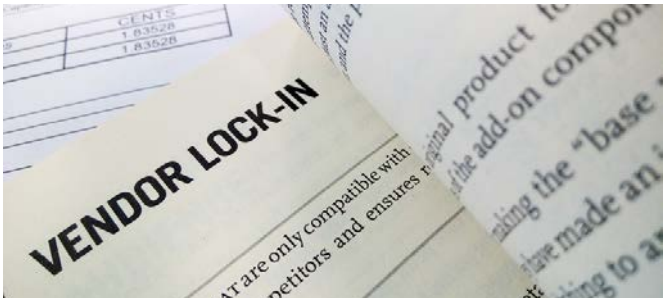
1. Wprowadzenie – zawierające założenia metodologiczne.
2. Podział zamówienia na części.
3. Określoność przedmiotu zamówienia.
4. Niedyskryminacyjny OPZ, czyli zasady konkurencyjności i równego traktowania wykonawców.
5. Kryteria stosowane w celu oceny równoważności.
6. Odpowiednie opisanie wymaganych uprawnień do korzystania z systemów informatycznych.
7. Przeciwdziałanie *vendor-lock in*.
8. Odpowiednie opisanie wymogów cyberbezpieczeństwa systemów informatycznych.

Jednocześnie dokument został przygotowany w taki sposób, aby zawierał jak najwięcej konkretnych, praktycznych rekomendacji. Tym samym, niezależnie od rozdziałów tematycznych, w całym dokumencie przyjęto **trójstopniową strukturę rekomendacji składającą się z rekomendacji ogólnych, rekomendacji szczegółowych oraz zagadnień** zawierających pewne szczegółowe wytyczne dla konkretnych typów zamówień na systemy IT, jak np. zamówienia i wymagania specyficzne dla zamawiania IaaS, PaaS czy SaaS.

Rekomendacje ogólne

Rekomendacje ogólne zawarte i omówione w Tomie II Rekomendacji stanowią uniwersalne i podstawowe wskazówki dla wszystkich zamawiających odnośnie do tego, jakimi zasadami i wytycznymi, mając na uwadze obowiązujące przepisy prawa zamówień publicznych oraz dobre praktyki obrotu, powinni się kierować przy przygotowywaniu OPZ na zamówienie systemu informatycznego. Tym samym zebrane łącznie **rekomendacje ogólne stanowią pewnego rodzaju**

kodeks dobrych praktyk dla wszystkich zamawiających zobowiązanych do stosowania prawa zamówień publicznych, którzy przygotowują postępowanie na zamówienie systemu informatycznego. Rekomendacje mogą też służyć jako praktyczna checklistaweryfikacyjna, przez którą zamawiający mogą przejść, aby upewnić się, czy przy przygotowywaniu OPZ na zamówienie systemu IT uwzględnili i rozważyli wszystkie istotne kwestie.



Nowe podejście do kwestii praw autorskich oraz *vendor lock-in*

W Tomie II Rekomendacji wiele miejsca poświęcono kwestii odpowiedniego opisania uprawnień do korzystania z systemów informatycznych, tak aby nie tylko przeciwdziałać *vendor lock-in* i dążyć do minimalizacji ryzyka przywiązania do jednego wykonawcy lub producenta, lecz także aby zawarte w dokumentacji postępowania wymagania były rynkowo uzasadnione i nie ograniczały niepotrzebnie konkurencji.

W rekomendacji ogólnej nr 13 podkreślono, że **zakres uprawnień wymaganych przez zamawiającego od wykonawcy w odniesieniu do zamawianego systemu informatycznego ma często istotne znaczenie cenotwórcze**, a niejednokrotnie może nawet decydować o tym, czy dany wykonawca postanowi złożyć ofertę, czy też zrezygnuje z jej składania. Jako przykład wskazano, że wymaganie przez zamawiającego, aby wykonawca przeniósł na niego majątkowe prawa autorskie do części lub całości dostarczanego oprogramowania składającego się na zamówiony system informatyczny, sprawia, że wykonawca w konsekwencji zawarcia umowy na realizację takiego zamówienia traci prawa do oprogramowania i nie będzie mógł wykorzystywać go w przyszłości na potrzeby wykonania innych projektów informatycznych. Może to spowodować decyzję wykonawcy o rezygnacji z udziału w postępowaniu, w którym postanowione są takie wymogi.

W tym kontekście na szczególną uwagę zasługuje **rekomendacja szczegółowa nr 14.3, która wprost wskazuje, że zamawiający nie powinien dążyć za wszelką cenę do nabycia pełni autorskich praw majątkowych do zamawianego systemu informatycznego**. W uzasadnieniu do tej rekomendacji zwrócono uwagę na często występujący problem polegający na tym, że zamawiający – chcąc zabezpieczyć sobie odpowiedni zakres praw do oprogramowania w ramach zamawianego systemu – oczekują od wykonawców przeniesienia majątkowych praw autorskich do systemu, tymczasem takie wymaganie nie zawsze jest optymalne i uzasadnione z punktu widzenia zamawiającego, a niejednokrotnie może wręcz działać na jego niekorzyść. Mając na uwadze powyższe, w uzasadnieniu rekomendacji szczegółowej nr 14.3 **wyraźnie wskazano, że nie w każdym przypadku zamawiający powinien dążyć za wszelką cenę do nabycia pełni autorskich praw majątkowych do zamawianego systemu informatycznego, a takie żądanie postawione w SWZ powinno być poprzedzone wcześniejszą analizą faktycznych potrzeb zamawiającego**.

Zgodnie z opublikowanymi rekomendacjami przed podjęciem decyzji przez zamawiającego co do tego, czy żądać przeniesienia majątkowych praw autorskich do systemu – a jeśli tak, to w jakim zakresie i w odniesieniu do jakich elementów oprogramowania – zamawiający powinien w szczególności sprawdzić:

1. Czy oprogramowanie spełniające potrzeby zamawiającego – lub część takich potrzeb – jest już dostępne na rynku jako standardowe rozwiązanie.
2. Na ile zamawiane oprogramowanie jest krytyczne, a co za tym idzie – na ile ryzyka związane z ewentualną wypowiadalnością licencji są dla zamawiającego krytyczne.
3. Jak długo zamawiający chce wykorzystywać oprogramowanie oraz czy chce je dostosowywać do swoich potrzeb po zakończeniu realizacji zamówienia.

Warto również zwrócić uwagę na to, że dokument rekomendacji, wskazując w rekomendacjach szczegółowych nr 13.3–13.7 na zakres uprawnień do systemu, jaki powinien być opisany w OPZ, **nie przesądza tego, czy uzyskanie tych uprawnień przez zamawiającego powinno następować przez przeniesienie majątkowych praw autorskich, czy poprzez licencję niewyłączną lub też inną podstawę prawną do korzystania z oprogramowania** – zostawia tę kwestię do indywidualnego rozpatrzenia przez zamawiającego w zależności od potrzeb zamawiającego oraz rodzaju zamawianego przez niego systemu informatycznego.

Cyberbezpieczeństwo jako istotny element, który należy uwzględnić przy konstruowaniu OPZ na zamawiany system IT

Zupełnie nowym elementem, który nie pojawił się w rekomendacjach z 2009 r. i niewątpliwie stanowi znak obecnych czasów, jest zwrócenie uwagi na konieczność przeanalizowania oraz odpowiedniego opisania przez zamawiającego wymagań w zakresie cyberbezpieczeństwa dla zamawianych systemów informatycznych. W Tomie II Rekomendacji kwestie te zostały opisane w rozdziale VIII w trzech rekomendacjach ogólnych oraz pięciu rekomendacjach szczegółowych.

W rekomendacjach wskazano, że zamawiający powinien zadbać, aby wykonawca zapewnił odpowiednie zabezpieczenia dostarczanego systemu informatycznego. Z powyższych względów w pierwszej kolejności zamawiający powinien dokonać **oceny, jakie regulacje dotyczące cyberbezpieczeństwa powinien stosować w ramach prowadzonej działalności** (rekomendacja ogólna nr 16), zarówno jeśli chodzi o powszechnie obowiązujące przepisy prawa (rekomendacja szczegółowa nr 16.1), jak i wytyczne i rekomendacje o charak-terze niewiążącym (rekomendacja szczegółowa nr 16.2).

W dalszej części rekomendacji wskazano również na **potrzebę przeprowadzenia przez zamawiającego analizy ryzyka w zakresie cyberbezpieczeństwa w celu określenia poziomu ryzyka związanego z wykorzystaniem systemu informatycznego** (rekomendacja ogólna nr 17), tak aby w sposób właściwy określić szczegółowe wymagania w zakresie cyberbezpieczeństwa, które powinien spełniać system informatyczny dostarczony przez wykonawcę, oraz w celu wyboru optymalnego z punktu widzenia bezpieczeństwa modelu wdrożenia systemu informatycznego. W rekomendacjach podkreślono też, że przeprowadzone przez zamawiającego szacowanie ryzyka powinno uwzględniać zagrożenia występujące dla zamawiającego w całym cyklu życia projektu, tj. zarówno na etapie projektowania systemu i jego wdrażania, jak i na etapie utrzymania i korzystania z systemu.

Ostatnia z ogólnych rekomendacji – rekomendacja ogólna nr 18 – wskazuje na konieczność **odpowiedniego określenia w OPZ wymagań dotyczących cyberbezpieczeństwa, jakie powinien spełniać system informatyczny**. W rekomendacjach szczegółowych uściślono, jak tę „odpowiedniość" należy rozumieć. W rekomendacjach zaznaczono, że opisanie wymagań w zakresie bezpieczeństwa powinno nastąpić **w sposób technologicznie neutralny**, tak aby nie ograniczać bezpodstawnie konkurencji i zapewnić możliwość udziału w postępowaniu możliwie najszerszemu gronu wykonawców. Opis wymagań w zakresie cyberbezpieczeństwa **powinien również uwzględniać wnioski z analizy ryzyka** (rekomendacja szczegółowa nr 18.1), a także **być ukształtowany w sposób, który pozwoli reagować na dynamicznie zmieniające się uwarunkowania, w szczególności pojawiające się nowe, nieznane wcześniej zagrożenia** (rekomendacja szczegółowa nr 18.2). Oznacza to, że w cyklu życia projektu IT zamawiający powinien mieć możliwość zmiany postawionych wymagań, tak aby na każdym etapie korzystania z systemu zagwarantować adekwatne i proporcjonalne środki na rzecz cyberbezpieczeństwa. Ostatnia z rekomendacji szczegółowych zwraca uwagę na to, **że przed przystąpieniem do korzystania z systemu informatycznego zamawiający powinien zaprojektować i wdrożyć odpowiednie procedury na wypadek wystąpienia incydentu bezpieczeństwa** (rekomendacja szczegółowa nr 18.3).

Podsumowanie i wnioski na przyszłość

Podjętą przez Prezesa UZP i konsekwentnie realizowaną inicjatywę stworzenia nowych, odpowiadających aktualnym potrzebom rynku rekomendacji dotyczących zamawiania systemów informatycznych należy ocenić bardzo pozytywnie. Mając jednocześnie na uwadze bardzo dynamiczny i stale zmieniający się rynek IT, należy również mieć nadzieję na to, że opracowane rekomendacje będą podlegały regularnym przeglądom i aktualizacjom, a uczestnicy rynku zamówień publicznych (zarówno zamawiający, jak i wykonawcy IT) będą przekazywać konstruktywne uwagi i aktywnie włączą się w prace nad kolejnymi wersjami rekomendacji.

Regulacyjne cybertsunami

Agnieszka Wachowska, Jakub Chlebowski

Na przestrzeni ostatnich lat – w szczególności od transpozycji przez państwa członkowskie Unii Europejskiej w 2018 r. pierwszej horyzontalnej regulacji w obszarze cyberbezpieczeństwa, czyli Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (**dyrektywa NIS**) – kwestia regulacji cyberbezpieczeństwa i określenia wspólnych cyberstandardów dla konkretnych branż nabiera coraz większego znaczenia. Najlepszym przykładem tej tendencji jest fakt, że już po transpozycji **dyrektywy NIS** zaproponowane w niej rozwiązania okazały się niewystarczające i dwa lata po jej implementacji, pod koniec 2020 r., Komisja Europejska opublikowała projekt tzw. dyrektywy NIS 2. Ma ona zastąpić stosowaną od ledwie trzech lat dyrektywę NIS, aby dokładniej uporządkować kwestie cyberbezpieczeństwa w całej Unii Europejskiej.

Zarówno dyrektywa NIS, jak i dyrektywa NIS 2 stanowią tylko preludium regulacyjnego cybertsunami, które jest coraz bardziej zauważalne w tym obszarze. Dotyczy to nie tylko legislacji i pojawiających się nowych projektów dyrektyw przygotowanych przez Komisję Europejską, które mają określać powszechne reguły ochrony przed cyberzagrożeniami, lecz także mnogości wytycznych dla kolejnych sektorów gospodarki wydawanych, często w sposób nieskoordynowany przez różne podmioty.

Kolejne regulacje dotyczące (cyber)bezpieczeństwa

O ile celem dyrektywy NIS (i implementującej ją w polskim prawie ustawy o krajowym systemie cyberbezpieczeństwa z 2018 r.[1]) oraz dyrektywy NIS 2 jest uporządkowanie i ustalenie w całej Unii Europejskiej generalnych zasad przeciwdziałania cyberzagrożeniom oraz sprawnego zarządzania występującymi incydentami bezpieczeństwa w kluczowych dla gospodarek państw członkowskich sektorach, o tyle w Unii Europejskiej dodatkowo pojawiają się pomysły szczegółowych regulacji dotyczących konkretnych kategorii podmiotów.

Wśród pomysłów, które obecnie się urealniają, jest propozycja Komisji Europejskiej dotycząca nowej dyrektywy w sprawie odporności podmiotów krytycznych (tzw. **dyrektywa CER**). Na podstawie tej dyrektywy ma zostać zharmonizowany sposób identyfikacji podmiotów krytycznych, a zatem pełniących podstawowe funkcje społeczne i mających wpływ na bezpieczeństwo publiczne państwa członkowskiego, oraz mają być określone sposoby ochrony podmiotów identyfikowanych jako krytyczne, w tym ustalenie zasad przeciwdziałania wszystkim zagrożeniom. Dyrektywa CER ma uzupełniać regulacje europejskie w zakresie bezpieczeństwa o to, co nie zostanie objęte dyrektywą NIS 2.

Unia Europejska zwraca również uwagę na bezpieczeństwo sektora finansowego, w związku z czym przedstawiła na początku 2021 r. propozycję rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (tzw. **rozporządzenie DORA**). Rozporządzenie DORA ma stworzyć jednolite przepisy na poziomie europejskim, które określą zasady zarządzania ryzykami dotyczącymi ICT oraz obsługi incydentów związanych z ICT wykorzystywanymi przez sektor finansowy. Sektor ten, oprócz banków i instytucji płatniczych, obejmuje nawet platformy crowdfundingowe czy usługodawców obsługujących kryptowaluty.

[1] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2020 r., poz. 1369).

Wzmożenie działań w zakresie regulacji cyberbezpieczeństwa jest zauważalne nie tylko na poziomie europejskim, lecz także w polskiej legislacji. Najjaskrawszym tego przykładem jest procedowany od ponad roku projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, który przy każdej kolejnej prezentacji nowego tekstu nowelizacji dokłada nowe propozycje regulacji cyberbezpieczeństwa, wykraczające poza to, czego wymaga obowiązująca obecnie dyrektywa NIS.

Lawina wytycznych

Pojawiające się na przestrzeni ostatnich kilku lat nowe legislacje na poziomie europejskim i krajowym to niejedyny element regulacji cyberbezpieczeństwa. Minione dwa lata to zauważalna tendencja pojawiania się wielu wytycznych i rekomendacji dotyczących cyberbezpieczeństwa poszczególnych sektorów.

Wytyczne publikowane są m.in. przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (tzw. ENISA)[2], której publikacje obejmują coraz więcej sektorów. Wytyczne ENISA jedynie w samym 2021 r. dotyczyły takich sektorów, jak: finansowy, energii, transportu wodnego i powietrznego, telekomunikacyjny czy zdrowia. Jednocześnie w ramach bieżącej działalności ENISA publikuje rekomendacje, raporty lub inne opracowania, które omawiają kwestię cyberbezpieczeństwa w kontekście takich zagadnień, jak: usługi chmurowe, usługi zaufania, interoperacyjność systemów, uczenie maszynowe, kryptowaluty.

Również na polskim podwórku pojawiły się opracowania podejmujące próbę standaryzacji rozwiązań zabezpieczających sieci i systemy informatyczne, w tym najbardziej kompleksowe w tym zakresie i dotyczące wszystkich sektorów Narodowe Standardy Cyberbezpieczeństwa[3], w ramach których powstały Standardy Cyberbezpieczeństwa Chmur Obliczeniowych. Dodatkowo opracowywane są konkretne rekomendacje przez organy publiczne, które odpowiadają za dany sektor. Warto wspomnieć opublikowane w październiku 2021 r. przez Ministerstwo Klimatu i Środowiska kompleksowe rekomendacje w zakresie cyberbezpieczeństwa dla polskiego sektora energii[4].

Co więcej, własne rekomendacje publikują organizacje z poszczególnych sektorów, aby samodzielnie ustalać standardy cyberbezpieczeństwa dla swojej branży. Za znak czasu należy uznać również to, że elementy cyberbezpieczeństwa pojawiły się w II tomie rekomendacji dotyczących zamówień publicznych na systemy informatyczne, przygotowanych przez Urząd Zamówień Publicznych pod koniec 2021 r.[5]

Co dalej?

Zauważalny w ostatnich latach wzrost zainteresowania kwestiami cyberbezpieczeństwa bez wątpienia przybiera na sile i będzie nadal postępował w najbliższych latach. Obecnie – bez zbędnej przesady – można stwierdzić, że nie ma miesiąca, w którym nie pojawiają się nowe wytyczne dla poszczególnych sektorów, publikowane czy to przez podmioty międzynarodowe, czy przez organizacje działające w Polsce. Można mówić o prawdziwej inflacji regulacji cyberbezpieczeństwa. Liczba publikowanych wytycznych jest na tyle duża, że chcąc być z nimi na bieżąco, można niemal utonąć w zalewnie opracowań i wytycznych. Niestety jednocześnie wraz ze wzrostem ilości publikacji na temat cyberbezpieczeństwa coraz bardziej uwidocznia się problem braku koordynacji wydawanych poszczególnych wytycznych. Co więcej ich ilość i objętość niekoniecznie przekładają się na jakość tych dokumentów, a tym samym na tworzone standardy w zakresie cyberbezpieczeństwa.

Niestety w najbliższym czasie można spodziewać się, że trend tworzenia nowych, zarówno twardych, jak i miękkich regulacji prawnych w zakresie cyberbezpieczeństwa może się nasilać, jeśli ciała prawodawcze (europejskie czy polskie) będą się decydowały – idąc śladem rozporządzenia DORA – na uregulowanie kwestii cyberbezpieczeństwa odrębnie dla kolejnych sektorów, m.in. takich jak energetyka, sektor zdrowia czy chociażby usługi publiczne. Pytanie tylko, czy naprawdę konieczne i celowe jest, aby każdy sektor posiadał własne odrębne, a jednocześnie bardzo zbliżone do pozostałych regulacje w zakresie cyberbezpieczeństwa i czy nie warto czasem zastanowić się nad maksymą „mniej znaczy więcej”?

[2] Zob. https://www.enisa.europa.eu/ (dostęp: 2.02.2022).
[3] Zob. https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyberbezpieczenstwa (dostęp: 2.02.2022).
[4] Zob. https://www.gov.pl/web/klimat/rekomendacje-w-zakresie-cyberbezpieczenstwa-dla-polskiego-sektora-energii (dostęp: 2.02.2022).
[5] Zob. https://www.uzp.gov.pl/strona-glowna/slider-aktualnosci/ii-tom-rekomendacji-dotyczacych-zamowien-publicznych-na-systemy-informatyczne/ii-tom-rekomendacji-dotyczacych-zamowien-publicznych-na-systemy-informatyczne (dostęp: 2.02.2022).

Exit plan – potężne narzędzie w rękach zamawiającego chmurę

Karolina Grochecka-Goljan

Wraz z coraz większym udziałem chmury obliczeniowej w rynku IT potencjalnie może czekać nas również zwiększenie liczby sporów pomiędzy zamawiającymi a dostawcami chmury obliczeniowej w sytuacji, gdy zamawiający zdecyduje się zakończyć współpracę z dostawcą. Potężnym narzędziem w rękach zamawiających chmurę obliczeniową – obok innych odpowiednio ukształtowanych postanowień umowy – jest exit plan.

Czym jest exit plan?

Exit plan (*exit strategy*) to plan działań na wypadek: zakończenia współpracy z dostawcą, obniżenia jakości usługi w sposób uniemożliwiający dalsze korzystanie z niej, całkowitego zaprzestania świadczenia usługi, a także w razie podjęcia decyzji biznesowej o przeniesieniu usług do innego dostawcy czy też do infrastruktury *on-premises*.

Exit plan powinien dotyczyć działania zarówno wewnątrz, jak i na zewnątrz organizacji. Plan działania powinien zostać opisany w umowie z wykonawcą i określać zakres jego obowiązków.

Dlaczego exit plan jest potrzebny?

Odpowiednio przygotowany exit plan pozwala uniknąć zjawiska *vendor lock-in* lub je zminimalizować, zadziałać szybko w sytuacji kryzysowej, a także ustalić zakres obowiązków wykonawcy na etapie, gdy stosunki między nim a zamawiającym są poprawne, a tym samym – kiedy jest to jeszcze możliwe.

Vendor lock-in polega na takim uzależnieniu zamawiającego od produktów lub usług danego dostawcy, że niemożliwa jest zmiana dostawcy bez poniesienia istotnych dodatkowych kosztów lub dużych niedogodności.

W przypadku usług chmurowych *vendor lock-in* jest szczególnie odczuwalny w momencie migracji danych i aplikacji, mogą bowiem wówczas wystąpić trudności z wydobyciem i wyeksportowaniem danych z chmury, a także dodatkowe koszty związane z transferem danych z chmury.

Poradniki i wytyczne dotyczące chmury a opracowanie planu wyjścia z chmury obliczeniowej

Opracowanie planu wyjścia z chmury obliczeniowej jest **rozwiązaniem powszechnie rekomendowanym** w poradnikach i wytycznych dotyczących korzystania z chmury obliczeniowej.

Szczególny nacisk na opracowanie planu wyjścia położony jest w rekomendacjach dotyczących korzystania z chmury obliczeniowej przez podmioty z rynku finansowego, ale z uwagi na doniosłość zagadnienia wytyczne w tym zakresie powinny być wzięte pod uwagę również przez podmioty spoza tego sektora. Uniwersalne wytyczne do zastosowania znajdują się natomiast między innymi w SWIPO Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) czy też w SWIPO Code of Conduct for Data Portability and Cloud Service Switching for Software as a Service (SaaS)[1].

Podstawą zastosowania planu wyjścia w umowie z dostawcą usług chmurowych powinny być odpowiednie klauzule umowne związane z rozwiązaniem umowy, które:

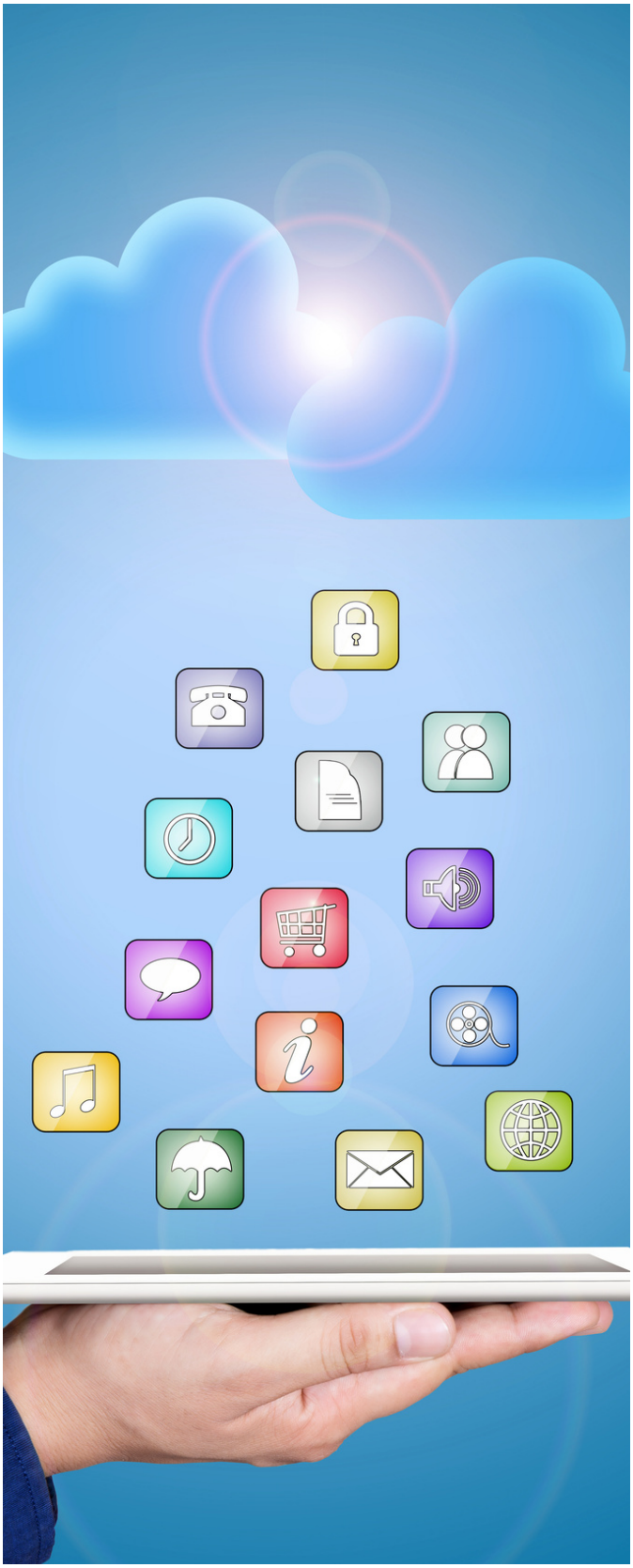
- zapewniają użytkownikowi możliwość rozwiązania umowy i przeniesienia danych w razie potrzeby;

[1] Wytyczne dostępne tutaj: https://swipo.eu/download-section/copyrighted-downloads/.

- zapewniają użytkownikowi własność przetwarzanych informacji w trakcie trwania umowy oraz po jej zakończeniu;
- gwarantują użytkownikowi, że należące do niego dane zostaną całkowicie i bezpiecznie usunięte przez dostawcę usług chmury obliczeniowej we wszystkich regionach, w których były przetwarzane;
- określają zasady i terminy zwrotu lub usunięcia przetwarzanych informacji.

Z kolei wśród najważniejszych zagadnień, które powinny znaleźć się w planie wyjścia z chmury przygotowanym na potrzeby wewnętrzne organizacji (w wewnętrznej procedurze przygotowania na wypadek zakończenia współpracy z dostawcą chmurowym), należy wskazać m.in.:

- scenariusz wycofania – należy określić przewidywane scenariusze wycofania usługi, takie jak migracja *on-premises*, zmiana dostawcy usług chmury obliczeniowej itp., z uwzględnieniem szczególnych sytuacji, np. nagłego zaprzestania świadczenia usługi, rezygnacji z usługi po zakończeniu kontraktu itp.;
- wpływ zmiany na organizację użytkownika chmury;
- opis transferu usługi chmury obliczeniowej – opis procesu migracji usługi chmury obliczeniowej oraz danych, wymaganych narzędzi itp., z uwzględnieniem niezbędnych do podjęcia czynności prawnych i technicznych;
- scenariusze testowe procesów migracji;
- określenie czasu pobrania danych do migracji od dostawcy usług chmury obliczeniowej;
- backup lokalny danych przekazanych do chmury obliczeniowej dla szczególnie istotnych usług;
- szacunkowy harmonogram migracji do infrastruktury *on-premises* lub do innego dostawcy chmury;
- określenie ról i odpowiedzialności użytkownika i dostawcy usług chmury obliczeniowej w procesie migracji;
- ustalenie obowiązków dostawcy chmury obliczeniowej w procesie migracji.



Podsumowanie

Sporządzenie odpowiedniego exit planu niewątpliwie wymaga zaangażowania, niemniej w przyszłości może nie tylko ochronić zamawiającego przed koniecznością ponoszenia dodatkowych kosztów, lecz przede wszystkim przyczynić się do zapobieżenia paraliżowi informatycznemu w organizacji, a tym samym wpłynąć na sprawność organizacyjną prowadzenia biznesu.

50% koszty i IP Box, czyli ulgi podatkowe dla pracowników z branży IT

Agnieszka Wachowska, Aleksander Elmerych

Wprowadzenie obowiązującego od dnia 1 stycznia 2022 r. pakietu zmian legislacyjnych dotyczących prawa podatkowego, w szczególności w zakresie podatku dochodowego od osób fizycznych (potocznie zwanego „Polskim Ładem")[1], wywołuje wiele kontrowersji. Komentatorzy zwracają uwagę na to, iż mimo zapowiadanych korzystnych zmian dla podatników w rzeczywistości okazało się, że duża część osób otrzymała niższe wynagrodzenie netto za styczeń 2022 r. – dotyczy to w szczególności przedsiębiorców oraz osób najlepiej zarabiających. W związku z tym wzrosło zainteresowanie możliwością optymalizacji osiąganych dochodów poprzez korzystanie z oferowanych przez prawo ulg podatkowych dla poszczególnych kategorii pracowników i przedsiębiorców. Do ulg podatkowych, z których najczęściej korzystają pracownicy i przedsiębiorcy z branży IT, należy zaliczyć w szczególności 50% koszty uzyskania przychodów (dalej: „50% koszty") oraz preferencyjną, 5-procentową stawkę podatku dochodowego IP Box (dalej: „IP Box"). Jak działają te ulgi i kto może z nich korzystać?

Jak działają 50% koszty?

Możliwość stosowania 50% kosztów uzyskania przychodów wynika z art. 22 ust. 9 pkt 3 Ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (t.j. Dz. U. z 2021 r., poz. 1128; dalej: „ustawa PIT") – **mogą z nich korzystać m.in. osoby zatrudnione na podstawie umowy o pracę**, nie ma jednak możliwości stosowania 50% kosztów przez przedsiębiorców prowadzących własną działalność gospodarczą. W dużym uproszczeniu 50% koszty pozwalają pracownikom twórcom na zmniejszenie podstawy opodatkowania poprzez stosowanie podwyższonych kosztów uzyskania przychodów do wynagrodzenia otrzymanego z tytułu przeniesienia majątkowych praw autorskich lub udzielenia licencji (honorarium autorskiego) – zamiast standardowych pracowniczych kosztów uzyskania przychodów (obecnie zryczałtowana kwota 250 zł lub 300 zł[2]) pracownicy mogą do takiego wynagrodzenia stosować koszty w wysokości 50% kwoty osiągniętego przychodu. Im wyższe jest honorarium autorskie, tym większe są koszty uzyskania przychodów po stronie pracownika, a tym samym mniejsza zaliczka na podatek dochodowy i wyższe wynagrodzenia netto otrzymywane przez pracownika. W praktyce 50% koszty pozwalają zatem na podwyższenie wynagrodzenia netto otrzymywanego przez pracownika przy zachowaniu dotychczasowych kosztów zatrudnienia po stronie pracodawcy.

Kto może korzystać z 50% kosztów?

Warto mieć na uwadze, że z 50% kosztów nie mogą korzystać wszyscy pracownicy tworzący utwory w ramach wykonywania obowiązków służbowych – **uprawniają do tego bowiem jedynie utwory wytworzone w ramach określonych rodzajów działalności twórczej**, które zostały wymienione w art. 22 ust. 9b ustawy PIT. Znalazła się wśród nich m.in. działalność tłumaczeniowa, publicystyczna, **działalność twórcza w zakresie sztuk plastycznych, twórczości audialnej i wizualnej** czy – co szczególnie istotne z perspektywy branży IT – **w zakresie programów komputerowych i gier komputerowych**. Korzystne dla pracowników z branży IT jest również szerokie rozumienie pojęcia „działalności twórczej w zakresie programów komputerowych" prezentowane przez Dyrektora Krajowej Informacji Skarbowej, zgodnie z którym podstawę do stosowania 50%

[1] Zob. Ustawa z dnia 29 października 2021 r. o zmianie ustawy o podatku dochodowym od osób fizycznych, ustawy o podatku dochodowym od osób prawnych oraz niektórych innych ustaw (Dz. U. z 2021 r., poz. 2105, z późn. zm.).
[2] Kwota ta zależy od tego, czy pracownik dojeżdża do zakładu pracy w innej miejscowości (300 zł), czy też nie (250 zł).

kosztów stanowią nie tylko same kody źródłowe oprogramowania, lecz także wszelkie inne utwory powstałe w procesie tworzenia oprogramowania, takie jak np. plany i prototypy systemów, bazy oraz struktury danych, strony internetowe, dokumentacja techniczna, plany, analizy, raporty, rekomendacje, projekty graficzne, interfejsy użytkownika czy materiały reklamowe i marketingowe[3].

Jakie są warunki stosowania 50% kosztów i jak je wdrożyć w praktyce?

Warunki stosowania 50% kosztów wynikają przede wszystkim z przepisów ustawy PIT (w szczególności z art. 22 ust. 9-9b) oraz wydanej przez Ministra Finansów ogólnej interpretacji podatkowej dotyczącej stosowania 50% kosztów (dalej: „interpretacja ogólna")[4], a także – w ograniczonym zakresie – z indywidualnych interpretacji podatkowych wydawanych przez Dyrektora Krajowej Informacji Skarbowej[5]. Wśród podstawowych warunków stosowania 50% kosztów należy wskazać w szczególności na:

- tworzenie przez pracownika utworów w rozumieniu prawa autorskiego, w ramach działalności twórczej, o której mowa w art. 22 ust. 9b ustawy PIT;
- przenoszenie przez pracownika majątkowych praw autorskich do ww. utworów na rzecz pracodawcy w sposób wtórny;
- uzyskiwanie przez pracownika z tego tytułu wynagrodzenia (honorarium autorskiego) oraz jego wyraźne wyodrębnienie w umowie o pracę;
- ewidencjonowanie utworów stanowiących podstawę wypłaty honorarium autorskiego i dokumentowanie przeniesienia majątkowych praw autorskich na pracodawcę.

W celu wdrożenia rozliczania 50% kosztów dla pracowników pracodawcy powinni przede wszystkim:

- przeprowadzić analizę możliwości stosowania 50% kosztów w danej organizacji;
- przeanalizować poszczególne stanowiska pod kątem możliwości stosowania 50% kosztów;
- wprowadzić stosowne zmiany do umów o pracę;
- szczegółowo i wyczerpująco uregulować zasady wypłaty honorarium autorskiego w wewnętrznych aktach organizacyjnych;
- wdrożyć odpowiednie procedury w zakresie ewidencjonowania utworów, tak aby zapewnić odprowadzanie zaliczek na podatek dochodowy w prawidłowej wysokości.

Wykonanie ww. kroków powinno zapewnić w pełni prawidłowe i zgodne z przepisami prawa podatkowego stosowanie 50% kosztów.

Czym jest IP Box?

IP Box jest z kolei preferencyjną stawką podatkową, która została uregulowana w art. 30ca i 30cb ustawy PIT i z której mogą korzystać **osoby prowadzące pozarolniczą działalność gospodarczą**[6]. Korzyści wynikające z IP Box polegają na opodatkowaniu dochodów uzyskiwanych z komercjalizacji kwalifikowanych praw własności intelektualnej (dalej: „KPWI"), takich jak np. **dochody z tytułu udzielenia licencji czy ze sprzedaży oprogramowania, preferencyjną stawką podatkową w wysokości 5%**. Dzięki temu osoby prowadzące działalność badawczo-rozwojową i wytwarzający w jej ramach lub ulepszający kwalifikowane prawa własności intelektualnej (np. autorskie prawa do programów komputerowych, patenty czy prawa ochronne na wzory użytkowe) mogą zwiększyć otrzymywane wynagrodzenie netto. Z uwagi na charakter ulgi IP Box korzystać z niej mogą niektóre osoby pracujące w branży IT na podstawie umów B2B, np. deweloperzy oprogramowania.

[3] Zob. indywidualna interpretacja podatkowa Dyrektora Krajowej Informacji Skarbowej z dnia 17 sierpnia 2021 r., sygn. 0113-KDIPT2-3.4011.470.2020.1.RR.
[4] Zob. interpretacja ogólna nr DD3.8201.1.2018 Ministra Finansów z dnia 15 września 2020 roku w sprawie zastosowania 50% kosztów uzyskania przychodów do honorarium autorskiego.
[5] Obecnie, z uwagi na opublikowanie interpretacji ogólnej, Dyrektor Krajowej Informacji Skarbowej nie wydaje indywidualnych interpretacji podatkowych potwierdzających prawidłowość stosowania 50% kosztów, ograniczając się jedynie do rozstrzygnięć dotyczących sposobu rozumienia kategorii działalności twórczej, o których mowa w art. 22 ust. 9b ustawy PIT.
[6] Z ulgi IP Box mogą również korzystać osoby prawne na podstawie art. 24e i 24d Ustawy z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych (t.j. Dz. U. z 2021 r., poz. 1800, z późn. zm.).

Jakie są warunki stosowania IP Box?

Do korzystania z IP Box niezbędne jest, aby osoba prowadząca działalność gospodarczą:

- prowadziła działalność badawczo-rozwojową;
- wytwarzała, rozwijała lub ulepszała w ramach tej działalności KPWI, do których przysługują jej prawa autorskie;
- uzyskiwała dochody z tych KPWI;
- prowadziła specjalną ewidencję podatkową na potrzeby stosowania IP Box.

W przypadku spełnienia przez przedsiębiorcę ww. warunków może on w rozliczeniu rocznym zastosować preferencyjną stawkę podatkową IP Box do osiągniętych dochodów, a w konsekwencji – **uzyskać zwrot części uiszczonego podatku dochodowego**.

Wśród przedmiotów zaliczanych do kategorii KPWI i mogących stanowić podstawę zastosowania ulgi IP Box (art. 30ca ustawy PIT) wskazano m.in. autorskie prawo do programu komputerowego. Warto jednocześnie zwrócić uwagę na to, że inne utwory (niestanowiące autorskich praw do programu komputerowego) nie zostały wskazane w katalogu KPWI, a co za tym idzie – nie mogą stanowić podstawy stosowania ulgi IP Box. Z tytułu tak określonych KPWI przedsiębiorca musi osiągać określonego rodzaju dochody, np. z opłat licencyjnych, ze sprzedaży majątkowych praw autorskich czy z KPWI uwzględnionego w cenie sprzedaży produktu lub usługi (zob. art. 30ca ust. 7 ustawy PIT). Dopiero takie dochody, po ich uprzednim wprowadzeniu do prowadzonej przez przedsiębiorcę ewidencji oraz obliczeniu dla nich tzw. wskaźnika *Nexus*[7], mogą stanowić podstawę zastosowania ulgi IP Box.

Kto w praktyce będzie mógł korzystać z IP Box?

W praktyce z ulgi IP Box będą mogli najczęściej korzystać programiści prowadzący działalność gospodarczą i zatrudnieni na podstawie umów B2B, pod warunkiem że:

- tworzą oni stanowiące KPWI autorskie prawa do programu komputerowego oraz
- przenoszą autorskie prawa majątkowe lub udzielają licencji na takie elementy podmiotowi zatrudniającemu w zamian za wyodrębnione w umowie B2B wynagrodzenie.

Dla osób chcących korzystać z tej ulgi podatkowej korzystne jest przy tym stanowisko zaprezentowane w objaśnieniach podatkowych dotyczących stosowania IP Box[8], zgodnie z którym **pojęcie „autorskiego prawa do programu komputerowego" na gruncie przepisów prawa podatkowego należy interpretować szeroko** i powinno ono obejmować nie tylko program komputerowy wyrażony w postaci kodu źródłowego lub wynikowego, lecz także inne sposoby wyrażenia programu komputerowego (np. opisy procedur operacyjnych czy zestawienia danych), interfejsy łączące program komputerowy z innym oprogramowaniem lub sprzętem komputerowym, architekturę systemu, poszczególne moduły funkcjonalne i techniczne oprogramowania czy nawet grafiki i interfejs użytkownika. Może się zatem okazać, że w związku z szerokim rozumieniem pojęcia „autorskiego prawa do programu komputerowego" uprawnieni do stosowania ulgi IP Box będą nie tylko deweloperzy oprogramowania, lecz także inne osoby biorące udział w procesie jego tworzenia – wymagałoby to jednak wcześniejszego uzyskania przez przedsiębiorcę indywidualnej interpretacji podatkowej w tym zakresie.

Co zrobić przed rozpoczęciem korzystania z ulgi IP Box?

Przed rozpoczęciem stosowania ulgi IP Box przedsiębiorcy z branży IT powinni przede wszystkim:

- przeprowadzić analizę pod kątem możliwości stosowania IP Box, w szczególności odnośnie do tego, czy prowadzona przez nich działalność stanowi działalność badawczo-rozwojową oraz czy tworzone przez nich utwory mogą zostać zakwalifikowane jako „autorskie prawa do programów komputerowych";
- uzyskać pozytywną indywidualną interpretację podatkową potwierdzającą możliwość stosowania ulgi IP Box;
- rozpocząć prowadzenie specjalnej ewidencji na potrzeby stosowania ulgi IP Box[9].

Podsumowanie

Zmiany podatkowe wprowadzone Polskim Ładem mogą mieć wpływ na wynagrodzenie pracowników branży IT – zarówno zatrudnionych na podstawie umowy o pracę, jak i zatrudnionych na podstawie kontraktu B2B – prowadząc w niektórych przypadkach do obniżenia otrzymywanego wynagrodzenia netto. 50% koszty oraz ulga IP Box umożliwiają zniwelowanie negatywnych skutków wejścia w życie tych zmian podatkowych, gwarantując pracownikom wyższe wynagrodzenie netto przy zachowaniu dotychczasowych kosztów zatrudnienia.

[7] Ulgę IP Box można stosować do kwalifikowanych dochodów z KPWI, których wysokość ustala się jako iloczyn dochodu osiągniętego z KPWI oraz wskaźnika *Nexus* (zob. art. 30ca ust. 3 i 4 ustawy PIT).

[8] Zob. objaśnienia podatkowe z dnia 15 lipca 2019 r. dotyczące preferencyjnego opodatkowania dochodów wytwarzanych przez prawa własności intelektualnej – IP Box.

[9] Prowadzona ewidencja powinna być zgodna z art. 30cb ustawy PIT.

Zakończenie publicznych konsultacji Urzędu ds. Własności Intelektualnej Wielkiej Brytanii w zakresie regulacji sztucznej inteligencji

MarcinRęgorowicz

Zamknięte 7 stycznia 2022 r. brytyjskie konsultacje publiczne dotyczące zmian w przepisach z zakresu prawa własności intelektualnej z polskiej czy europejskiej perspektywy są interesującym źródłem spostrzeżeń. Konsultacje te obejmują bowiem oceny i propozycje zmian do już obowiązujących przepisów i funkcjonujących w praktyce obrotu prawnego konstrukcji związanych z wykorzystaniem systemów tzw. sztucznej inteligencji. Co istotne, omawiane regulacje nie są skupione na bezpieczeństwie i etyce stosowania systemów sztucznej inteligencji (jak w przypadku propozycji unijnych przepisów), ale dotyczą bardziej praktycznych dla obrotu prawnego kwestii – takich jak kwalifikacja i ochrona utworów powstających bez udziału człowieka.

Zakres konsultacji

Zakończone 7 stycznia 2022 r. konsultacje publiczne dotyczące sztucznej inteligencji zostały otwarte przez Urząd ds. Własności Intelektualnej Wielkiej Brytanii we wrześniu 2021 r. Były to już drugie konsultacje w tym zakresie (pierwsze odbyły się w okresie od końca 2020 r. do marca 2021 r.). Ich głównym celem było zebranie poglądów i stanowisk zainteresowanych podmiotów w dwóch zasadniczych kwestiach. Po pierwsze: w jakim zakresie prawo autorskie i prawo własności przemysłowej powinno regulować i chronić utwory czy wynalazki stworzone przez systemy sztucznej inteligencji. Po drugie przedmiotem konsultacji było zbadanie, w jakim zakresie należy umożliwić korzystanie z wytworów systemów sztucznej inteligencji w celu wsparcia innowacji i rozwoju gospodarczego.

Omawiane konsultacje publiczne obejmowały głównie przepisy brytyjskiego prawa własności intelektualnej zawarte w ustawie z 1988 r. – Copyright, Designs and Patents Act (dalej: „CDPA"). Mowa przede wszystkim o regulacjach instytucji utworów wygenerowanych komputerowo (*computer-generated works*), kwestii zmian definicji pojęcia wynalazcy na gruncie prawa patentowego w celu uwzględniania wynalazków wytwarzanych przy udziale systemów sztucznej inteligencji (m.in. rozszerzenia definicji wynalazcy czy możliwości wskazywania systemów SI jako wynalazcy we wnioskach u udzielenie patentu) oraz wyjątków od ochrony prawnoautorskiej w ramach wykorzystywania utworów bez zgody uprawnionych na potrzeby komputerowej analizy danych (*text and data mining*).

Computer-generated works

Z perspektywy prawa autorskiego szczególnie interesujące jest poddanie konsultacjom publicznym już obowiązujących w Wielkiej Brytanii przepisów, na podstawie których chronione są utwory wygenerowane przez komputer (*computer-generated works*). Są one wprost zdefiniowane w przepisach brytyjskiego prawa własności intelektualnej jako utwory, które zostały wygenerowane komputerowo w takich okolicznościach, że brak jest człowieka będącego autorem (twórcą) danego utworu („*the work is generated by computer in circumstances such that there is no human author of the work*", art. 178 CDPA). Utwory takie objęte są ochroną prawnoautorską przez okres 50 lat (art. 12 ust. 7 CDPA), a prawa autorskie do takiego utworu przysługują osobie, która podjęła działania niezbędne do jego wytworzenia („*person by whom the arrangements necessary for the creation of the work are undertaken*", art. 9 ust. 3 CDPA).

Co interesujące, konsultacje publiczne w zakresie powyższych regulacji związane były m.in. z krytyką instytucji utworów wygenerowanych komputerowo, w ramach której w szczególności wskazywano, że przyznana ochrona jest zbyt szeroka lub wręcz zbędna. W ramach konsultacji respondenci byli przede wszystkim zachęcani do zajęcia stanowiska, czy regulacja ma pozostać w mocy, zostać całkowicie zniesiona, czy też zastąpiona nowym typem prawa o ograniczonym zakresie bądź czasie ochrony.

Podsumowanie

Wynik omawianych konsultacji i wnioski z nich mogą być interesujące również z polskiej czy unijnej perspektywy – dotyczą bowiem oceny rzeczywiście funkcjonującej w obrocie prawnym instytucji odmiennej od założeń przyjmowanych w ramach planowanej europejskiej regulacji. Mogą zatem być źródłem cennych informacji dla doktryny prawa autorskiego i ustawodawcy na potrzeby tworzenia regulacji związanych ze sztuczną inteligencją w polskim porządku prawnym. Zwłaszcza że mowa tutaj o bardzo konkretnej i fundamentalnej dla praktyki obrotu prawnego i gospodarczego kwestii ochrony prawnej utworów wytwarzanych rzeczywiście przez systemy sztucznej inteligencji bez bezpośredniego udziału człowieka.

Brytyjskie doświadczenia w powyższym zakresie oparte są bowiem na modelu regulacji odmiennym niż proponowany aktualnie przez instytucje unijne w ramach toczących się prac legislacyjnych. Wskazać należy, że w ramach Rezolucji Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji przyjęto odmienne od brytyjskich założenia – zgodnie z którymi utwory stworzone wyłącznie przez systemy sztucznej inteligencji nie powinny być chronione na gruncie przepisów prawa autorskiego (przede wszystkim ze względu na fundamentalne założenie związania praw do utworów z osobą fizyczną będącą twórcą), a na podstawie odrębnej kategorii uprawnień. W powyższym kontekście oraz wobec faktu wyjścia Wielkiej Brytanii z Unii Europejskiej, wynik brytyjskich prac może być szczególnie interesujący dla dalszych prac w UE dotyczących rodzaju praw ochronnych dla wytworów sztucznej inteligencji.

Usługi telekomunikacyjne dla osadzonych – planowane ciche upaństwowienie rynku

Kamila Dymek

Projekt ustawy o zmianie ustawy o Służbie Więziennej oraz niektórych innych ustaw został opublikowany 4 listopada 2021 r. na stronie Rządowego Centrum Legislacji. Proponowane w nim zmiany w trzech ustawach – ustawie o Służbie Więziennej[1], Kodeksie karnym wykonawczym[2] oraz Prawie zamówień publicznych[3] – w połączeniu mają zrewolucjonizować świadczenie usług telekomunikacyjnych w zakładach karnych i aresztach śledczych. Wprowadzenie przepisów w projektowanym kształcie w zasadzie zamknie rynek w sektorze usług telekomunikacyjnych dla osadzonych.

Nowelizacja przewiduje powołanie przywięziennego zakładu pracy do realizacji uprawnień osadzonych do rozmów telefonicznych, co prowadzić ma do ujednolicenia zasad korzystania z aparatów telefonicznych. Zgodnie z projektem umowę na realizację usług telefonicznych będą zawierać dyrektor generalny Służby Więziennej z dyrektorem przywięziennego zakładu pracy wskazanym przez Ministra Sprawiedliwości.

Powyższe oznacza, że dostarczaniem usług telekomunikacyjnych dla osadzonych zajmie się najprawdopodobniej jeden wybrany podmiot zamiast — jak dotychczas — przedsiębiorców telekomunikacyjnych wybieranych w postępowaniach, które co do zasady powinny być przeprowadzane z zachowaniem kryterium transparentności i konkurencyjności. Obecnie w zakładach penitencjarnych funkcjonuje kilka wyspecjalizowanych podmiotów, które ze sobą konkurują.

Zgodnie z uzasadnieniem ww. projektu ustawy nowelizacja ma na celu zapewnienie realizacji kodeksowego prawa osób pozbawionych wolności do prowadzenia rozmów telefonicznych, przy czym projektodawca przyjmuje założenie, że gwarancją tego będzie przeprowadzanie rozmów w jednakowy sposób i na takich samych zasadach we wszystkich jednostkach penitencjarnych. Ponadto treść uzasadnienia wskazuje, że w efekcie realizacji przedsięwzięcia mają zostać wdrożone mechanizmy umożliwiające skuteczne wykonanie kodeksowego obowiązku kontroli rozmów telefonicznych osadzonych, co ma poprawić bezpieczeństwo w jednostkach.

[1] Ustawa z dnia 9 kwietnia 2010 r. o Służbie Więziennej (t.j. Dz. U. z 2021 r., poz. 1064).
[2] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (t.j. Dz. U. z 2021 r., poz. 53).
[3] Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2021 r., poz. 1129).

21 grudnia 2021 r. opublikowano uwagi Prezesa Urzędu Ochrony Konkurencji i Konsumentów (UOKiK) do ww. projektu ustawy. Prezes UOKiK wskazuje, że proponowane rozwiązania niewątpliwie wpłyną na poziom konkurencji na rynku usług telekomunikacyjnych w jednostkach penitencjarnych, a ich wpływ na przedsiębiorców działających na wskazanym rynku nie został wyczerpująco wyjaśniony w uzasadnieniu projektu. Proponowane zmiany dotkną przy tym w szczególności operatorów, którzy poczynili znaczne inwestycje na tworzenie obecnej infrastruktury telekomunikacyjnej w zakładach karnych i aresztach śledczych (często niedemontowalnej) oraz mają zobowiązania wobec abonentów w formie niewykorzystanych środków finansowych. Jak podkreśla Prezes UOKiK, w przypadku niektórych z tych przedsiębiorców jedynym lub głównym przedmiotem działalności jest świadczenie usług telefonicznych dla osób osadzonych, a co za tym idzie – wprowadzenie nowych przepisów zmusi ich do całkowitego zamknięcia działalności.

Podkreślenia wymaga również fakt, że wnioskodawca, umieszczając proponowane regulacje w ustawach, które swoim zakresem co do zasady nie normują działalności telekomunikacyjnej, sprawił, że planowana nowelizacja była trudno dostrzegalna dla branży. Co więcej, w zaproszeniu do przesyłania opinii w ramach konsultacji publicznych pominięte zostały izby branżowe zrzeszające przedsiębiorców telekomunikacyjnych.

Po nagłośnieniu sprawy pojawiły się liczne głosy krytyki wobec zaproponowanych w projekcie zmian. Przedstawiciele branży w swoich stanowiskach podkreślają w szczególności, że eliminacja wszystkich, poza jednym, przedsiębiorców z rynku świadczenia usług telekomunikacyjnych dla osadzonych doprowadzi do utworzenia monopolu, centralizacji i ograniczenia swobody prowadzenia działalności gospodarczej. Ucierpi na tym również bezpieczeństwo realizacji usług telekomunikacyjnych w jednostkach penitencjarnych. W związku z powyższymi zastrzeżeniami na rynku postulowane jest m.in. dokonanie stosownej oceny skutków regulacji, wprowadzenie dłuższego okresu przejściowego, a także ustalenie odpowiedniej rekompensaty dla przedsiębiorców.

Prace nad nowelizacją są obecnie na etapie opiniowania. Dalsze etapy procesu legislacyjnego można śledzić tutaj.

Kara umowna za zwłokę bez określonego limitu

Piotr Nepelski

Sąd Najwyższy stanął na stanowisku, że: „Dopuszczalne jest zastrzeżenie kary umownej za zwłokę w wykonaniu zobowiązania w postaci określonego procentu ustalonego wynagrodzenia umownego za każdy dzień zwłoki, nawet jeżeli nie określono końcowego terminu naliczania kary umownej ani jej kwoty maksymalnej”[1].

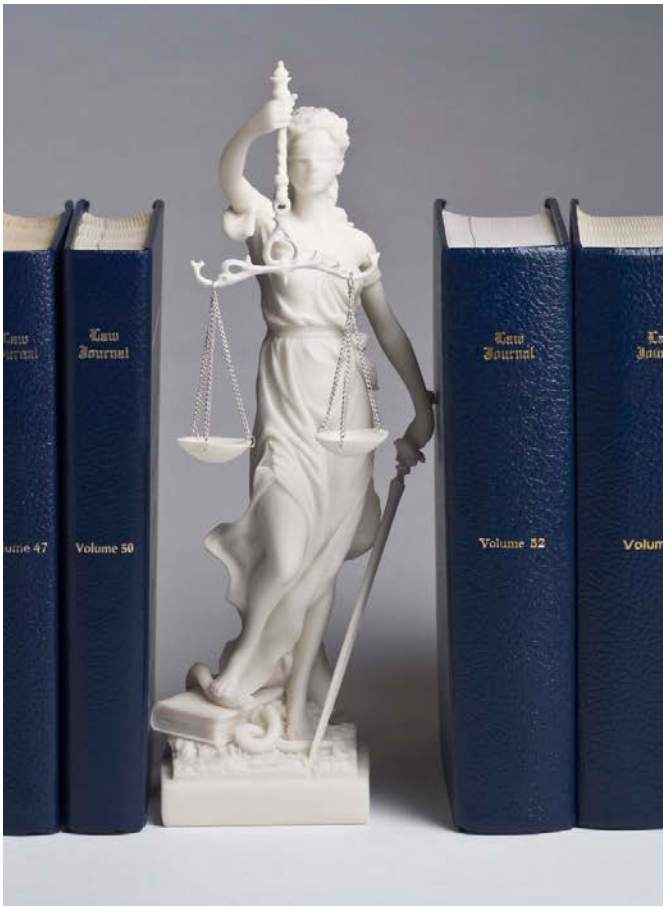
Zostało już opublikowane uzasadnienie orzeczenia. Wynika z niego, że źródłem zapytania prawnego był spór, w którym powód naliczył pozwanemu karę umowną za zwłokę w wykonaniu przedmiotu umowy w wysokości 2% wynagrodzenia brutto wartości umowy za każdy dzień zwłoki. Sąd Rejonowy oddalił powództwo, stając na stanowisku, że postanowienie zastrzegające karę umowną jest bezwzględnie nieważne. Sąd I instancji odwołał się do wyroku Sądu Najwyższego z 22 października 2015 r., IV CSK 687/14, przyjmując, że niemożliwe jest zastrzeżenie kary umownej bez określenia terminu końcowego jej naliczania ani kwoty maksymalnej, gdyż prowadziłoby to do obciążenia dłużnika zobowiązaniem wieczystym.

Od rozstrzygnięcia Sądu Rejonowego została wniesiona apelacja do Sądu Okręgowego. Sąd II instancji powziął wątpliwość wyrażoną w zagadnieniu prawnym przedstawionym do rozstrzygnięcia Sądowi Najwyższemu.

Sąd Najwyższy wydając uchwałę, wskazał m.in. na następujące:

- nie ma ogólnego przepisu, który wprost zakazywałby zastrzegania kary umownej bez określenia jej maksymalnej wysokości;
- na tle sformułowań użytych w art. 483 § 1 k.c.[2] wątpliwości może budzić zastrzeżenie „określonej sumy”, lecz w tym zakresie wystarczające jest określenie kary przez oznaczenie (procentowe lub wprost) należnej kwoty za każdy dzień zwłoki.

Sąd Najwyższy porównał ponadto zobowiązanie do zapłaty kary umownej do roszczenia o zapłatę odsetek, wchodząc w rozważania na temat charakteru zobowiązania ciągłego i płaconego periodycznie. Niemniej dla praktyków prawa istotna jest konkluzja rozważań Sądu Najwyższego. Rynek wstrzymywał bowiem oddech w obawie, że rozstrzygnięcie pójdzie w przeciwnym kierunku. Stawiałoby to pod znakiem zapytania skuteczność postanowień wielu umów, włącznie ze skutecznością kar umownych już pobranych przez stronę umowy.



[1] Sentencja uchwały dostępna jest na stronie internetowej Sądu Najwyższego: http://www.sn.pl/sprawy/SitePages/Zagadnienia_prawne.aspx?ItemSID=1503-301f4741-66aa-4980-b9fa-873e90506a11&ListName=Zagadnienia_prawne (dostęp: 20.01.2022).
[2] Ustawa z dnia z dnia 23 kwietnia 1964 r. Kodeks cywilny (tj. Dz. U. z 2020 r. poz. 1740).

Orzeczenie Sądu Najwyższego w praktyce oznacza, że możliwe jest zastrzeganie kary umownej np. za zwłokę we wdrożeniu systemu teleinformatycznego lub dostawie sprzętu IT bez ograniczenia limitu tejże kary. A przynajmniej w obrocie prywatnym, ponieważ w przypadku umów zawieranych w reżimie ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2021 r., poz. 1129; dalej: „PZP") prawodawca przewidział obowiązek określenia limitu kar. Stosownie do art. 436 pkt 3 PZP umowa w sprawie zamówienia publicznego zawiera postanowienie o łącznej maksymalnej wysokości kar umownych, których mogą dochodzić strony.

Orzeczenie w sprawie III CZP 16/21 nie wyłącza obowiązku określenia tego limitu w umowach w sprawie zamówienia publicznego. Co więcej, do tej regulacji odwołał się Sąd Najwyższy wskazując, że art. 436 pkt 3 PZP odnosi się wyłącznie do stosunków prawnych regulowanych PZP (spór natomiast dotyczył relacji generalnego wykonawcy z podwykonawcą), a ponadto, że ustanawia on normę szczególną na tle całości systemu prawnego, gdyż w innym wypadku jego wprowadzenie trudno byłoby uznać za racjonalne.

Warto dodać, że rygor z art. 436 pkt 3 PZP nakazuje wprowadzić limit wszelkich kar umownych, które zostały określone w umowie. Nie tworzy takiego wymagania w stosunku do każdej kary umownej z osobna. Logiczną konsekwencją tego ograniczenia jest jednak limitowanie wysokości każdej z kar umownych z osobna, w tym np. kary umownej za zwłokę w dostawie sprzętu IT.

Niezależnie od powyższego, konstruując postanowienia o karach umownych, warto pamiętać o problemach, które mogą się pojawić w toku realizowania umowy. W przypadku zamawiających publicznych zbyt rygorystycznie określone kary umowne mogą tworzyć problem związany z potrzebą ich egzekwowania (w obawie o naruszenie dyscypliny finansów publicznych), kiedy zamawiający z różnych powodów może nie być tym zainteresowany (np. nie chcąc pogarszać relacji z wykonawcą). Ponadto zbyt wysokie kary umowne wzmacniają ryzyko ich miarkowania przez sąd, jeśli doszłoby do sporu sądowego.

Nowy, „słabszy" skutek zawezwania do próby ugodowej: zawieszenie zamiast przerwania biegu przedawnienia

Piotr Nepelski

W dniu 29 grudnia 2021 r. została ogłoszona Ustawa z dnia 2 grudnia 2021 r. o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz. U. z 2021 r., poz. 2459)[1]. Ustawa wchodzi w życie po upływie 6 miesięcy od dnia ogłoszenia (z wyłączeniem art. 4 i art. 11, które weszły w życie z dniem następującym po dniu ogłoszenia, oraz art. 3 i art. 5–7, które weszły w życie 1 stycznia 2022 r.). Ustawa zawiera istotną zmianę skutku zawezwania do próby ugodowej. Zgodnie z treścią znowelizowanego art. 121 ust. 6 k.c.[2] zawezwanie nie będzie już przerywać biegu przedawnienia roszczenia, lecz jedynie je zawieszać na czas prowadzenia postępowania pojednawczego. Zamiast przerwania terminu przedawnienia będzie on ulegał jedynie przedłużeniu o czas trwania przeszkody (okres trwania postępowania pojednawczego).

Kontekst zmian

Nowe zmiany kończą trwające od lat wątpliwości na temat doniosłości prawnej, na którą zasługuje złożenie wniosku o zawezwanie do próby ugodowej. Do momentu uchwalenia nowelizacji przyjmowało się, że do przerwania biegu terminu przedawnienia dochodzi m.in. na skutek złożenia pierwszego wniosku o zawezwanie do próby ugodowej – jako czynności podjętej przed sądem bezpośrednio w celu dochodzenia lub ustalenia albo zaspokojenia lub zabezpieczenia roszczenia. Przedmiotem kontrowersji pozostawało jednak to, czy ten sam skutek odnosiły także kolejne wezwania do próby ugodowej.

W powszechnej opinii nowelizacja przepisów Kodeksu cywilnego dot. skutków wniosku o zawezwanie do próby ugodowej wpłynie znacząco na dotychczasowe praktyki zarządzania sporami[3]. W praktyce wniosek ten (czasami składany w ostatnim dniu przed upływem terminu) często składany był tylko po to, aby przerwać bieg terminu przedawnienia roszczenia, tworząc fikcję chęci rozpoczęcia postępowania pojednawczego. Takie postępowanie często uznawane jest za sprzeczne z samą istotą instytucji przedawnienia, której głównym celem jest stabilizacja obrotu prawnego.

Jak wskazywano w motywach uzasadnienia ustawy, takie działanie „nie jest również zgodne z podstawowym założeniem postępowania pojednawczego, którym jest zawarcie ugody, a nie przerwanie biegu przedawnienia. Dodatkowo może prowadzić do skrajnej sytuacji, w której roszczenie, co do którego są składane wnioski o zawezwanie do próby ugodowej, nigdy nie ulegnie przedawnieniu"[4].

Skutek zawezwania do próby ugodowej w orzecznictwie Sądu Najwyższego

W orzecznictwie Sądu Najwyższego kwestia skutku zawezwania do próby ugodowej była rozstrzygana niejednolicie. Przykładowo Sąd Najwyższy w uchwale z dnia 28 czerwca 2006 r., sygn. akt III CZP 42/06, stwierdził, że zawezwanie do próby ugodowej przerywa bieg przedawnienia. W późniejszym orzecznictwie Sądu Najwyższego (uchwała z dnia 15 listopada 2012 r., V CSK 515/11) sprecyzowano, że „zawezwanie do próby ugodowej przerywa bieg terminu przedawnienia na podstawie art. 123 § 1 pkt 1 k.c. tylko wówczas, gdy określona w nim wierzytelność obejmuje precyzyjnie określenie zarówno przedmiotu żądania, jak i jej wysokości".

W innych natomiast orzeczeniach Sądu Najwyższego (wyrok z dnia 28 stycznia 2016 r., III CSK 50/15; wyrok z dnia 19 lutego 2016 r., V CSK 365/15; wyrok z dnia 10 stycznia 2017 r., V CSK 204/16) dostrzegalne było kształtowanie się poglądu, według którego możliwe jest, że drugi wniosek nie wywoła już skutku w postaci przerwania biegu terminu. Kluczowe jest kryterium bezpośredniości, interpretowane jako rzeczywisty charakter zamiaru wnioskodawcy[5].

Powyższe wątpliwości, przynajmniej częściowo, stracą na znaczeniu wskutek uchwalonych zmian w przepisach prawa.

[1] Akt prawny można znaleźć pod adresem: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20210002459/O/D20212459.pdf (dostęp: 24.01.2022).
[2] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2020 r., poz. 1740; dalej: „k.c.").
[3] Jedno zawezwanie do próby ugodowej mogło wydłużyć trzyletni termin przedawnienia o kolejne trzy lata.
[4] Uzasadnienie do projektowanej zmiany art. 121, art. 123 i art. 124 k.c., str. 1, dostępne pod adresem: https://www.sejm.gov.pl/sejm9.nsf/druk.xsp?nr=1344 (dostęp: 24.01.2022).
[5] *Kodeks cywilny. Komentarz*, red. E. Gniewek, P. Machnikowski, Warszawa 2021.

NADCHODZĄCE WYDARZENIA

4.03.2022
KONGRES

KONGRES PRAWA NOWYCH TECHNOLOGII

Nowe zasady dostępności i wykorzystywania danych w obrocie cyfrowym w Unii Europejskiej – adw. prof. INP PAN dr hab. Grzegorz Sibiga

Esport – ramy prawne w Polsce – adw. Xawery Konarski

Umowy na rozwiązania Low-Code / No-Code – wyzwania prawne dla nowego modelu tworzenia i wdrażania – r.pr. Agnieszka Wachowska, r.pr. Marcin Ręgorowicz

Więcej informacji >>

8.03.2022
SZKOLENIE

NIEWYKONANIE LUB NIENALEŻYTE WYKONANIE UMOWY IT – CO ZROBIĆ ABY UNIKNĄĆ SPORU I JAK SIĘ ZACHOWAĆ W SYTUACJACH KOLIZYJNYCH POMIĘDZY WYKONAWCĄ I ZAMAWIAJĄCYM?

adw. Xawery Konarski, r. pr. Agnieszka Wachowska

Więcej informacji >>

22.03.2022
SZKOLENIE

UMOWY NA UTRZYMANIE, SERWIS I ROZWÓJ SYSTEMÓW IT – NAJLEPSZE PRAKTYKI I SPORNE KWESTIE

r. pr. Agnieszka Wachowska

Więcej informacji >>

30-31.03.2022
KONFERENCJA

UMOWY WDROŻENIOWE NA SYSTEMY IT – ASPEKTY PRAWNE I PRAKTYCZNE

adw. Xawery Konarski, r. pr. Agnieszka Wachowska

Więcej informacji >>

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

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

Jakub Chlebowski
Radca prawny, Senior Associate
jakub.chlebowski@traple.pl

Marcin Ręgorowicz
Radca prawny, Senior Associate
marcin.regorowicz@traple.pl

Małgorzata Kotwica
Associate
malgorzata.kotwica@traple.pl

Aleksander Elmerych
Aplikant radcowski, Associate
aleksander.elmerych@traple.pl

Kamila Dymek
Junior Assosiate
kamila.dymek@traple.pl

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

Redaktorka newslettera:
adw. Karolina Grochecka-Goljan