NR 2 - MARZEC 2021

NEWSLETTER

IT-TECH

W NUMERZE M.IN.:

- Dekompilacja na potrzeby naprawy błędów możliwa, jeśli nie zabrania tego umowa
- Nowy projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa
- Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020 uchwalona
- Wytyczne SWIPO pomogą uniknąć chmurowego vendor lock-in
- Wstrzymanie świadczenia serwisu oprogramowania a obowiązek zapłaty wynagrodzenia

Traple
Konarski
Podrecki
& Wspólnicy

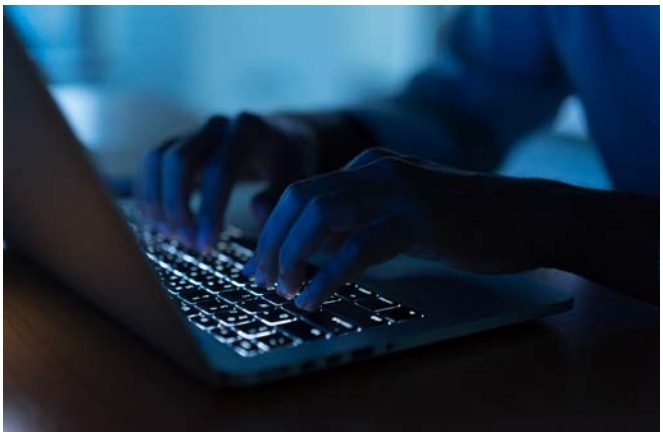
TKP

Nowy projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa

Joanna Jastrząb

Pierwszy projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa został opublikowany we wrześniu 2020 r. – wzbudził wtedy niemałe emocje, związane zarówno z propozycjami nowych przepisów, jak i z trybem jego procesowania. O projekcie pisaliśmy w poprzednim wydaniu newslettera: klik.

Po zebraniu uwag przez dłuższy czas brak było informacji, jakie są dalsze losy projektu. Do czasu, aż 20 stycznia 2021 r. opublikowano jego nową, drugą wersję. Przebieg prac nad projektem jest dostępny pod linkiem: klik. W momencie przygotowywania newslettera projekt nie został jeszcze skierowany do prac w Sejmie. Poniżej omówione zostaną najistotniejsze propozycje zmian.



Nowością w projekcie z 20 stycznia 2021 r. są przepisy dotyczące procesu certyfikacji, zapowiadane zresztą od dłuższego czasu (art. 59a projektu i kolejne). Proponowane regulacje są wzorowane na przepisach aktu o cyberbezpieczeństwie – unijnego rozporządzenia, które wyznacza ramy europejskiej certyfikacji procesów, produktów i usług ICT. Zgodnie z uzasadnieniem projektu przyjęte rozwiązania zakładają mieszany model certyfikacji cyberbezpieczeństwa, w którym podstawową rolę odgrywają podmioty prywatne. Certyfikacja będzie odbywała się na zasadach rynkowych, a klienci będą mogli swobodnie wybierać spośród podmiotów działających na rynku. Co istotne, zgodnie z projektem certyfikacja w zakresie cyberbezpieczeństwa będzie procesem całkowicie dobrowolnym.

W projekcie z 20 stycznia 2021 r. nie znalazły się poprzednio przedstawione przepisy dotyczące włączenia przedsiębiorców komunikacji elektronicznych do krajowego systemu cyberbezpieczeństwa. Nie oznacza to, że projektodawca zrezygnował z tego pomysłu; po prostu ujął go w innym projekcie dotyczącym przepisów wprowadzających – Prawo komunikacji elektronicznej (klik). Kwestia ta nie jest jednak jeszcze przesądzona – nie jest wykluczone, że na etapie dalszych prac podejście ulegnie zmianie.

Z projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa nie skreślono propozycji wprowadzenia oceny profili ryzyka dostawców, choć zmieniono – wobec licznych zgłoszonych zastrzeżeń – podmiot dokonujący takiej oceny. Zgodnie z projektem z 20 stycznia 2021 r. (art. 66a i kolejne) byłby to minister właściwy ds. informatyzacji, który w ramach postępowania administracyjnego mógłby wydać decyzję o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli z przeprowadzonego badania wynikałoby, że dostawca ten stanowi poważne zagrożenie dla bezpieczeństwa narodowego. Taka decyzja miałaby istotne znaczenie m.in. dla podmiotów krajowego systemu cyberbezpieczeństwa, które byłyby zobowiązane do wycofania sprzętu lub oprogramowania wskazanego dostawcy w określonym w projekcie okresie.

Na pozór nieznaczne zmiany wobec wrześniowej propozycji nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa zostały wprowadzone także do instytucji ostrzeżeń i poleceń zabezpieczających w zakresie zapobiegania i zwiększenia skuteczności reagowania na incydenty krytyczne (art. 67a i kolejne projektu z 20 stycznia 2021 r.). Będą mogły być one stosowane w przypadku ryzyka wystąpienia (ostrzeżenie) lub po zaistnieniu incydentu krytycznego, czyli najpoważniejszego z rodzajów incydentów, mającego znaczenie m.in. dla bezpieczeństwa lub porządku publicznego, w celu skoordynowania efektywnej reakcji (polecenie zabezpieczające).

Ostrzeżenie ma być w założeniu miękkim, niewiążącym środkiem wydawanym przez pełnomocnika rządu ds. cyberbezpieczeństwa, wskazującym na ryzyko związane z możliwością

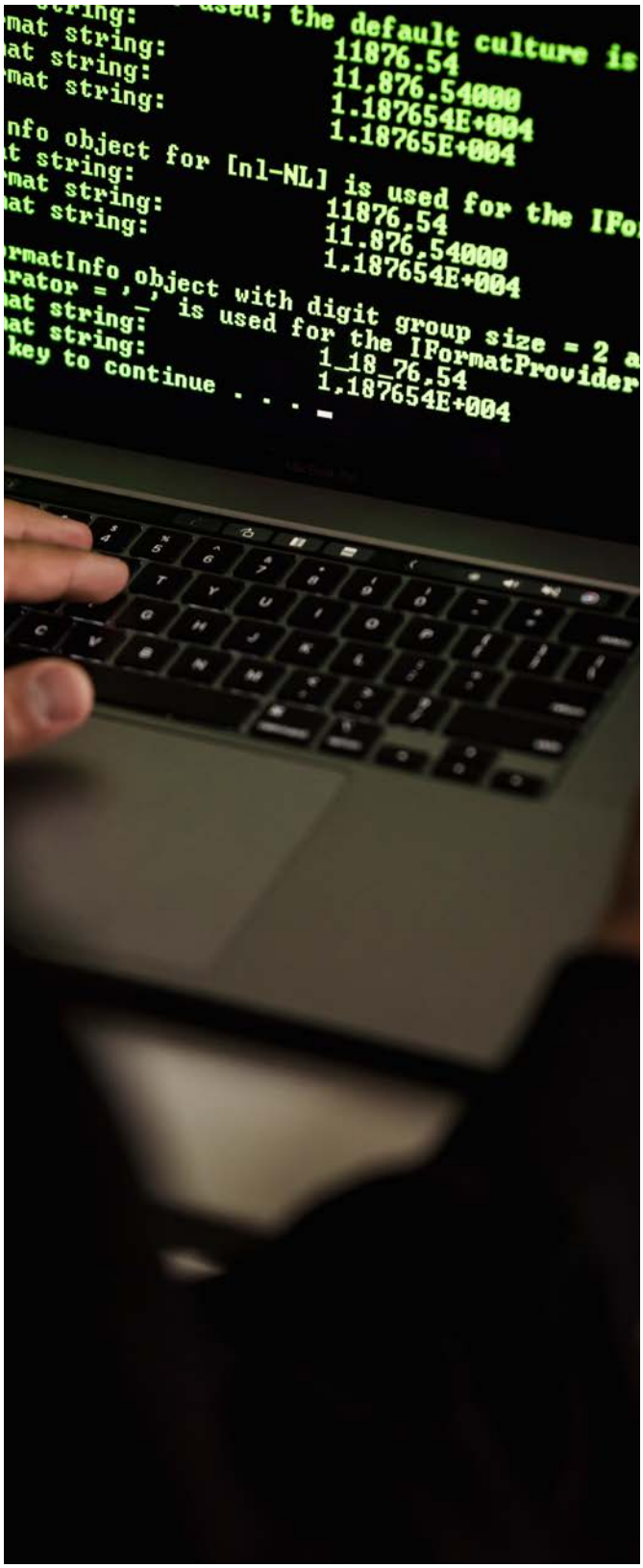
wystąpienia incydentu krytycznego oraz zalecającym określone działania zmniejszające ryzyko jego wystąpienia. Nowelizacja zawiera katalog działań, które mogą być „zalecone" do podjęcia – np. odstąpienie od korzystania z określonego sprzętu lub oprogramowania, dokonanie określonej konfiguracji sprzętu/ oprogramowania.

Z kolei minister właściwy ds. informatyzacji będzie mógł wydać w formie decyzji administracyjnej polecenie zabezpieczające w przypadku wystąpienia incydentu krytycznego. Zgodnie z projektem polecenie zabezpieczające będzie wydawane w sytuacji zapewnienia koordynacji reakcji na incydent krytyczny oraz konieczności ograniczenia jego skutków. Będzie zawierało wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu. Katalog zachowań został wskazany w art. 67b ust. 9 i jest podobny – ale nie identyczny – do katalogu dla ostrzeżeń. Jego wykonanie jest zabezpieczone karą administracyjną do 3% rocznego obrotu. Co jest kontrowersyjne, to czas, na jaki te zachowania mogą zostać wprowadzone (aż do 2 lat), i możliwość odstąpienia od sporządzenia uzasadnienia faktycznego decyzji dotyczącej tego polecenia (jeśli wymagają tego względy obronności lub bezpieczeństwa państwa bądź bezpieczeństwa i porządku publicznego).

W projekcie z 20 stycznia 2021 r. utrzymano inne propozycje z poprzedniego projektu, takie jak:

- wprowadzenie obowiązków wojewody dotyczących wymiany informacji w województwie (art. 24a);
- włączenie do krajowego systemu cyberbezpieczeństwa ISAC (centra wymiany i analizy informacji) – choć konkretne przepisy przeredagowano (art. 25a);
- uregulowanie SOC jako jednostki odpowiedzialnej za realizację zadań przez operatorów usług kluczowych – wciąż jednak SOC może być powołany wewnątrz organizacji danego operatora usługi kluczowej lub stanowić odrębny podmiot (art. 14).

W momencie przygotowywania newslettera przyjęcie przez rząd wyżej wskazanych przepisów nie jest jeszcze przesądzone, a przedstawiciele rynku i organizacji branżowych wciąż zgłaszają swoje uwagi i postulaty. Nie jest więc wykluczone, że projekt nowelizacji, który trafi do Sejmu, uwzględni chociaż część z postulowanych zmian.



"Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020" uchwalona

Karolina Grochecka-Goljan, Dominika Duda

Pod koniec grudnia 2020 r. Rada Ministrów uchwaliła „Politykę dla rozwoju sztucznej inteligencji w Polsce od roku 2020"[1] (dalej: „Polityka AI"). To dokument wskazujący główne działania i cele dla Polski w zakresie szeroko pojętego rozwoju oraz badania sztucznej inteligencji w trzech perspektywach czasowych: krótkoterminowej (do 2023 r.), średnioterminowej (do 2027 r.) i długoterminowej (po 2027 r.). Jest on częścią tworzonej nowej polskiej Strategii Produktywności oraz planu „Sprawne i Nowoczesne Państwo 2030". W Polityce AI wskazano, że jej treść została zaprojektowana na podstawie kierunkowych działań państwa, Unii Europejskiej, a także w konsekwencji przyjęcia dokumentów przez organizacje międzynarodowe. Jednocześnie uwzględnia ona cele wskazane w dokumentach strategicznych, m.in. Strategii Odpowiedzialnego Rozwoju, komunikacie Komisji Europejskiej „Skoordynowany plan w sprawie sztucznej inteligencji" i innych wymienionych w Polityce AI.

Cele i zadania określone w Polityce AI

Polityka AI przedstawia ponad 200 zadań w zakresie rozwoju oraz badania sztucznej inteligencji dla podmiotów sektora zarówno publicznego, jak i prywatnego. Polityka AI uwzględnia rozwój ekosystemu AI, w tym następujące wymiary w ramach polskiego ekosystemu AI: międzynarodowy, standardów technicznych i organizacyjnych, prawny oraz etyczny. Rada Ministrów zaznacza przy tym, że Polityka AI będzie wymagać ewaluacji i aktualizacji ze względu na charakter sektora nowoczesnych technologii, który ulega ciągłej zmianie.

Działania i cele dla Polski określone w Polityce AI zostały podzielone na sześć głównych obszarów:

- **AI i społeczeństwo** – działania, które mają uczynić z Polski jednego z większych beneficjentów gospodarki opartej na danych, a z Polaków –społeczeństwo świadome konieczności ciągłego podnoszenia wiedzy i umiejętności, w tym kompetencji cyfrowych;
- **AI i innowacyjne firmy** – działania, których celem jest wspieranie polskich przedsiębiorstw AI, tworzenie mechanizmów finansowania ich rozwoju, zwiększanie ilości zamówień, współpraca start-upów z rządem i wdrażanie nowych, prorozwojowych regulacji (piaskownic cyfrowych);
- **AI i nauka** – działania wspierające polskie środowisko naukowe i badawcze w projektowaniu interdyscyplinarnych wyzwań lub rozwiązań w obszarze AI, z uwzględnieniem nauk humanistycznych i społecznych, a także tworzenie katedr AI, kształcenie doktorantów, przyznawanie grantów dla badaczy oraz inne czynności mające na celu przygotowanie kadry ekspertów zdolnych do wytworzenia rozwiązań AI, z uwzględnieniem ram etycznego i bezpiecznego wykorzystania tej technologii, z pożytkiem dla gospodarki i dobrobytu obywateli;
- **AI i edukacja** – działania podejmowane od kształcenia podstawowego przez poziom ponadpodstawowy aż do poziomu uczelni – programy kursów dla osób zagrożonych utratą pracy w wyniku postępującej automatyzacji i wdrażania nowych technologii, granty edukacyjne, które mają pomóc w przygotowaniu najlepszych kadr dla polskiej gospodarki związanej z AI;
- **AI i współpraca międzynarodowa** – działania na arenie międzynarodowej, które wesprą promocję polskiego biznesu w zakresie AI oraz rozwój technologii AI z poszanowaniem godności człowieka i jego praw podstawowych, zgodnie ze standardami UE i OECD, a także działania dyplomacji cyfrowej w obszarze polityk lub regulacji dotyczących sztucznej inteligencji;
- **AI i sektor publiczny** – działania, które mają wesprzeć sektor publiczny w realizacji zamówień na rzecz AI, lepszej koordynacji działań i dalszym rozwoju takich programów jak GovTech Polska oraz w zapewnieniu ochrony ludności adekwatnej do zagrożenia.

[1] Tekst Polityki AI dostępny tutaj: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20210000023/O/M20210023.pdf (dostęp: 1.03.2021).

Podmioty odpowiedzialne za wdrażanie Polityki AI

Koordynacja wdrażania Polityki AI będzie realizowana przez ministra właściwego do spraw informatyzacji. Polityka AI zakłada również stworzenie Zespołu Zadaniowego Polityki AI – funkcjonującego przy Komitecie Rady Ministrów do spraw Cyfryzacji – który będzie odpowiedzialny za operacyjne aspekty wdrażania Polityki AI w Polsce. Wykonywanie zadań w ramach Polityki AI ma być oparte na planach wykonawczych przygotowywanych przez ministrów i przedstawianych corocznie ministrowi właściwemu do spraw informatyzacji, a następnie analizowanych przez Zespół Zadaniowy Polityki AI. Plany te mają zawierać m.in. wykaz działań, celów oraz planowanych kosztów, a także źródła ich finansowania.

Zgodnie z informacjami wskazanymi w Załączniku nr 2 do Polityki AI oprócz Zespołu Zadaniowego Polityki AI – działającego przy Komitecie Rady Ministrów do spraw Cyfryzacji – w celu skutecznego monitorowania, realizowania i koordynowania Polityki AI planowane jest powołanie następujących organów:

- Punktu Kontaktowego AI;
- Obserwatorium AI dla Rynku Pracy;
- Obserwatorium Międzynarodowej Polityki Sztucznej Inteligencji i Transformacji Cyfrowej;
- Rady AI;
- Zespołu legislacyjnego AI.

Definicja sztucznej inteligencji

Polityka AI przyjęła za własną definicję systemu AI wypracowaną przez zespół niezależnych ekspertów grupy AIGO utworzonej w ramach Organizacji Współpracy Gospodarczej i Rozwoju (ang. Organisation for Economic Co-operation and Development; OECD).

Zgodnie z przywołaną w dokumencie definicją OECD system AI to system oparty na koncepcji maszyny, która może wpływać na środowisko, formułując zalecenia, przewidywania lub decyzje dotyczące zadanego zestawu celów.

Analogicznie jak w przypadku rezolucji Parlamentu Europejskiego z dnia 20 października 2020 r., Polityka AI podkreśla, że system AI powinien być zgodny z zasadą nadzorczej roli człowieka[2], a także opierać się na zasadach sztucznej inteligencji opracowanych przez grupę ekspertów wysokiego szczebla ds. sztucznej inteligencji powołaną przez Komisję Europejską – w tym m.in. na zasadzie ochrony prywatności i zarządzania danymi, transparentności oraz rozliczalności i odpowiedzialności.

Dalsze kroki?

Polityka AI ma być realizowana z naciskiem na rozwój ekosystemu AI, mającym na względzie kierunki działań każdego z czterech wymiarów ram polskiego ekosystemu AI:

- **międzynarodowego** – w ramach którego założono m.in. współpracę europejską i pozaeuropejską, przeciwdziałanie monopolizacji dostępu do danych i zamykaniu łańcuchów wartości, wspieranie równoprawnej i zdecentralizowanej współpracy ośrodków badawczo-naukowych, eksport usług AI;
- **etycznego** – w ramach którego kierunkiem działań politycznych ma być m.in. godność ludzka i wsparcie autonomii człowieka wobec automatyki maszyn cyfrowych;
- **prawnego** – w ramach którego kierunkiem działań politycznych będą: definicja legalna AI, przeciwdziałanie nadaniu osobowości prawnej AI, własność danych osobowych i ich przenaszalności, ochrona tajemnic przedsiębiorstwa i brak własności danych przemysłowych, własność intelektualna, odpowiedzialność za szkody wytwórców AI na zasadzie staranności, a operatorów AI na zasadzie ryzyka[3], a także rozróżnienie odpowiedzialności użytkowników końcowych od odpowiedzialności operatorów AI, wsparcie specyfikacji zamówień publicznych na rozwiązania AI oraz ułatwienie procesu zamawiania;
- **standardów technicznych i organizacyjnych** – w ramach którego kierunkiem działań politycznych mają być: normy techniczne, wzajemne uznawanie certyfikatów i protokołów zgodności, reguły interoperacyjności i standardy zarządzania danymi.

Polityka AI jest jednym z kluczowych dokumentów dla losów dalszego rozwoju sztucznej inteligencji w Polsce. Trzeba mieć jednak na uwadze, że realizacja przyjętych w niej planów i zadań będzie niewątpliwie wymagała nakładów zarówno czasowych, jak i finansowych. Czas pokaże, czy uda się osiągnąć te cele, a jeśli tak, to w jakim stopniu.

[2] W rezolucji Parlamentu Europejskiego z dnia 20 października 2020 r. zawierającej zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii (2020/2012(INL)) mowa o tzw. sztucznej inteligencji ukierunkowanej na człowieka i stworzonej przez człowieka (*a human-centric and human-made AI*) oraz tzw. *human-centric approach*. Rezolucja dostępna tutaj: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_PL.html (dostęp: 1.03.2021).

[3] Zob. zagadnienie odpowiedzialności za AI przedstawione w rezolucji Parlamentu Europejskiego z dnia 20 października 2020 r. z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję (2020/2014(INL)), w której wskazano, że istotnym czynnikiem determinującym odpowiedzialność powinien być rodzaj systemu AI, nad którym sprawuje kontrolę dany operator. O rezolucjach Parlamentu Europejskiego dot. AI pisaliśmy już w numerze 1/2021 newslettera IT-Tech. Rezolucja dostępna tutaj: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_PL.html (dostęp: 1.03.2021).

Wytyczne SWIPO pomogą uniknąć chmurowego vendor lock-in

Agnieszka Wachowska, Aleksander Elmerych

Vendor lock-in jest zjawiskiem polegającym na uzależnieniu zamawiającego od produktów lub usług dostawcy w sposób, który uniemożliwia zmianę tego dostawcy bez poniesienia dodatkowych kosztów lub znacznych niedogodności po stronie zamawiającego. W przypadku usług chmurowych *vendor lock-in* wiąże się zwykle z brakiem możliwości prostej rezygnacji ze świadczenia usług przez danego dostawcę chmurowego oraz przeniesienia danych i procesów biznesowych do innego dostawcy lub na własną infrastrukturę *on-premises*. Trudności związane są najczęściej z samym procesem odzyskania danych w takiej formie, aby następnie mogły zostać bez większych problemów ponownie wykorzystane – w praktyce może się bowiem okazać, że odzyskanie danych od dostawcy nie jest możliwe lub wiąże się z koniecznością poniesienia dodatkowych kosztów albo że dane te mogą co prawda zostać odzyskane, lecz w konfiguracji lub formacie, który czyni je całkowicie bezużytecznymi poza infrastrukturą chmurową dostawcy.

Problemy związane ze zmianą dostawcy chmury

Katalog problemów, które mogą pojawić się na etapie rozwiązania umowy i zakończenia współpracy z wykonawcą, jest bardzo szeroki – dostawcy usług chmurowych mogą np. odmówić współpracy w zakresie odzyskania i migracji danych, podnosząc, że nie są do tego zobowiązani na gruncie umowy i jeżeli zamawiający chce dokonać migracji danych, to powinien to zrobić we własnym zakresie (mimo że nie jest to technicznie możliwe). Inną występującą czasem praktyką jest pobieranie dodatkowych opłat za usługi związane z odzyskaniem i migracją danych. Mogą one przy tym przybrać najróżniejszą postać – od dodatkowych usług bezpośrednio związanych ze wsparciem przy odzyskiwaniu i migracji danych, przez koszty konwersji danych do powszechnie znanych i stosowanych formatów, aż po opłaty za pobieranie danych z chmury obliczeniowej. Te ostatnie są szczególnie istotne, bo często pomijane przy analizie kosztów związanych z migracją – przy zwykłym korzystaniu z chmury obliczeniowej opłaty za pobieranie danych mogą nie być znaczące, natomiast w przypadku, gdy do odzyskania są terabajty plików umieszczanych w chmurze przez dłuższy okres (np. kilka lat), należności te mogą urosnąć do bardzo pokaźnej sumy, skutecznie zniechęcającej do zmiany dostawcy. Szczególnie skomplikowana sytuacja może mieć miejsce w przypadku usług Infrastructure as a Service (IaaS) oraz *Platform as a Service* (PaaS), czyli gdy zamawiającemu udostępniana jest infrastruktura dostawcy, na której zamawiający może rozwijać i testować tworzone przez siebie aplikacje. Interfejs programowania aplikacji (API) stosowany przez dostawcę, jak również inne elementy środowiska dostawcy, mogą się okazać na tyle specyficzne, że rozwijana aplikacja nie będzie działać lub będzie działać nieprawidłowo w innym środowisku – stworzonym przez innego dostawcę chmury obliczeniowej czy też przez zamawiającego na własnej infrastrukturze. W takim przypadku aplikacja staje się bezużyteczna, a jej dostosowanie do nowego środowiska wymaga poniesienia przez zamawiającego znacznych nakładów finansowych.

Vendor lock-in w wytycznych SWIPO

Mimo ciągle rosnącej popularności usług chmurowych obecnie brakuje powszechnie obowiązujących przepisów prawa, które regulowałyby zobowiązania dostawców, np. w zakresie sposobu świadczenia usług czy stosowania konkretnego rodzaju zabezpieczeń. Pojawiają się natomiast coraz to nowsze wytyczne i rekomendacje na poziomie krajowym i europejskim, które z reguły kierowane są do podmiotów z poszczególnych sektorów (np. z sektora finansowego czy publicznego) i uwzględniają specyfikę ich działania. Takie wytyczne mają charakter przepisów *soft law*, a więc przepisów, które nie obowiązują powszechnie, lecz do których uczestnicy rynku powinni się dostosować. Poza wytycznymi sektorowymi art. 6 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (dalej: „rozporządzenie") zakłada opracowywanie samoregulacyjnych kodeksów postępowania, m.in. w zakresie ułatwiania zmiany dostawcy usług i przenoszenia danych z wykorzystaniem ustrukturyzowanych, powszechnie używanych formatów. Kodeksy postępowania mają być tworzone z udziałem zainteresowanych stron, w tym dostawców usług w chmurze, oraz przy wsparciu Komisji Europejskiej. Dążąc do osiągnięcia celów wynikających z art. 6 rozporządzenia, w 2020 r. utworzona z inicjatywy Komisji Europejskiej grupa SWIPO (Switching Cloud Providers and Porting Data), zrzeszająca największych dostawców chmury obliczeniowej, takich jak Google, Microsoft, SAP czy OVH, opracowała zestaw dobrych praktyk w zakresie przenoszalności danych oraz zmiany dostawców chmury obliczeniowej

Dobre praktyki zostały opracowane osobno dla usług Iaas[1] oraz SaaS[2], a ich celem jest ustanowienie wytycznych, które zapewnią użytkownikom chmur obliczeniowych interoperacyjność danych i możliwość ich przenoszenia pomiędzy usługami poszczególnych dostawców oraz na infrastrukturę *on-premises* zamawiającego. Choć dobre praktyki nie mają mocy bezpośrednio wiążącej dla zamawiających i dostawców (od strony prawnej stanowią rodzaj *soft law*, którego można, ale nie trzeba przestrzegać), to zastosowanie się do nich ma zminimalizować negatywne skutki *vendor lock-in* w przypadku rozwiązania umowy z dostawcą chmury i umożliwić tanią i bezproblemową migrację danych i usług.

Co zrobić, by zminimalizować ryzyko *vendor lock-in*?

Na podstawie dobrych praktyk SWIPO w odniesieniu do usług IaaS i SaaS można wskazać na ogólny zestaw wytycznych, których stosowanie pozwoli zamawiającym zminimalizować negatywne skutki uzależnienia od dostawcy chmury obliczeniowej. Zamawiający korzystający z usług chmurowych powinni przede wszystkim:

1. Przed rozpoczęciem współpracy z dostawcą zapoznać się z:
- warunkami rozwiązania umowy;
- kosztami migracji danych.

2. Przed rozpoczęciem procesu migracji:
- opracować plan migracji danych;
- upewnić się, że obecny i docelowy dostawca chmury zapewniają możliwość przeniesienia danych w wybrany przez siebie sposób;
- zapewnić sobie współdziałanie obecnego oraz docelowego dostawcy przy przenoszeniu danych.

Wytyczne SWIPO określają również wymagania dla dostawców usług chmurowych w zakresie umożliwienia swoim użytkownikom odzyskania danych oraz przeniesienia ich do innego dostawcy. Szczególny nacisk został w tym przypadku położony na obowiązki informacyjne – dostawcy powinni informować zamawiających o:
- Warunkach migracji.
- Kosztach migracji.
- Wymaganiach, które należy spełnić przed rozpoczęciem migracji.
- Dodatkowych usługach niezbędnych do przeprowadzenia migracji danych.

nformacje te powinny zostać udostępnione przed zawarciem umowy w specjalnym dokumencie, określanym jako „transparency statement". Dodatkowo dostawcy:

- Nie powinni ograniczać możliwości eksportu danych w sposób nieuzasadniony obowiązującymi przepisami prawa.
- Powinni określać zakres danych, które mogą zostać wyeksportowane (np. czy oprócz samych danych mogą to być także grafiki lub wizualizacje).
- Powinni określać format, w jakim dane mogą zostać wyeksportowane.
- Powinni wskazywać na to, jakie zabezpieczenia stosują w trakcie eksportu danych.

Ponadto w przypadku usług PaaS dostawcy chmurowi powinni także dostarczyć użytkownikowi interfejsy programowania aplikacji (API) wraz z dokumentacją oraz zapewnić, by transfer danych odbywał się przy wykorzystaniu otwartych standardów i otwartych protokołów.

Deklaracja zgodności dostawcy z wytycznymi SWIPO

Co istotne, dostawcy chmury obliczeniowej mogą zadeklarować zgodność z wytycznymi SWIPO, co oznacza, że zapewniają możliwość migracji danych zgodnie z określonymi w tych wytycznych zasadami. Przed zawarciem umowy o świadczenie usług zamawiający mogą zatem zweryfikować, czy dany dostawca zadeklarował zgodność z wytycznymi SWIPO, a tym samym – czy możliwe będzie ewentualne przeniesienie danych w przyszłości. Część dostawców już teraz deklaruje zgodność z wytycznymi SWIPO, choć nie jest to obecnie żaden formalny wymóg świadczenia usług chmurowych. Niewykluczone natomiast, że kwestia stosowania praktyki uzależniania klientów od usług świadczonych przez dostawców chmury stanie się w najbliższym czasie obiektem zainteresowania polskiego ustawodawcy lub organów unijnych – często bowiem ma miejsce sytuacja, w której niewiążące wytyczne w miarę upływu czasu przekształcają się w obowiązujące przepisy prawa.

Podsumowanie

Należy mieć na uwadze, że wytyczne SWIPO z pewnością nie wyeliminują całkowicie uzależnienia zamawiających od dostawcy chmury w sytuacji zaprzestania świadczenia usług i konieczności migracji danych. Zmiana podmiotu przetwarzającego dane zawsze będzie wiązała się z pewnym poziomem ryzyka i niedogodności, a także z koniecznością poniesienia dodatkowych kosztów, niekoniecznie związanych z samym procesem przenoszenia danych. Warto jednak dążyć do zminimalizowania tego ryzyka oraz być świadomym konsekwencji podjęcia decyzji o zmianie dostawcy chmury, co pozwoli przygotować się na ten niełatwy proces biznesowy – zarówno pod względem finansowym, jak i organizacyjnym.

[1] Zob. SWIPO Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services z dnia 27 maja 2020 r.
[2] Zob. SWIPO Code of Conduct for Data Portability and Cloud Service Switching for Software as a Service (SaaS) z dnia 8 lipca 2020 r.

Dekompilacja na potrzeby naprawy błędów możliwa, jeśli nie zabrania tego umowa – wnioski z opinii Rzecznika Generalnego w sprawie C 13/20 Top System S.A. z dnia 10 marca 2021 r.

Agnieszka Wachowska

Treść opinii Rzecznika Generalnego

10 marca 2021 r. Rzecznik Generalny Maciej Szpunar wydał opinię w ciekawej i ważnej dla świata IT sprawie Top System SA. przeciwko État belge toczącej się pod sygnaturą C 13/20 na skutek pytania prejudycjalnego złożonego przez cour d'appel de Bruxelles (sąd apelacyjny w Brukseli, Belgia) dotyczącej zakresu dozwolonej dekompilacji oprogramowania.

O sprawie tej pisaliśmy już wcześniej, m.in. na blogu kancelarii (https://www.traple.pl/2020/10/14/dekompilacja-programu-komputerowego-przed-tsue-sprawa-c-13-20/).

Odpowiadając za zadane przez belgijski sąd pytania prejudycjalne Rzecznik Generalny stwierdził, że:

1. Artykuł 5 ust. 1 dyrektywy Rady 91/250/EWG z dnia 14 maja 1991 r. w sprawie ochrony prawnej programów komputerowych należy interpretować w ten sposób, że **zezwala on uprawnionemu nabywcy programu komputerowego na przeprowadzenie dekompilacji tego programu, jeżeli jest ona konieczna do poprawienia błędów mających wpływ na funkcjonowanie owego programu**;
2. Artykuł 5 ust. 1 dyrektywy 91/250 należy interpretować w ten sposób, że dekompilacja programu komputerowego dokonana na podstawie tego przepisu przez uprawnionego nabywcę do celów poprawienia w nim błędów **nie podlega wymogom przewidzianym w art. 6 owej dyrektywy**. Dekompilacja taka może jednakże **zostać przeprowadzona jedynie w zakresie koniecznym do poprawienia tych błędów i w granicach zobowiązań umownych nabywcy**.

Główne problemy prawne

Główny spór prawny, jaki rzecznik musiał rozstrzygnąć dotyczył tego, czy art. 5 ust. 1 dyrektywy Rady 91/250/EWG zezwalając na dokonywanie czynności, o których mowa w art. 4 lit. a) i b) tej dyrektywy, czyli następujących czynność:

„a) *trwałe lub czasowe powielanie programu komputerowego jakimikolwiek środkami i w jakiejkolwiek formie, częściowo lub w całości. W zakresie, w jakim ładowanie, wyświetlanie, uruchamianie, transmitowanie lub przechowywanie programu komputerowego wymaga takiego powielenia, takie czynności wymagają uzyskania zezwolenia uprawnionego;*

b) *translację, adaptację, porządkowanie i jakiekolwiek inne modyfikacje programu komputerowego i powielenie wyników tych działań bez uszczerbku dla praw osoby, która modyfikuje program*",

pozwala również na zdekompilowanie oprogramowania, czyli jego przekształcenie z formy kodu wynikowego na kod źródłowy, skoro dekompilacji poświęcony jest odrębny art. 6 dyrektywy Rady 91/250/EWG. Wskazany problem prawny przekłada się na praktyczne zagadnienie – czy na potrzeby używania programu przez uprawnionego nabywcę zgodnie z zamierzonym celem (jego przeznaczeniem), włącznie z poprawianiem błędów dozwolone jest zdekompilowanie oprogramowania.

A w razie przesądzenia, że na potrzeby naprawy błędów taka dekompilacja jest dozwolona – ustalenie czy mają do niej zastosowanie ograniczenia wynikające z art. 6 dyrektywy Rady 91/250/EWG i przesądzenie wymogów, jakim taka dekompilacja powinna podlegać.

Z racji tego, że w stanie faktycznym, w którym zadane zostały pytania prejudycjalne umowa zawarta między dostawcą oprogramowania, które zostało zdekompilowane nie regulowała kwestii możliwości dokonywania dekompilacji – w przedmiotowej sprawie TSUE nie zostało zadane pytanie, czy ewentualne uprawnienie do dokonywania dekompilacji

oprogramowania na potrzeby naprawy błędów w oprogramowaniu może być skutecznie wyłączone w postanowieniach umowy.

Tezy i wnioski z Opinii Rzecznika Generalnego

Przedstawiona opinia Rzecznika Generalnego, jest niezwykle ciekawa, gdyż dotyka wielu praktycznych zagadnień związanych z korzystaniem z programów komputerowych oraz analizuje specyfikę programów komputerowych oraz ich ochronę prawnoautorską na tle innych utworów.

Kluczowe wnioski jakie wynikają z opinii Rzecznika Generalnego są następujące:
W umowie licencyjnej można skutecznie zakazać dokonywania dekompilacji oprogramowania na potrzeby naprawy błędów oprogramowania;
2. O ile umowa tego nie zakazuje, na podstawie art. 5 ust. 1 dyrektywy 91/250 (w polskiej implementacji art. 75 ust. 1 pr. aut.) dekompilacja oprogramowania jest możliwa na potrzeby naprawy błędów oprogramowania, jeśli jej wykonanie jest konieczne dla normalnego korzystania z oprogramowania;
3. Dozwolona na potrzeby naprawy błędów dekompilacja może być dokonana zgodnie z następującymi założeniami:

- jeśli jest ona dokonywana przez uprawnionego nabywcę programu komputerowego;
- jedynie na potrzeby naprawy błędów, które powodują wadliwe działanie uniemożliwiające używanie programu zgodnie z jego przeznaczeniem, przy czym błąd powinien być rozumiany w sposób wąski;
- żadna zmiana, ani ulepszenie programu nie stanowi poprawiania błędów i nie może być dokonana na podstawie art. 5 ust. 1 dyrektywy 91/250 (art. 75 ust. 1 pr. aut), co oznacza, że naprawa błędów rozumiana jest w sposób wąski;
- w zakresie koniecznym do poprawienia błędu *sensu stricto*, ale także do poszukiwania tego błędu i może również obejmować części programu, w których nie ma co prawda błędu, ale które powinny być zmienione na potrzeby błędu;
- nabywca programu dokonujący legalnej dekompilacji nie jest zobowiązany do zwracania się do uprawnionego o poprawienie błędów ani do wnoszenia o dostęp do kodu źródłowego programu, ani do wytaczania powództwa zmierzającego do nakazania uprawnionemu wykonania takiej czy innej czynności.

Warto w tym miejscu podkreślić, że choć w pytaniach prejudycjalnych nie zadano wprost tego pytania Rzecznik Generalny wyraził jednoznaczny pogląd, że umowa sprzedaży programu może regulować używanie programu, w tym poprawianie błędów, ograniczając możliwość nabywcy do dokonania, do celów poprawienia tych błędów, czynności należących do monopolu uprawnionego. Rzecznik podkreślił jednocześnie, że jego zdaniem, ograniczenie to może osiągnąć rozmiary całkowitego zakazu poprawiania błędów przez nabywcę. Oznacza to, że jeśli umowa na korzystanie z oprogramowania wyraźnie zakazuje dekompilacji tego oprogramowania na potrzeby naprawy błędów wyjątek przewidziany w art. 5 ust. 1 dyrektywy 91/250 nie znajduje zastosowania, a czynności nabywcy ograniczają się do tych zezwolonych na podstawie umowy.

Wnioski

Należy pamiętać o tym, że Opinia Rzecznika Generalnego nie stanowi finalnego rozstrzygnięcia, które zostanie wydane dopiero przez Trybunału Sprawiedliwości Unii Europejskiej i nie wiąże ona Trybunału.

Niemniej jednak z uwagi na autorytet Rzecznika Generalnego, jego opinia ma bardzo duże znaczenie i może mieć istotny wpływ na treść finalnego wyroku.

Zgadzając się z głównymi tezami opinii Rzecznika, w mojej opinii należy spodziewać się, że Trybunał dopuści na podstawie art. 5 ust. 1 dyrektywy 91/250 (w polskiej implementacji art. 75 ust. 1 pr. aut.) dekompilację oprogramowania na potrzeby naprawy błędów oprogramowania.

Najciekawsze jednocześnie i mające największy wpływ na praktykę obrotu IT będzie miało natomiast to, czy Trybunał Sprawiedliwości odniesie się w swoim wyroku do możliwości pełnego wyłączenia tego uprawniania w drodze postanowień umownych i podzieli kategoryczne i nieco bardziej kontrowersyjne stanowisko Rzecznika dopuszczające możliwość skutecznego zakazania w umowie dekompilacji oprogramowania na potrzeby naprawy błędów oprogramowania.

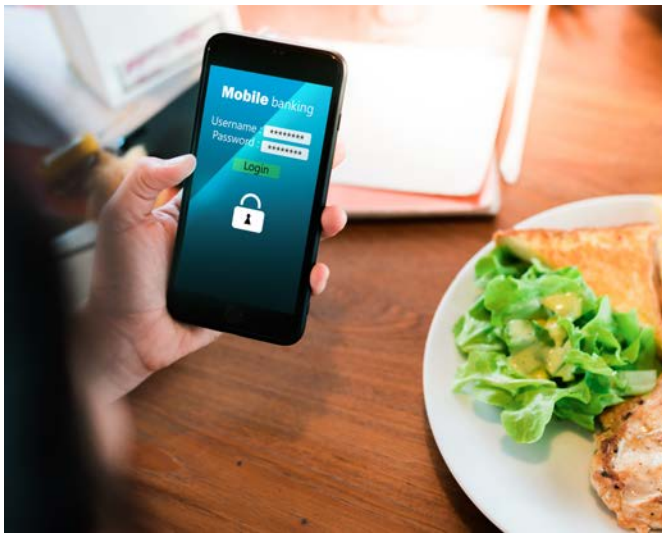
Wstrzymanie świadczenia serwisu oprogramowania a obowiązek zapłaty wynagrodzenia

Karolina Grochecka-Goljan, Aleksander Elmerych

Na podstawie umowy serwisowej oprogramowania (umowy wsparcia korzystania z oprogramowania) w zamian za opłatę serwisową wykonawca zobowiązuje się do świadczenia na rzecz zamawiającego szeregu różnych usług, które mają na celu zapewnienie zamawiającemu możliwości niezakłóconego korzystania z oprogramowania. Katalog tych usług uzależniony jest od zakresu wsparcia wykonawcy oraz od rodzaju oprogramowania. Zazwyczaj umowy serwisowe obejmują zobowiązanie wykonawcy do usuwania błędów i wad oprogramowania, dokonywania jego aktualizacji oraz dostosowania do zmieniających się przepisów prawa, a także do zapewnienia bazy wiedzy czy wdrażania modyfikacji odpowiadających potrzebom zamawiającego. Do świadczenia usług serwisowych wykonawca powinien mieć odpowiednie licencje, pozwalające na dostarczenie i zapewnienie zamawiającemu możliwości korzystania z patchy serwisowych oraz aktualizacji, a także powinien dysponować specjalistyczną wiedzą dotyczącą budowy i sposobu działania oprogramowania. Z tego powodu w praktyce usługi serwisowe najczęściej świadczone są przez podmioty związane z producentem oprogramowania (partnerów), przez co możliwość wyboru wykonawcy jest znacznie ograniczona. Wpływa to również na możliwość negocjowania umownych warunków świadczenia usług serwisowych. Zazwyczaj warunki te nie podlegają negocjacjom, a zamawiający może jedynie wybrać odpowiedni dla siebie zakres wsparcia. Tym samym zamawiający może albo zaakceptować warunki zaproponowane przez wykonawcę, albo zrezygnować z korzystania z usług serwisowych, co w dłuższej perspektywie może doprowadzić do dezaktualizacji oprogramowania i utraty możliwości zmiany czy dostosowania jego funkcjonalności do potrzeb zamawiającego.

Dopuszczalność wstrzymania świadczenia usług przez wykonawcę, a prawo wykonawcy do wynagrodzenia

Dążąc do zapewnienia sobie płynności finansowej, partnerzy świadczący usługi wsparcia korzystania z oprogramowania często wprowadzają do umów postanowienie, zgodnie z którym w razie opóźnienia z zapłatą opłaty serwisowej przez zamawiającego wykonawcy (partnerowi) przysługuje prawo do wstrzymania świadczenia usług z zachowaniem prawa do wynagrodzenia. Mamy zatem w takim przypadku do czynienia z sytuacją, w której wykonawca z jednej strony zwolniony jest z obowiązku świadczenia usług, a z drugiej strony – pozostaje uprawniony do pobierania opłaty serwisowej. Postanowienie takie jest z pewnością korzystne dla wykonawcy – pojawia się jednak pytanie czy może być ono zakwestionowane przez zamawiającego, a w konsekwencji czy jest ono dopuszczalne w świetle obowiązujących przepisów prawa i zasad współżycia społecznego.



Kwestię dopuszczalności wprowadzania do umów postanowień umożliwiających wstrzymanie przez wykonawcę świadczenia usług z zachowaniem prawa do wynagrodzenia w przypadku braku płatności ze strony zamawiającego badał Sąd Okręgowy w Łodzi w wyroku z dnia 29 kwietnia 2016 r., sygn. XIII Ga 289/16. Sprawa dotyczyła sporu powstałego na gruncie umowy serwisowej sprzętu komputerowego i oprogramowania, która przewidywała uprawnienie wykonawcy do wstrzymania świadczenia usług w przypadku przekroczenia przez zamawiającego terminu płatności wynagrodzenia powyżej 7 dni, z jednoczesnym zachowaniem prawa wykonawcy do wynagrodzenia za ten okres. W związku z opóźnieniem zapłaty wynagrodzenia przez zamawiającego pomiędzy stronami powstał spór dotyczący tego, czy zasadne jest domaganie się przez wykonawcę zapłaty wynagrodzenia za okres, w którym świadczenie usług było wstrzymane.

W swoim wyroku Sąd Okręgowy w Łodzi podzielił stanowisko sądu pierwszej instancji, który uznał, że zastrzeżenie umowne, zgodnie z którym wykonawcy przysługuje wynagrodzenie za okres wstrzymania świadczenia usług serwisowych, stanowi w istocie karę umowną zastrzeżoną na wypadek niespełnienia świadczenia pieniężnego, niedopuszczalną na gruncie art. 483 § 1 k.c. Szersze uzasadnienie tego rozstrzygnięcia można znaleźć w wydanym w tej sprawie w pierwszej instancji wyroku Sądu Rejonowego dla Łodzi-Śródmieścia w Łodzi z dnia 1 lutego 2016 r., sygn. XIII GC 1553/15 (Sąd Okręgowy przyjął ustalenia, ocenę dowodów i rozważania prawne Sądu Rejonowego za własne):

„W ocenie Sądu umowne prawo powodów do wynagrodzenia za okres, w którym nastąpiło »zawieszenie« ich obowiązku spełniania wzajemnych świadczeń niepieniężnych, jako skutek ponad siedmiodniowego opóźnienia pozwanej w zapłacie należności, ***przyjmuje postać kary umownej za niewykonanie lub nienależyte wykonanie zobowiązania pieniężnego, co jest niedopuszczalne na gruncie art. 483 § 1 k.c.*** *Zważyć bowiem należy, że mimo, że* ***strony nie nazwały przysługującego powodom świadczenia pieniężnego karą umowną lecz prawem do wynagrodzenia, to świadczenie to posiada konstytutywne cechy kary umownej wymienione w dyspozycji przywołanego przepisu*** *– obejmuje zapłatę określonej sumy w związku z niewykonaniem lub nienależytym wykonaniem zobowiązania. Ponieważ jednocześnie nie stanowi ono ekwiwalentu świadczenia wzajemnego powodów, należy przyjąć, że* ***ma na celu jedynie naprawienie szkody powodów wynikłej z niewykonania lub nienależytego wykonania zobowiązania przez pozwaną***”.

Konsekwencją przyjęcia przez Sąd takiego rozstrzygnięcia było uznanie postanowienia przewidującego obowiązek zapłaty wynagrodzenia wykonawcy mimo wstrzymania przez niego świadczenia usług za nieważne na podstawie art. 58 § 1 k.c. Wyrażone stanowisko sądu pozbawia wykonawcę możliwości skutecznego dochodzenia zapłaty przez zamawiającego opłaty serwisowej za okres wstrzymania świadczenia usług – wykonawca może bowiem domagać się zapłaty wynagrodzenia wyłącznie za okres, w którym faktycznie świadczył usługi, nawet jeżeli zgodnie z umową miałoby to polegać jedynie na pozostawaniu w gotowości do świadczenia usług.

Brak ekwiwalentności świadczeń

Dodatkowo Sądy obu instancji zwróciły w tej sprawie uwagę na fakt, że w sytuacji, w której jedna ze stron zwolniona jest ze świadczenia usług, a druga mimo to zobowiązana jest do zapłaty wynagrodzenia, zachodzi brak ekwiwalentności wzajemnych świadczeń stron. To z kolei może dawać podstawy do twierdzeń, że poza naruszeniem art. 483 § 1 k.c. umowy serwisowe w zakresie, w jakim dają wykonawcy możliwość dochodzenia wynagrodzenia za okres wstrzymania usług, są sprzeczne z zasadami współżycia społecznego, a tym samym również nieważne w związku z naruszeniem art. 5 k.c. W orzecznictwie przyjmuje się bowiem, że rażące zachwianie ekwiwalentności świadczeń stron może świadczyć o sprzeczności umowy z zasadami współżycia społecznego (zob. wyrok Sądu Apelacyjnego w Warszawie z dnia 16 maja 2014 r., sygn. I ACa 1254/12).

Podsumowanie

Podsumowując powyższe, w świetle orzeczenia Sądu Okręgowego w Łodzi z dnia 29 kwietnia 2016 r., sygn. XIII Ga 289/16, zastrzeżenie umowne, zgodnie z którym wykonawcy przysługuje uprawnienie do wstrzymania świadczenia usług serwisowych z jednoczesnym zachowaniem prawa do wynagrodzenia, stanowi karę umowną zastrzeżoną na wypadek niewykonania lub nienależytego wykonania zobowiązania pieniężnego, co jest niedopuszczalne na gruncie art. 483 § 1 k.c. Tym samym wykonawca nie ma możliwości domagania się od zamawiającego zapłaty wynagrodzenia za okres, w którym nie świadczył usług, niezależnie od tego, czy umowa taką możliwość przewiduje, czy też nie.

Skuteczność depozytu kodów źródłowych w przypadku upadłości wykonawcy

Joanna Dworak

Serce każdego oprogramowania stanowi kod źródłowy. Jest on też ściśle chronioną przez każdego producenta tajemnicą przedsiębiorstwa. Nawet złożony jako zabezpieczenie zamawiających z umowy na dostawę lub wdrożenie oprogramowania podlega podjęciu przez uprawnionych w ściśle określonych sytuacjach. Czy również w przypadku upadłości wykonawcy?

Często stosowanym zabiegiem w umowach na dostawy systemów IT jest wymaganie przez zamawiających złożenia przez wykonawców kodu źródłowego oprogramowania do depozytu. Ma to na celu zabezpieczenie dostępu zamawiającego do kodu źródłowego oprogramowania w razie wystąpienia trudności po stronie wykonawcy – czy to w dalszym utrzymywaniu lub rozwoju oprogramowania przez wykonawcę, czy też w przypadku jego upadłości lub restrukturyzacji. Strony określają w umowie obowiązek złożenia kodu do depozytu, osobę depozytariusza, określoną postać składanego kodu i jego zabezpieczenie, często obowiązek aktualizacji kodu i warunki podjęcia takiego kodu z depozytu przez każdą ze stron.

Czy jednak możliwość podjęcia kodu źródłowego w przypadku upadłości wykonawcy będzie w praktyce możliwa, czy taka czynność byłaby sprzeczna z prawem? Jak wynika z art. 83 Ustawy z dnia 28 lutego 2003 r. Prawo upadłościowe (t.j. Dz. U. z 2020 r., poz. 1228; dalej: „Prawo upadłościowe"), postanowienia umowy zastrzegające na wypadek złożenia wniosku o ogłoszenie upadłości lub ogłoszenia upadłości zmianę lub rozwiązanie stosunku prawnego, którego stroną jest upadły, są nieważne. Reguła ustanowiona w tym przepisie ma na celu przede wszystkim pozbawienie mocy prawnej tych postanowień umów zawartych przez dłużnika przed ogłoszeniem jego upadłości, które wiążą zmianę lub rozwiązanie danego stosunku prawnego z samym ogłoszeniem upadłości, bez potrzeby zajścia jakichkolwiek dodatkowych okoliczności. Nieważność, o której mowa w art. 83 Prawa upadłościowego, ma charakter nieważności bezwzględnej, uwzględnianej – jak wiadomo – z urzędu, bez potrzeby powoływania się na nią przez któregokolwiek z uczestników obrotu prawnego; nie wchodzi tu też w grę konwalidacja przedmiotowego postanowienia[1]. W świetle tego przepisu możliwość podjęcia kodów źródłowych na wypadek ogłoszenia upadłości przez wykonawcę lub już samego złożenia wniosku o ogłoszenie upadłości będzie miała na celu właśnie zmianę stosunku prawnego (w rozumieniu art. 83 Prawa upadłościowego), w którym zamawiający nie mógł podjąć kodów źródłowych przed nadejściem takich zdarzeń – po ich nadejściu taka możliwość już istnieje. Tym samym postanowienia uprawniające stronę do podjęcia kodu źródłowego z depozytu będą objęte nieważnością bezwzględną.

[1] Por. S. Gurgul, Prawo upadłościowe, [w:] S. Gurgul, Prawo upadłościowe. Prawo restrukturyzacyjne. Komentarz, wyd. 12, Warszawa 2020.

Powyższy skutek jest logiczną konsekwencją celu postępowania upadłościowego – maksymalnej ochrony wierzycieli niewypłacalnego dłużnika. Z dniem ogłoszenia upadłości dłużnika majątek upadłego staje się masą upadłości, która służy zaspokojeniu jego wierzycieli (por. art. 61 Prawa upadłościowego). Jeśli zatem prawa do kodu źródłowego znajdowały się w majątku wykonawcy, który upadł, prawa te z dniem ogłoszenia upadłości nie będą mu już przysługiwały. Gdyby natomiast już wskutek złożenia wniosku o ogłoszenie upadłości kod źródłowy przysługujący danemu podmiotowi, dotychczas pilnie strzeżony, został podjęty, jego wartość majątkowa zmalałaby znacznie. To z kolei mogłoby uniemożliwić ochronę wierzycieli upadłego wykonawcy.

Mimo że strony są niekiedy świadome konsekwencji wynikających z prawa upadłościowego, zastrzegają w umowach „dla bezpieczeństwa" możliwość podjęcia kodów źródłowych z depozytu na wypadek ogłoszenia upadłości wykonawcy. Pomimo iż postanowienia te będą nieważne, w praktyce mogą doprowadzić do problemów dla osoby depozytariusza. Z jednej strony depozytariusz będzie związany postanowieniami umowy obligującymi go do wydania kodów i zapewne będzie ponaglany przez uprawnionego z umowy depozytu, z drugiej zaś nie można pomijać obowiązujących przepisów prawa. W obu przypadkach depozytariuszowi może grozić odpowiedzialność odszkodowawcza, niemniej nie sposób nie przyznać prymatu ustawie. W takiej sytuacji, tj. w razie wskazania złożenia wniosku o ogłoszenie upadłości lub ogłoszenia upadłości jako przypadku umożliwiającego podjęcie kodów przez drugą stronę, najprostszym rozwiązaniem byłaby odmowa przyjęcia kodu źródłowego do depozytu.

Na marginesie warto wspomnieć, że analogiczne postanowienie do art. 83 Prawa upadłościowego znajduje się w art. 247 Ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2020 r., poz. 814), który stanowi, że postanowienia umowy zastrzegające na wypadek złożenia wniosku o otwarcie przyspieszonego postępowania układowego lub jego otwarcia zmianę lub rozwiązanie stosunku prawnego, którego stroną jest dłużnik, są nieważne.

Dokumentacja dotycząca rozliczeń 50% kosztów uzyskania przychodów

Joanna Jastrząb

Nowy rok podatkowy stał się dla wielu pracodawców branży IT momentem wprowadzenia rozliczeń 50% kosztów uzyskania przychodów dla pracowników. O tej podatkowej preferencji wielokrotnie pisaliśmy wcześniej, m.in. na naszym blogu: klik. W tym miejscu warto jednak przypomnieć, że podstawowe warunki zastosowania 50% kosztów obejmują:

- tworzenie przez pracowników utworów w ramach jednego z rodzajów działalności wymienionych w art. 22 ust. 9b ustawy o podatku dochodowym od osób fizycznych[1], np. działalności w zakresie programów komputerowych;
- rozporządzanie przez pracownika prawami autorskimi do tych utworów lub korzystanie z tych praw – co w praktyce najczęściej oznacza przeniesienie praw autorskich na pracodawcę;
- osiągnięcie przez pracownika konkretnego przychodu z tytułu przeniesienia praw autorskich.

Spełnienie tych warunków pozwala na zastosowanie podwyższonych kosztów uzyskania przychodów, które powodują, że pensja netto pracownika wzrasta – obniżona zostaje bowiem wysokość podatku dochodowego.

Kluczowe dla zagwarantowania prawidłowości rozliczeń będzie prowadzenie odpowiedniej dokumentacji, tak aby w razie kontroli podatkowej móc wykazać, że powyższe warunki zostały spełnione. Warto przy tym na marginesie zaznaczyć, że przepisy prawa nie stawiają konkretnych wymogów wobec takiej dokumentacji, a ponadto umożliwiają podatnikom i płatnikom w ramach postępowań prowadzonych przez organy podatkowe i skarbowe wykazanie spełnienia ww. przesłanek dowolnymi środkami dowodowymi. Niemniej praktyka pokazuje, że brak prowadzenia dokumentacji na bieżąco, zwłaszcza w przypadku większych organizacji, może utrudnić potwierdzenie prawidłowości rozliczeń po upływie kilku lat.

Z tych powodów warto uporządkować wewnętrzne regulacje, tak aby obowiązywały one pracowników i pracodawcę od początku rozliczeń 50% kosztów. Można przy tym wyróżnić dwa rodzaje dokumentacji:

- dokumenty tworzące ramy dla zastosowania 50% kosztów – potwierdzające przenoszenie praw autorskich na pracodawcę i dotyczące obowiązków stron stosunku pracy związanych z rozliczaniem 50% kosztów;
- dokumenty potwierdzające stworzenie utworów przez pracownika, przygotowywane na bieżąco w toku rozliczeń oraz dokumenty okresowe potwierdzające zastosowanie 50% kosztów.

Powyższe rozróżnienie jest o tyle istotne, że pierwszy rodzaj dokumentacji wdrażany jest co do zasady jednorazowo, a drugi rodzaj wymaga bieżącego prowadzenia. Warto o tym pamiętać, gdyż jest to ważne dla okresowej aktualizacji i weryfikacji dokumentów:

- ramy zastosowania 50% kosztów należy weryfikować zwłaszcza wtedy, gdy zmienią się założenia organizacyjne (np. siatka stanowisk, proces raportowania) lub przepisy prawa w zakresie 50% kosztów;
- dokumenty potwierdzające stworzenie utworów powinny być weryfikowane częściej, tak aby wychwycić ewentualne błędy w rozliczeniach (np. zastosowanie 50% kosztów w sytuacji, gdy utwór nie powstał).

[1] Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (Dz. U. z 2020 r., poz. 1426, z późn. zm.).

Rozwijając powyższe, dokumentacja tworząca ramy dla zastosowania 50% kosztów to przede wszystkim odpowiednie postanowienia umowy o pracę, które potwierdzą, że dochodzi do przeniesienia praw autorskich na pracodawcę w zamian za wyodrębnioną część wynagrodzenia (zwykle za konkretnie określone – kwotowo lub procentowo – honorarium autorskie). Najważniejsze jest odpowiednie sformułowanie postanowień umowy, aby było jasne, jakie są ramy przeniesienia tych praw, a tym samym – aby nie powstały wątpliwości, w jakim zakresie pracodawca może korzystać z wytworzonych utworów. Oprócz umów o pracę warto zadbać o wewnętrzne regulacje jednolite dla wszystkich pracowników, dla których stosuje się 50% kosztów, takie jak regulamin prac autorskich.

Dokumenty stanowiące ramy rozliczania 50% kosztów powinny również wyznaczać konkretne obowiązki pracowników i ewentualnie pracodawcy, jeśli chodzi o potwierdzenie stworzenia utworów. Najpopularniejsze w tym zakresie pozostaje okresowe, regularne składanie przez pracowników oświadczeń lub raportów dotyczących stworzonych utworów. Zgodnie ze stanowiskiem Ministra Finansów przedstawionym w interpretacji ogólnej w sprawie 50% kosztów uzyskania przychodów (sygn. DD3.8201.1.2018) takie oświadczenia lub raporty powinny być na tyle konkretne, aby jednoznacznie określały, jaki utwór powstał. W interesie pracodawcy pozostawać więc będzie określenie wzoru takich oświadczeń lub raportów (aby pracownikowi przy ich wypełnianiu nie umknęły żadne kwestie).

Dobrym rozwiązaniem mogą okazać się także okresowe informacje na temat zastosowanych 50% kosztów, np. roczne lub kwartalne informacje o wypłaconym honorarium i powstałych utworach, przygotowane przez pracodawcę na bazie dokonanych rozliczeń oraz raportów/oświadczeń złożonych przez pracowników. Takie informacje roczne/kwartalne pełnią również funkcję porządkującą – mobilizują pracodawcę do weryfikacji raportów/oświadczeń złożonych przez pracownika w ciągu roku lub kwartału pod kątem kompletności (czy rzeczywiście zostały wskazane utwory wytworzone przez pracownika).

Opisane powyżej w zarysie rodzaje rekomendowanych dokumentów dla rozliczania 50% kosztów pozwolą uporządkować wewnętrzne procesy, określić obowiązki każdej ze stron stosunku pracy przy rozliczaniu 50% kosztów, a w efekcie – pozwolą w prosty sposób potwierdzić prawidłowość dokonanych rozliczeń. Mając to na uwadze, dokumenty te nie powinny być bagatelizowane, gdyż mogą znacząco ułatwić wykazanie w ramach kontroli spełnienia wymogów wskazanych w ustawie o podatku dochodowym od osób fizycznych.

NADCHODZĄCE WYDARZENIA

27.04.2021
SZKOLENIE

UMOWY NA KORZYSTANIE Z OPROGRAMOWANIA W CHMURZE OBLICZENIOWEJ – WYZWANIA, RYZYKA I PRAKTYCZNE ASPEKTY ZAWIERANIA I NEGOCJOWANIA UMÓW NA CLOUD COMPUTING

adw. Xawery Konarski, r. pr. Agnieszka Wachowska

Więcej informacji >>

13.05.2021
SZKOLENIE

WDROŻENIE IT – JAK PRZYGOTOWAĆ DOBRĄ UMOWĘ ORAZ DOBRZE PRZYGOTOWAĆ SIĘ DO WDROŻENIA?

r. pr. Agnieszka Wachowska

Więcej informacji >>

NR 2 - MARZEC 2021

PUBLIKACJE

Nr 2/2021 IT Professional:

- **r.pr. Joanna Jastrząb** – Wymiana informacji w zakresie cyberbezpieczeństwa

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

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, Senior Associate
karolina.grochecka@traple.pl

Małgorzata Kotwica
Associate
malgorzata.kotwica@traple.pl

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

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

Redaktorki newslettera:
r.pr. Joanna Jastrząb
adw. Karolina Grochecka-Goljan