02/2020 MAJ

NEWSLETTER

IT-TECH/PZP LAW

W NUMERZE:

Traple
Konarski
Podrecki
& Wspólnicy

TKP

Chmura obliczeniowa i COVID-19 – przepisy i wytyczne

Chmura obliczeniowa określana jest nieraz jako „superbohater" pandemii COVID-19. Bez tych usług nie byłoby możliwe kontynuowanie działalności gospodarczej, załatwianie spraw administracyjnych, czy korzystanie z cyfrowej rozrywki przez konsumentów.

Znaczenie dostępu do rozwiązań chmurowych zostało dostrzeżone przez polskiego ustawodawcę i regulatorów, którzy na czas pandemii COVID-19 wprowadzili szereg szczególnych rozwiązań prawnych. Zawarte są one w tzw. specustawie o COVID-19 z dnia 2 marca 2020 r. (Dz.U. z 2020 r. poz. 374), znowelizowanej następnie w dniu 31 marca 2020 r. (Dz.U. z 2020 r. poz. 568), a także rekomendacjach organów regulacyjnych. Podstawowym celem przyjęcia tych aktów prawnych było ułatwienie dostępu do usług chmury obliczeniowej, odnoszą się one również do szczególnych ryzyk związanych ze zdalnym korzystaniem z danych i aplikacji IT.

Praca zdalna w chmurze obliczeniowej

Zgodnie z art. 3 specustawy o COVID - „W celu przeciwdziałania COVID-19 pracodawca może polecić pracownikowi wykonywanie, przez czas oznaczony, pracy określonej w umowie o pracę, poza miejscem jej stałego wykonywania (praca zdalna)". O takiej organizacji pracy decyduje pracodawca, bez konieczności uzgadniania tego z pracownikami ani zbiorowo (porozumienie z przedstawicielami pracowników), ani indywidualnie (porozumienie z każdym pracownikiem). Mimo, że z formalnego punktu widzenia praca zdalna, inaczej niż telepraca w rozumieniu art. 675 kodeksu pracy, nie wymaga przekazywania jej wyników za pomocą środków komunikacji elektronicznej, to jednak powszechnie wykonywana jest ona w środowisku chmury obliczeniowej (np. aplikacje do przetwarzania w chmurze dokumentów, czy komunikacji bezpośredniej).

Z pracą zdalną związane są dla pracodawcy dodatkowe ryzyka. Przykładowo, pracownicy dysponujący zdalnym dostępem do infrastruktury pracodawcy nie podlegają środkom bezpieczeństwa fizycznego, które mogą obowiązywać w lokalu pracodawcy. Zagrożenia te dostrzegł Minister Cyfryzacji, który w komunikacie z dnia 13 marca 2020 r. zawarł szereg rekomendacji dotyczących zasad wykonywania zdalnej pracy (link). Zalecane jest między innymi podjęcie tak działań jak nieużywanie prywatnych skrzynek pocztowych czy grup na portalach społecznościowych do komunikacji firmowej oraz zadbanie o bezpieczeństwo urządzeń w sieci domowej poprzez używanie „silnego" hasła do sieci WiFi oraz aktualizacji oprogramowania.

Z kolei, w komunikacie z dnia 17 marca 2020 r. Urząd Ochrony Danych Osobowych (UODO) wskazał na kilka zasad ochrony danych osobowych poza miejscem pracy (https://uodo.gov.pl/pl/138/1459). W kontekście korzystania z chmury obliczeniowej podkreślono między innymi potrzebę korzystania z zaufanych dostawców oraz przestrzegania wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych. W kontekście bezpieczeństwa danych osobowych warto również zapoznać się z poradnikiem Urzędu Ochrony Danych Osobowych, opracowanym przy współpracy z MEN, („Dane osobowe bezpieczne podczas zdalnego nauczania"),

Z pracą zdalną związane są szczególne problemy prawne przetwarzania danych osobowych, dotyczące takich sytuacji jak: praca na własnym sprzęcie (Bring Your Own Device, BYOD), zarządzanie urządzeniami mobilnymi (np. konfigurowanie aplikacji, usuwanie danych na żądanie), czy monitorowanie wykonywania obowiązków pracowniczych w trakcie pracy zdalnej. W tym ostatnim przypadku trzeba między innymi pamiętać o obowiązku informowania pracownika o wykorzystaniu i celach technologii monitorowania, a także zadbaniu aby odbywało się ono zgodnie z zasadą proporcjonalności i minimalizacji danych. Oznacza to, że przetwarzanie danych w tym kontekście musi być proporcjonalne do ryzyka, jakie ponosi pracodawca, a także, że należy w miarę możliwości ograniczać do minimum informacje rejestrowane w ramach ciągłego monitorowania. Wytyczne w tym zakresie określono w Opinii nr 2/2017 Grupy Roboczej art.29 na temat przetwarzania danych osobowych w miejscu pracy.

Wyłączenia z prawa zamówień publicznych

Istotne wyłączenie stosowania prawa zamówień publicznych zawarte zostało w art. 6.1 specustawy o COVID. Zgodnie z nim, „do zamówień na usługi lub dostawy nie-

zbędne do przeciwdziałania COVID-19 nie stosuje się przepisów ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843), jeżeli zachodzi wysokie prawdopodobieństwo szybkiego i niekontrolowanego rozprzestrzeniania się choroby lub jeżeli wymaga tego ochrona zdrowia publicznego." W Komunikacie Prezesa UZP z dnia 24 marca 2020 r., wyjaśniono, że wyłączenie to może znaleźć zastosowanie również do zamówień publicznych, których przedmiotem są dostawy sprzętu IT, czy też usługi z zakresu IT. Będzie tak np. w przypadku kupna usług chmury obliczeniowej w celu wykonywania pracy zdalnej. Zamawiający może bowiem argumentować, że zakup ten jest niezbędny do przeciwdziałania COVID-19 (zamknięcie miejsca pracy), a także że zachodzi wysokie prawdopodobieństwo szybkiego i niekontrolowanego rozprzestrzeniania się choroby wśród pracowników. W pewnych przypadkach, zastosowanie znajdzie również przesłanka ochrony zdrowia publicznego (np. przy zakupie usług chmurowych na potrzeby monitorowania wykonania obowiązków dotyczących kwarantanny domowej).

Ułatwienia z korzystania z chmury obliczeniowej przez administrację publiczną

Niezależnie od zmian w prawie zamówień publicznych, podejmowane są również inne inicjatywy, które mają ułatwiać podmiotom publicznym korzystanie z usług chmury obliczeniowej. W II kwartale 2020 r. planowana jest w zmiana uchwały nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (WIIP). Uchwała ta odnosi się do usług przetwarzania w Rządowej Chmurze Obliczeniowej lub publicznych chmurach obliczeniowych przez podmioty publiczne wymienione w jej § 6 ust.1.

Planowana zmiana ma na celu ułatwienie przejścia na usługi chmurowe przez te podmioty, których zamiar skorzystania z usług przetwarzania w chmurach wynika z przeciwdziałania COVID-19. Przewidywane ułatwienia dotyczą w szczególności wymogów zawartych w § 6 ust.2 i §8 WIIP. Po pierwsze, planowane jest tymczasowe wyłączenie stosowania załącznika nr 2 do uchwały WIIP, w którym wymieniono kategorie systemów teleinformatycznych, które mogą korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej lub w publicznych chmurach obliczeniowych. Oznacza to zwolnienie z wymogu spełnienia kryteriów klasyfikacji systemów teleinformatycznych (np. wymogu spełnienia jurysdykcji krajowej), jeżeli zamiar skorzystania z usług przetwarzania w publicznych chm-rach obliczeniowych wynika z przeciwdziałania COVID-19. Po drugie, planowane jest tymczasowe skrócenie terminu na wydanie przez właściwy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego opinii w zakresie możliwości wykorzystania publicznych chmur obliczeniowych. W obecnym stanie prawnym, konieczne jest dochowanie 30-dniowego terminu (§ 8).

Liberalizacja obowiązków dla sektora finansowego

W komunikacie Urzędu Krajowego Nadzoru Finansowego (UKNF) z 23 stycznia 2020 r., dotyczącym przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej wprowadzono obowiązki dotyczące dostosowania się do zawartych w nim wymogów oraz uprzedniego informowania UKNF o zamiarze korzystania z usług chmury obliczeniowej. Obowiązki te dotyczą między innymi banków, zakładów ubezpieczeń, funduszy inwestycyjnych oraz funduszy emerytalnych.

Z dniem 25 marca 2020 r. UKNF wprowadził dwie, istotne zmiany w zakresie stosowania w/w Komunikatu. Po pierwsze, dla podmiotów nadzorowanych, które już korzystają z usług chmury obliczeniowej, zmianie uległ termin dostosowania się do wymagań Komunikatu - z dnia 1 sierpnia 2020 r. na dzień 1 listopada 2020 r. Po drugie, dla podmiotów nadzorowanych, które zamierzają dopiero korzystać z usług chmury obliczeniowej, obowiązek informowania UKNF o zamiarze korzystania z usługi z wyprzedzeniem 14-dniowym został zastąpiony obowiązkiem informowania UKNF o fakcie korzystania z usługi nie później niż 30 dni po rozpoczęciu korzystania z usługi.

Obydwie zmiany należy ocenić pozytywnie, przesunięcie terminu poinformowania UKNF-u o korzystaniu z chmury obliczeniowej może być istotnym ułatwieniem, szczególnie w czasie, gdy od pracodawców wymaga się umożliwienia pracy zdalnej, a podmioty nadzorowane zmuszone są do jak najszerszego umożliwienia klientom zdalnego załatwienie spraw. Dzięki wprowadzonym zmianom, zgłoszenia będzie można dokonać już po produkcyjnym wdrożeniu usług chmury obliczeniowej.

Chmura dla administracji – udostępniono katalog usług

Administracja publiczna ma w niedalekiej przyszłości rozpocząć korzystanie z chmury obliczeniowej stworzonej specjalnie na jej potrzeby w ramach Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (WIIP). Zgodnie z informacjami przekazywanymi jeszcze w marcu przez Ministerstwo Cyfryzacji, w tym roku miały zostać uruchomione przetargi na zawarcie umów ramowych z dostawcami publicznych chmur obliczeniowych, którzy będą świadczyć usługi przetwarzania dla administracji. Na razie jednak na rządowej stronie Systemu Zapewniania Usług Chmurowych (ZUCH) pojawiła się – zamiast informacji o przetargach – informacja o otwarciu pierwszego wydania katalogu Publicznych Chmur Obliczeniowych (PChO), który pomoże organom administracji w przeprowadzeniu postępowania zakupowego na usługi oferowane przez dostawców publicznej chmury obliczeniowej.

Od teraz zarówno kupujący (podmioty administracji publicznej), jak i sprzedający (podmioty świadczące usługi przetwarzania w chmurze obliczeniowej) mają możliwość rejestracji w systemie ZUCH. Ci ostatni muszą dodatkowo wypełnić szczegółową deklarację sprzedającego, zawierającą liczne pytania dotyczące m.in. cyberbezpieczeństwa, licencjonowania czy spełnienia wymagań formalnych, która następnie podlega weryfikacji. Dopiero po jej zaakceptowaniu przez Operatora ZUCH usługi oferowane przez sprzedającego będą widoczne w systemie dla kupujących – katalog tych usług może być szeroki, dopuszczono bowiem usługi IaaS (Infrastructure as a Service), PaaS (Platform as a Service) oraz SaaS (Software as a Service). Kupujący mają otrzymać możliwość prostego wyszukiwania usług, których w danej chwili potrzebują.

Jednocześnie opublikowano również Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO)[2], określające wymagania techniczne dotyczące przetwarzania informacji w chmurach obliczeniowych przez jednostki administracji publicznej. Powinny one, przed dokonaniem zakupu konkretnej usługi chmurowej za pośrednictwem systemu ZUCH, przeprowadzić m.in. analizę ryzyka i klasyfikację systemu oraz przetwarzanych za jego pomocą informacji. Na tej podstawie następuję przyporządkowanie do jednego z czterech poziomów wymagań bezpieczeństwa, które wpływają na wybór rodzaju wykorzystywanej chmury (chmura publiczna lub Rządowa Chmura Obliczeniowa) oraz lokalizacji centrum przetwarzania danych. Przyjęty poziom wymagań bezpieczeństwa stanowi również podstawę do określenia środków technicznych z zakresu cyberbezpieczeństwa, które jednostka administracji zobowiązana jest zapewnić wdrażając rozwiązania oparte na chmurze obliczeniowej – szczegółowy ich wykaz stanowi Załącznik nr 5 do SCCO.]

Niestety zgodnie z umieszczonymi na rządowej stronie informacjami w obecnym wydaniu katalogu PChO nie ma możliwości zakupu usług bezpośrednio w systemie ZUCH. Oznacza to konieczność przeprowadzenia postępowania zakupowego przez jednostkę administracji publicznej we własnym zakresie, choć pierwotnym założeniem było prowadzenie postępowań w zamówieniu wspólnym lub przez centralnego zamawiającego[3]. Wobec tego system ZUCH w obecnej formie wydaje się jedynie narzędziem pomocniczym dla organów administracji przy prowadzeniu postępowania na zakup usług chmurowych. Jego wykorzystanie pozwoli organom na zapoznanie się z ofertą dostawców chmur publicznych i kosztami przeprowadzenia migracji, a uzyskane informacje mogą im posłużyć jako wkład do opisu przedmiotu zamówienia. Istnieje jednocześnie szansa, że w niedalekiej przyszłości zostanie zapewniona możliwość zakupu poszczególnych usług bezpośrednio w systemie ZUCH.

W świetle powyższych uwag szczególnie istotne wydają się najświeższe doniesienia prasowe, w których zapowiadane są zmiany legislacyjne w obszarze zamawiania usług przetwarzania w chmurze obliczeniowej przez administrację publiczną. W związku z trwającą pandemią planuje się zarówno nowelizację uchwały dotyczącej Inicjatywy WIIP[4], jak i uchwalenie specustawy, która wyłączy obowiązek stosowania przepisów Prawa zamówień publicznych do zakupu usług chmurowych[5]. Po więcej informacji na temat tych zmian odsyłamy do poprzedniego artykułu „Chmura obliczeniowa i COVID-19 – przepisy i wytyczne".

Przy założeniu sprawnego funkcjonowania systemu ZUCH oraz uzyskania przez organy administracji publicznej prawa do nabywania usług przetwarzania w chmurze obliczeniowej pojawiłaby się możliwość przeniesienia części ich zadań oraz systemów utrzymywanych obecnie on premises do publicznych chmur obliczeniowych. Sektor publiczny dołączyłby tym samym do grona innowacyjnych przedsiębiorstw korzystających z dobrodziejstw przetwarzania w chmurze obliczeniowej i zyskałby większe możliwości pracy zdalnej, co jest szczególnie istotne w dobie pandemii COVID-19.

[1] Zob. https://chmura.gov.pl/zuch.
[2] Zob. https://chmura.gov.pl/informacje/scco/.
[3] Zob. § 10 ust. 4 i 5 uchwały nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (M.P. z 2019 r., poz. 862).
[4] Zob. https://www.money.pl/gielda/rzad-planuje-ulatwienia-w-korzystaniu-publicznych-chmur-obliczeniowych-6499792422352513a.html.
[5] Zob. https://www.crn.pl/aktualnosci/rzad-poluzuje-ograniczenia-dotyczace-chmury.

Chmura obliczeniowa w liczbach

216 mld USD tyle mają wynieść globalne wydatki związane z migracją firm do chmury obliczeniowej do końca 2020 r.

94% ruchu sieciowego w 2021 r. będzie obsługiwane przez „chmurowe centra danych”

492 mld USD tyle wyniesie globalny rynek publicznych usług chmurowych w 2023 r.

IDC przewiduje, że pomimo kurczenia się tegorocznych budżetów IT,**wzrośnie popyt na usługi w chmurze publicznej**, bo firmy zaczną przenosić do niej obciążenia. Światowe wydatki na serwery, pamięć masową, przełączniki **zmniejszą się o 9,2 %** w stosunku do zeszłego roku, za to **o 3,6 % więcej niż w 2019 r.** firmy wydadzą na infrastrukturę chmurową

przyjmuje się, że przedsiębiorstwa, które wdrożyły rozwiązania chmurowe, osiągnęły średnio **15 % oszczędności w obszarze IT**

Przygotowane na podstawie:

- Cisco Global Cloud Index: Forecast and Methodology, 2016–2021
- http://it-manager.pl/chmura-zmienia-rynek-pracy/, powołanie się na dane Gartner
- IDC, Worldwide and Regional Public IT Cloud Services Forecast 2019–2023;#US44202119
- https://www.skyhighnetworks.com/cloud-security-blog/11-advantages-of-cloud-computing-and-how-your-business-can-benefit-from-them/ (Business Impact of the Cloud by Vanson Bourne)

Aukcje 5G zostaną unieważnione?

Komunikaty i przepisy

Ogłoszone przez Urząd Komunikacji Elektronicznej (UKE) aukcje na 4 rezerwacje częstotliwości z pasma 3,6 GHz, umożliwiających rozwój sieci 5G, zostały zawieszone ze skutkiem od 31 marca 2020 r. na czas trwania epidemii COVID-19. Poinformował o tym Prezes UKE 16 marca, odwołując się do regulacji tarczy antykryzysowej przewidujących zawieszenie biegu terminów prowadzonych postępowań.

Niemal dwa tygodnie później Ministerstwo Cyfryzacji (MC) opublikowało na swojej stronie internetowej nieoczekiwany komunikat sugerujący, że aukcje zostaną unieważnione. Powodem miały być wątpliwości formalne dotyczące zawieszenia aukcji, mogące skutkować postępowaniami sądowymi i znacznym opóźnieniem we wdrożeniu 5G (zawieszenie aukcji miało bowiem skutek wsteczny i obejmowało okres, w którym operatorzy podejmowali czynności w ramach postępowania – niektórzy zdążyli nawet złożyć oferty wstępne). Ministerstwo nie przekazało jednak żadnych szczegółowych informacji na temat unieważnienia aukcji, w tym podstawy tego unieważnienia.

Takie informacje znalazły się natomiast w projekcie tzw. tarczy 3.0, którą w czasie, gdy powstaje ten artykuł, rozpatruje Senat. Projekt ten zakłada uzupełnienie warunków rezerwacji częstotliwości o dodatkowy element dotyczący wymagań w zakresie cyberbezpieczeństwa:

> **wymagania dotyczące bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i usług ustalone przez Prezesa UKE z uwzględnieniem rekomendacji i wytycznych Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA), po zasięgnięciu opinii Kolegium,** o którym mowa w art. 64 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560, z 2019 r. poz. 2248 oraz z 2020 r. poz. 695), jeżeli rezerwacja jest dokonywana po przeprowadzeniu aukcji, o której mowa w art. 116 ust. 1 pkt 2.

W planowanej nowelizacji tarczy antykryzysowej (Tarcza 3.0) zakłada się przy tym, że jeśli w aukcji nie określono tego elementu, powinna ona zostać z urzędu unieważniona.

Trudno nie zauważyć rozbieżności między stanowiskami MC i UKE – zwłaszcza że 29 kwietnia na stronie Urzędu opublikowano stanowisko Prezesa UKE, zgodnie z którym aukcja jest prowadzona zgodnie z przepisami prawa i uwzględnia wymogi dotyczące cyberbezpieczeństwa. Wymogi te były zresztą, zgodnie z komunikatem, konsultowane z MC – minister miał stwierdzić, że wystarczające są wymogi ustanowione w Prawie telekomunikacyjnym oraz rozporządzeniach wydanych na jego podstawie.

Praktyczne skutki – opóźnienie 5G w Polsce?

W tym stanie rzeczy istnieją spore wątpliwości, czy nowe aukcje zostaną ogłoszone i rozstrzygnięte wystarczająco szybko, aby udało się dotrzymać terminu wyznaczonego w Europejskiej Agendzie Cyfrowej (do końca 2020 r.) na uruchomienie sieci 5G w przynajmniej jednym dużym mieście w krajach członkowskich. Nie ma przy tym jednak pewności, czy wskazane w Agendzie terminy nie ulegną zmianie z uwagi na pandemię COVID-19.

Niezależnie od tego operatorzy będą musieli wziąć pod uwagę nowe wymogi w zakresie cyberbezpieczeństwa, których kształt nie został jeszcze sprecyzowany. Od ich brzmienia może zależeć planowany model wdrożenia sieci 5G, szczególnie jeśli chodzi o urządzenia czy oprogramowanie, które zamierzali wykorzystać operatorzy.

Warto w tym kontekście przypomnieć, że spore wątpliwości budziło potencjalne wykluczenie Huawei z udziału w budowie 5G w Polsce – ostatecznie jednak na ten krok nie zdecydowało się ani MC w rozporządzeniu dotyczącym sieci 5G, ani UKE w warunkach aukcji. Nowe przepisy, jeśli zostaną przyjęte, znów otworzą taką możliwość.

Trzeba też zaakcentować, że projektowany przepis zakłada uszczegółowienie wymogów w zakresie cyberbezpieczeń-

stwa przez Prezesa UKE po konsultacji z Kolegium do Spraw Cyberbezpieczeństwa. Ustanowione na mocy ustawy o krajowym systemie cyberbezpieczeństwa Kolegium jest organem opiniodawczo-doradczym, w skład którego wchodzi m.in. premier oraz ministrowie właściwi ds. wewnętrznych, ds. informatyzacji, ds. zagranicznych oraz minister obrony narodowej. Kolegium jest uprawnione do wyrażania opinii m.in. w sprawach stosowania konkretnych urządzeń informatycznych lub oprogramowania, przy czym dotychczas żadna taka opinia nie została opublikowana.

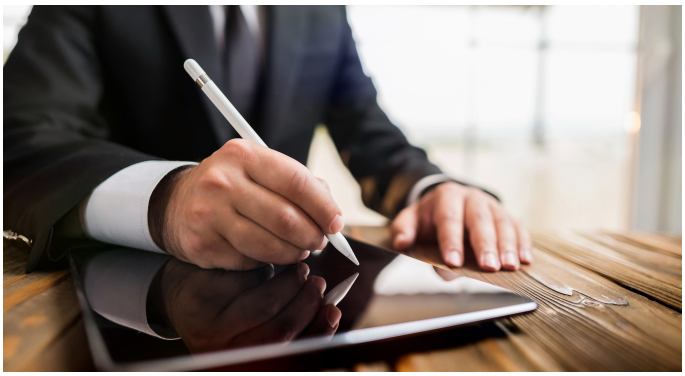
Mając to na uwadze, można stwierdzić, że projektowana zmiana może nie tylko przynieść formalną podstawę do unieważnienia prowadzonej aukcji, ale również stworzyć możliwość ustanowienia dodatkowych wymogów w zakresie cyberbezpieczeństwa. Na obecnym etapie trudno jednak przewidzieć, jaki kształt wymogi te przyjmą, a także czy doprowadzą do wykluczenia konkretnych rozwiązań, urządzeń bądź podwykonawców. Wcześniejsze deklaracje MC i UKE mogą się wkrótce zdezaktualizować – zostanie to przesądzone po ogłoszeniu nowej aukcji na częstotliwości 5G.

Pułapki podpisu elektronicznego

Parafrazując popularne w sieci żarty, można by zadać pytanie: kto wdrożył kwalifikowany podpis elektroniczny w Twojej firmie – (a) CEO, (b) CIO, (c) COVID-19? W istocie, nadal obowiązujące w obszarach fizycznego kontaktu oraz przemieszczania się ograniczenia wprowadzone w związku z pandemią COVID-19 są w przedsiębiorstwach silnym motorem zmian polegających na przechodzeniu na tzw. model paperless. Jednym z jego elementów jest stosowanie w składanych oświadczeniach woli kwalifikowanego podpisu elektronicznego zamiast podpisu własnoręcznego.

Forma elektroniczna czynności prawnych, która wyraża się poprzez stosowanie kwalifikowanego podpisu elektronicznego, nie jest nowością.[1] Od 1 lipca 2016 r. zgodnie z rozporządzeniem eIDAS kwalifikowany podpis elektroniczny rodzi taki sam skutek prawny jak podpis własnoręczny. W Kodeksie Cywilnym przepisy o formie elektronicznej realizowanej za pomocą „bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy ważnego kwalifikowanego certyfikatu" obowiązywały od września 2016 r., zaś od 7 października 2016 r. obowiązywało już nazewnictwo jednolite z eIDAS, tj. kwalifikowany podpis elektroniczny.

W polskich przepisach, w szczególności w art. 78^1 Kodeksu cywilnego, formę elektroniczną traktuje się jako odrębną formę czynności prawnych, która jest realizowana za pomocą kwalifikowanego podpisu elektronicznego. Jednocześnie oświadczenie woli złożone w formie elektronicznej jest równoważne z oświadczeniem woli złożonym w formie pisemnej. Powinni jednak uważać ci, którzy z tego stwierdzenia wywodzą uniwersalną, obowiązującą w każdym przypadku, dwustronną zamienność i równoważność formy pisemnej i elektronicznej. Na gruncie polskich przepisów wskazuje się bowiem, że strony umowy mogą w jej treści zastrzec formę wyłącznie pisemną lub wyłącznie elektroniczną jako wymaganą dla skutecznego zawarcia czy zmiany umowy. Uznanie możliwości takiego umownego wyłączenia równoważności formy pisemnej i elektronicznej, które jak wydaje się na gruncie obecnych regulacji prawnych jest możliwe, rodzi niestety wiele praktycznych problemów, szczególnie obecnie, kiedy w dobie pandemii większość podmiotów próbuje wyeliminować konieczność fizycznej wymiany papierowych dokumentów i liczy na proste zastąpienie zwykłego podpisu – podpisem elektronicznym. Aby uniknąć ryzyka wyłączenia możliwości zastosowania formy elektronicznej dla zmiany umowy, strony powinny dobrze się zastanowić, zanim następnym razem machinalnie umieszczą w jej treści postanowienie: „Dla zmiany umowy strony zastrzegają wyłącznie formę pisemną pod rygorem nieważności". Niektórzy bowiem z takiego postanowienia wywodzą wolę stron wyłączenia możliwości stosowania formy elektronicznej - przy czym według nas przypisywanie takiej intencji stronom, stosującym to postanowienie najczęściej automatycznie, jest niewłaściwe.



Innym praktycznym problemem może być brak odpowiednika parafy. Zastosowanie kwalifikowanego podpisu elektronicznego, który nanosi się na cały plik cyfrowy zawierający treść oświadczenia woli, w tym np. umowy, nie wymaga parafowania. Ponieważ jednak graficzne uwidocznienie podpisu znajduje się tylko na jednej stronie pliku, wiele osób zadaje sobie pytanie, czy – i jak – można nanieść parafy bądź podpisy w dodatkowych miejscach dokumentu. Rozwiązaniem może być umieszczenie skanu parafy czy podpisu w uzgodnionych miejscach przed sygnowaniem całości pliku kwalifikowanym podpisem elektronicznym.

Pewne pułapki wiążą się ponadto z zawieraniem umów w formie elektronicznej z kontrahentami zagranicznymi. Z jednej strony w ramach Unii Europejskiej kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym przez certyfikowanego dostawcę z jednego państwa członkowskiego jest ważny w całej UE, jednak z drugiej strony zasada ta nie ma zastosowania poza Unią, a możliwość

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, s. 73).

uznania za wiążący podpisu elektronicznego pochodzącego spoza UE musi wynikać z umowy zawartej przez UE z danym krajem lub być badana case by case w drodze weryfikacji konkretnego podpisu. tj. jego właściwości, technologii itp.

Wdrażając zatem w organizacji wykorzystywanie kwalifikowanych podpisów elektronicznych w ramach obiegu umów, warto upewnić się, że treść istniejących umów wiążących naszą firmę nie wyklucza stosowania formy elektronicznej, jak również, że treść zawieranych umów jest dostosowana do tej formy, m.in. poprzez wskazanie adresów elektronicznych do korespondencji stron. Konieczne będzie też oczywiście zapewnienie osobom składającym oświadczenia w imieniu przedsiębiorcy kwalifikowanych certyfikatów podpisu elektronicznego, a także oprogramowania umożliwiającego weryfikację podpisów złożonych w formie elektronicznej przez kontrahentów firmy.

Więcej na temat zagadnień związanych ze stosowaniem kwalifikowanego podpisu elektronicznego przeczytasz na naszym blogu.

Warto zadbać o bezpieczeństwo urządzeń IoT

Urządzenia IoT znajdują coraz powszechniejsze zastosowanie, ułatwiając nam funkcjonowanie w kolejnych obszarach życia. Liczba tych urządzeń ciągle rośnie, zaś one same coraz częściej stają się celem ataków. Fundamentalnego znaczenia nabiera więc zarówno odpowiednie zabezpieczenie oprogramowania na etapie produkcji, jak i zapewnienie ochrony urządzeniom wykorzystywanym od lat. Dobrym przykładem są tu układy CAN, stosowane od lat 80. ubiegłego wieku w samochodach w celu umożliwienia komunikacji i współpracy między urządzeniami elektronicznymi i współpracy między nimi. Układy te nie są w żaden sposób zabezpieczane, stając się łatwym celem ataków. Podmioty zajmujące się bezpieczeństwem rozwiązań w sieci mają już świadomość, jak duża może być liczba ataków hakerskich możliwych dlatego, że urządzenia IoT podłączane do sieci nie są odpowiednio zabezpieczane na etapie produkcji.

Kalifornia – ataki i nowe prawo

Ofiarą braku odpowiednich zabezpieczeń padła ostatnio kamera Ring firmy Amazon, przez którą hakerzy wykrzykiwali obsceniczne komunikaty do dzieci, a od ich rodziców żądali okupu za zaprzestanie swoich działań. To wyraźnie pokazało, jak ważne jest wprowadzanie oprogramowania zabezpieczającego urządzenia przed dostępem osób trzecich. W reakcji na to stan Kalifornia wprowadził IoT Security Law – regulację nakładającą na producentów urządzeń IoT obowiązek stosowania się do zasad cyberbezpieczeństwa podczas tworzenia i rozwijania urządzeń internetu rzeczy. Wprowadzone przepisy zobowiązują te podmioty do zapewnienia racjonalnych zabezpieczeń urządzeń, które są:

- odpowiednie do przeznaczenia i funkcji urządzenia;
- dostosowane do rodzaju danych, jakie to urządzenie pobiera, zachowuje lub przekazuje;
- przeznaczone do ochrony urządzeń przed nieautoryzowanym dostępem, zniszczeniem, użyciem, modyfikacją lub ujawnieniem.

Zgodnie z uchwalonym prawem dosyć ogólny wymóg stosowania „racjonalnych zabezpieczeń" będzie spełniony, jeśli:

- każde wyprodukowane urządzenie IoT będzie chronione unikalnym wstępnie zaprogramowanym hasłem;
- urządzenie będzie zawierać zabezpieczenie wymuszające na użytkowniku wygenerowanie nowego sposobu uwierzytelnienia, zanim uzyska on dostęp do urządzenia po raz pierwszy.

ENISA i akt o cyberbezpieczeństwie

Niewątpliwie Kalifornia wykonała ważny krok w kierunku uregulowania obowiązku stosowania zabezpieczeń dla urządzeń IoT. W naszym krajowym porządku prawnym na ten moment brak jest analogicznych przepisów, co jednak nie oznacza, że nie są one potrzebne. Konkretnych propozycji uregulowań w tym zakresie dotychczas jednak nie przedstawiono.

Na poziomie unijnym natomiast wprowadzono niedawno europejskie ramy certyfikacji (na gruncie aktu o cyberbezpieczeństwie, tj. rozporządzenia PE i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA oraz certyfikacji cyberbezpieczeństwa). Ramy certyfikacji muszą jednak zostać dopiero skonkretyzowane w poszczególnych programach dla danych usług (np. usług chmurowych) i procesów (w całym cyklu życia danego urządzenia). Warto przy tym podkreślić, że europejskie programy certyfikacji co do zasady nie będą obowiązkowe, lecz dobrowolne – można się jednak spodziewać, że staną się one powszechne i przyczynią się nie tylko do wzrostu konkurencji na rynku, ale też do poprawy bezpieczeństwa konkretnych rozwiązań IoT.

W tym obszarze niewątpliwie aktywną rolę będzie pełnić ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa. Warto zresztą wskazać, że już teraz prowadzi ona prace w tym zakresie, czego efektem jest m.in. zbiór dobrych praktyk w zakresie bezpieczeństwa IoT – ogłoszony w listopadzie 2019 roku raport pt. „Good Practices for Security of IoT", mający promować bezpieczeństwo IoT w fazie projektowania.

Podsumowując: jakkolwiek obecnie w Polsce nie obowiązuje żadne wiążące prawo obligujące producentów urządzeń IoT do ich odpowiedniego zabezpieczania ani nie funkcjonuje żaden konkretny krajowy model certyfikacyjny IoT, tak powtarzające się incydenty bezpieczeństwa mogą przynieść pożądany skutek w postaci unormowań dotyczących odpowiedniej ochrony na etapie produkcji urządzeń IoT przez ich producentów, co pokazuje przykład kalifornijskiej regulacji.

IP Box – przeważają pozytywne interpretacje podatkowe

W związku z przyjęciem tzw. tarczy antykryzysowej roczne zeznanie podatkowe wyjątkowo w tym roku można złożyć do końca maja (bez obaw o odsetki czy odpowiedzialność karnoskarbową). Podatnicy otrzymali dzięki temu więcej czasu na skorzystanie z obowiązujących od 2019 roku przepisów dotyczących ulgi IP Box – wspierającego innowacyjnych twórców rozwiązania polegającego na zastosowaniu obniżonej, 5-procentowej stawki podatku dochodowego od osób fizycznych lub osób prawnych.

Pozytywne interpretacje podatkowe

Z ulgi IP Box skorzystać mogą przedsiębiorcy prowadzący działalność badawczo-rozwojową, którzy wytwarzają co najmniej jedno z kwalifikowanych praw własności intelektualnej, takich jak patenty czy też programy komputerowe. Do dochodu uzyskiwanego z tych praw mogą oni zastosować 5-procentową stawkę podatku dochodowego w miejsce opodatkowania go stawką liniową czy stawkami ze skali podatkowej. Dzięki uldze mogą więc zapłacić znacznie niższy podatek.

Pomimo wątpliwości dotyczących interpretacji obecnych przepisów podatkowych można się spodziewać, że wielu podatników skorzysta z ulgi IP Box. Wskazuje na to przede wszystkim duża liczba złożonych w ostatnich miesiącach wniosków o wydanie indywidualnej interpretacji podatkowej – od początku roku, złożono ich ponad 700 (głównie w imieniu programistów prowadzących jednoosobową działalność gospodarczą). W przeważającej większości Dyrektor

Pomimo wątpliwości dotyczących interpretacji obecnych przepisów podatkowych można się spodziewać, że wielu podatników skorzysta z ulgi IP Box. Wskazuje na to przede wszystkim duża liczba złożonych w ostatnich miesiącach wniosków o wydanie indywidualnej interpretacji podatkowej – od początku roku, złożono ich ponad 700 (głównie w imieniu programistów prowadzących jednoosobową działalność gospodarczą). W przeważającej większości Dyrektor

Krajowej Informacji Skarbowej, który wydaje interpretacje, uznaje stanowiska podatników za prawidłowe, zapewniając im tym samym podatkową ochronę (o czym piszemy niżej). Statystyki za marzec i kwiecień bieżącego roku przedstawiają się następująco:

Miesiąc	Ilość złożonych wniosków	Interpretacje stanowisko wnioskodawców za:		
		prawidłowe w całości	**nieprawidłowe** w części	**nieprawidłowe** w całości
Marzec	268	210 (ok. 78%)	33 (ok. 12%)	25 (ok. 9,3%)
Kwiecień	233	201 (ok. 86%)	30 (ok. 13%)	2 (ok. 0,8%)

Analiza dostępnych już interpretacji skłania przy tym do wniosku, że u podłoża większości interpretacji uznających stanowisko wnioskodawców za nieprawidłowe leżą przede wszystkim kwestie ogólne oraz techniczne zasady rozliczeń, a nie kwestionowanie badawczo-rozwojowego charakteru działalności wnioskodawców. Uznając stanowisko wnioskodawcy za nieprawidłowe, Dyrektor KIS wskazuje zwłaszcza na:

- nieprawidłowości lub brak prowadzenia ewidencji dla celów IP Box, umożliwiającej identyfikację przychodów, kosztów i dochodów dotyczących kwalifikowanych praw własności intelektualnej;
- konieczność ustalania dochodu z kwalifikowanych praw własności intelektualnej w sposób jednostkowy dla każdego z tych praw, nie zaś sumarycznie dla wszystkich z nich;
- nieprawidłowości przy wyliczaniu wskaźnika nexus, dotyczące np. nieprawidłowego zaliczania do kosztów bezpośrednio poniesionych na wytworzenie kwalifikowanego IP należności w zakresie np. najmu biura.

Gra komputerowa jako kwalifikowane prawo własności intelektualnej

Interpretacje podatkowe rozstrzygają przy tym często wątpliwości, które branża IT sygnalizowała od początku – szczególnie te związane z pojęciem „autorskie prawo do programu komputerowego". Nie było bowiem jasne, czy należy utożsamiać je z pojęciem programu komputerowego wypracowanym na gruncie prawa autorskiego, które za programy komputerowe uznaje jedynie kod źródłowy, kod wynikowy i dokumentację techniczną, czy też traktować je szerzej – uznając za oprogramowanie także inne elementy w nim bezpośrednio osadzone (grafikę, interfejs itd.). Wątpliwości tych nie rozwiały także objaśnienia Ministerstwa Finansów, które rekomendowały każdorazowe składanie wniosków o wydanie interpretacji indywidualnej. Szerzej na ten temat pisaliśmy w artykule dostępnym na naszym blogu (tutaj).

W interpretacjach Dyrektora KIS można zauważyć dosyć liberalne podejście, polegające na szerokim rozumieniu pojęcia autorskiego prawa do programu komputerowego. W rozstrzygnięciu m.in. wniosku złożonego przez jednego z czołowych polskich producentów gier komputerowych uznano, że prawo do wytwarzanych przez spółkę gier komputerowych (których status na gruncie prawa autorskiego nie jest jednoznaczny) można uznać za autorskie prawo do programów komputerowych w rozumieniu przepisów dotyczących ulgi IP Box.

Korzystne skutki interpretacji podatkowych

Duża liczba wniosków o wydanie interpretacji podatkowej nie jest zaskoczeniem. W zamian za bardzo niską opłatę (40 zł) podatnik otrzymuje bowiem stanowisko Dyrektora KIS potwierdzające lub negujące prawidłowość działań, które już podjął bądź podjąć dopiero zamierza. Podatnik nie ma obowiązku zastosowania się do interpretacji podatkowej, ale jeśli się na to zdecyduje, zyskuje ochronę przed negatywnymi konsekwencjami wynikającymi z zastosowania się do niej w przypadku następczego rozstrzygnięcia organów podatkowych, np. w toku kontroli. Ochrona ta obejmuje:

- brak obowiązku zapłaty odsetek za zwłokę;
- brak wszczęcia postępowania o przestępstwo lub wykroczenie skarbowe;
- brak obowiązku zapłaty podatku, w sytuacji gdy interpretacja dotyczyła zdarzeń przyszłych (w przypadku gdy interpretacja dotyczyła zdarzeń zaistniałych przed wydaniem interpretacji, obowiązek zapłaty podatku powstanie)

Trzeba mieć jednak na uwadze, że powyższy skutek wystąpi tylko pod warunkiem, że stan faktyczny przedstawiony we wniosku o wydanie interpretacji nie ulegnie zmianie i będzie opisany na tyle szczegółowo, aby podatnik mógł wykazać, że wydana interpretacja rzeczywiście go dotyczyła. Warto więc przygotować wniosek ze szczególną starannością, nie ograniczając się do lakonicznych stwierdzeń o prowadzeniu działalności badawczo-rozwojowej lub wytwarzaniu programów komputerowych. W innym przypadku wydana interpretacja może okazać się w toku kontroli nieprzydatna.

Orzekanie Krajowej Izby Odwoławczej – co dalej?

Zawieszenie prac Krajowej Izby Odwoławczej

W dniu 12 marca 2020 r. na stronie internetowej Urzędu Zamówień Publicznych (UZP) pojawił się wspólny komunikat Prezesa UZP oraz Prezesa Krajowej Izby Odwoławczej[1], w którym poinformowano, że w okresie od 16 do 27 marca 2020 r. zawiesza się organizację i rozpoznawanie spraw przed Krajową Izbą Odwoławczą (KIO). UZP powiadomił także o ograniczeniu kontaktu bezpośredniego w Kancelarii UZP i KIO[2].

Następnie 27 marca 2020 r. UZP opublikował informację[3], z której wynika, że w związku z ogłoszonym stanem epidemii oraz z przyjętymi przez Sejm RP zmianami w tzw. ustawie o COVID-19 w czasie trwania epidemii nie będą odbywały się rozprawy ani posiedzenia jawne przed KIO. UZP zaznaczył przy tym, że wnoszenie odwołań do KIO odbywa się na niezmienionych zasadach. Oznacza to, że bieg terminów do wnoszenia do KIO odwołań, przystąpień i innych pism procesowych nie uległ zawieszeniu. Powyższe okoliczności potwierdza treść art. 15zzs ust. 3 tzw. ustawy o COVID-19.

Informator UZP – zapowiedź przywrócenia prac KIO

W dniu 21 kwietnia 2020 r. UZP opublikował Informator UZP nr 1/2020[4], w którym na stronie 9 zamieszczono artykuł pt. „Prace nad przywróceniem orzekania Krajowej Izby Odwoławczej". Z jego treści wynika, że UZP wraz z KIO oraz Ministerstwem Rozwoju pracuje nad rozwiązaniami zmierzającymi do wznowienia rozpatrywania odwołań złożonych do KIO. W artykule poinformowano ponadto, że przygotowany został tymczasowy tryb orzekania KIO na podstawie dokumentacji przekazanej przez strony postępowania.

Najnowsze sygnały z UZP

W dniu 28 kwietnia 2020r.[5] UZP opublikował kolejny dokument, w którym poinformował, że Rada Ministrów przyjęła projekt ustawy o zmianie niektórych ustaw w zakresie działań osłonowych w związku z rozprzestrzenianiem się wirusa SARS-CoV-2. Wskazał przy tym, że tenże projekt przewiduje uchylenie art. 15zzs Ustawy o COVID-19.

W art. 43 datowanego na 27 kwietnia 2020 r. projektu nowelizacji Ustawy o COVID-19 założono uchylenie przywołanego wyżej przepisu art. 15zzs. Może to oznaczać, że w razie uchwalenia projektu KIO wznowi pracę w normalnym trybie, choć brak co do tego całkowitej pewności Jednocześnie oznaczałoby to rezygnację z wprowadzenia szczególnych rozwiązań w pracy KIO.

Co dalej z orzekaniem przez KIO

Obecnie KIO nie orzeka, co przyczynia się do przestoju w zamówieniach publicznych – rynku, który w 2018 r. stanowił niemalże 10 % polskiego PKB[6], co z pewnością nie jest korzystne dla polskiej gospodarki. Jak wynika z treści art. 183 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 1843 j.t.), dalej: „PZP", jeżeli sprawa jest rozpatrywana przez KIO, niemożliwe jest zawarcie umowy w sprawie zamówienia publicznego. Wprawdzie art. 183 ust. 2 PZP przewiduje możliwość uchylenia powyższego zakazu, jednak do rozpatrzenia wniosku w trybie art. 183 ust 2 PZP konieczne byłoby orzeczenie KIO. Skoro więc KIO nie orzeka, obecnie nie można spodziewać się uchylenia zakazu zawarcia umowy w sprawie zamówienia publicznego.

[1] Komunikat dostępny jest pod adresem: https://www.uzp.gov.pl/aktualnosci/komunikat-ws.-dzialalnosci-kio-w-zwiazku-z-pandemia-koronawirusa.
[2] Zgodnie z informacją dostępną pod adresem: https://www.uzp.gov.pl/aktualnosci/ograniczony-dostep-bezposredni.
[3] Informacja dostępna jest pod adresem: https://www.uzp.gov.pl/aktualnosci/dzialalnosc-krajowej-izby-odwolawczej-w-czasie-epidemii.
[4] Informator dostępny jest pod adresem: https://www.uzp.gov.pl/__data/assets/pdf_file/0010/43003/INFORMATOR_1_2020.pdf.
[5] Dokument dostępny pod adresem: https://www.uzp.gov.pl/strona-glowna/slider-aktualnosci/odwieszenie-postepowan-przed-kio-projekt-ustawy-przyjety-przez-rade-ministrow/odwieszenie-postepowan-przed-kio-projekt-ustawy-przyjety-przez-rade-ministrow.
[6] Dokładniej – ok. 9,55% zgodnie z informacjami wynikającymi ze Sprawozdania Prezesa Urzędu Zamówień Publicznych o funkcjonowaniu systemu zamówień publicznych w 2018 r., dostępnego pod adresem: https://www.uzp.gov.pl/__data/assets/pdf_file/0020/41555/Sprawozdanie-UZP-za-2018.pdf.

Doniesienia prasowe dotyczące „Tarczy 4.0”

Pojawiły się także doniesienia prasowe o kolejnych planach dotyczących przywrócenia orzekania KIO. Mają one zostać zawarte w tzw. „Tarczy 4.0”, której treść do dnia dzisiejszego nie została zamieszczona na stronach internetowych Rządu lub Sejmu. Część informacji prasowych stwierdza, że projekt ustawy zakłada wznowienie prac KIO bez udziału stron[7]. Z innych informacji wynika, że ostatecznie zrezygnowano z pomysłu wymiany pisemnych stanowisk i orzekania bez udziału stron[8]. W chwili obecnej nie można wykluczyć żadnego scenariusza.

Pomysł wznowienia prac w oparciu o pisemne stanowiska stron wydaje się rozsądnym rozwiązaniem, które z jednej strony zapewniłoby wznowienie orzekania przez KIO, a z drugiej strony prowadziłoby do zachowania standardów bezpieczeństwa w związku z zagrożeniem epidemicznym.

Zrezygnowanie z rozpraw jest oczywiście minusem, gdyż strony zostałyby pozbawione możliwości bezpośredniego prezentowania swojego stanowiska członkom składu orzekającego. Jednakże takie rozwiązanie wydaje się uzasadnione i akceptowalne w obecnej sytuacji.

Trzeba zauważyć, że komunikaty dotyczące dalszych prac KIO trudno uznać za spójne. Aktualne warunki są wyjątkowe, jednak jednolity przekaz dotyczący wznowienia prac KIO (w tym informacja o trybie orzekania) mógłby pomóc ustabilizować sytuację na rynku zamówień publicznych. Najistotniejsze z punktu widzenia interesu jego uczestników jest przywrócenie orzekania KIO niezależnie od form rozpatrywania spraw.

[7] Por. https://www.rynekinfrastruktury.pl/wiadomosci/drogi/tarcza-40-co-ma-sie-zmienic-w-zamowieniach-publicznych-w-zwiazku-covid19-71645.html.
[8] Por. https://biznes.gazetaprawna.pl/artykuly/1474042,zaswiadczenie-o-niezaleganiu-ze-skladkami-zus-przetarg.html.

Platforma e-Zamówienia – aktualny status prac

Informacje dotyczące statusu prac nad Platformą e-Zamówienia

Platforma e-Zamówienia ma być powszechnie dostępną, bezpłatną platformą, która umożliwi zamawiającym dostosowanie się do obowiązku prowadzenia postępowania o udzielenie zamówienia publicznego przy użyciu środków komunikacji elektronicznej[1].

Platforma ma zostać wykonana przez wykonawcę wybranego w ramach postępowania o zamówienie publiczne. Dnia 17 września 2019 r. Urząd Zamówień Publicznych (UZP) wszczął postępowanie składające się z dwóch części:

- dotyczące budowy Platformy e-Zamówienia,
- dotyczące świadczenia usług Inżyniera Kontraktu podczas budowy Platformy e-Zamówienia[2].

W zakresie obu części postępowania wystąpiły pewne problemy. Pierwotny wybór najkorzystniejszej oferty w części dotyczącej budowy Platformy e-Zamówienia został zakwestionowany przez Krajową Izbę Odwoławczą, przez co UZP musiał dokonać ponownej oceny ofert. Finalnie umowa w sprawie budowy Platformy e-Zamówienia została zawarta dnia 31 marca 2020 r. Wykonawcą został Pentacomp Systemy Informatyczne S.A[3].

Z kolei część postępowania dotycząca świadczenia usług Inżyniera Kontraktu podczas budowy Platformy e-zamówienia została unieważniona, gdyż wpłynęła tylko jedna oferta, której cena przewyższała kwotę, którą UZP zamierzało przeznaczyć na sfinansowanie zamówienia[4]. Wobec powyższego, UZP wszczął kolejne postępowanie, po zakończeniu którego zawarto umowę dnia 9 kwietnia 2020 r. Wykonawcą został Softiq sp. z o.o.[5]

[1] Cele i oczekiwane rezultaty w stosunku do Platformy e-Zamówienia według UZP dostępne są pod linkiem: https://www.uzp.gov.pl/e-zamowienia2/informacje
[2] Link do postępowania: https://uzp.bip.gov.pl/publiccontracts/view/20623
[3] Szczegółowy harmonogram realizacji tego projektu dostępny jest pod adresem: https://www.uzp.gov.pl/e-zamowienia2/informacje
[4] Więcej informacji pod adresem: https://uzp.bip.gov.pl/fobjects/details/646767/uniewaznienie-postepowania-cz-ii-pdf.html
[5] Link do postępowania: https://uzp.bip.gov.pl/publiccontracts/view/21413

Czym jest Platforma e-Zamówienia?

Platforma e-Zamówienia ma zapewnić kompleksową możliwość obsługi postępowania o udzielenie zamówienia publicznego w formie elektronicznej i ma posiadać więcej funkcjonalności, niż Platforma miniPortal. Przykładowo, na Platformie e-Zamówienia mają zostać udostępnione wzory dokumentów wykorzystywanych w postępowaniu o udzielenie zamówienia publicznego. Platforma e-Zamówienia ma również zapewniać zamawiającym możliwość składania do UZP rocznych sprawozdań o udzielonych zamówieniach publicznych.

Korzystanie z Platformy e-Zamówienia ma być dobrowolne. Zamawiający będą mieli wybór, czy chcą korzystać z bezpłatnej platformy e-Zamówienia, czy też korzystać z platform prywatnych.

Obecnie funkcję taką spełnia miniPortal (https://miniportal.uzp.gov.pl/). Platforma miniPortal ma charakter tymczasowy i ma zostać zastąpiona przez Platformę e-Zamówienia.

Dlaczego Platformy e-Zamówienia powinna być gotowa do 1 stycznia 2021 r.?

Datą rozstrzygającą z punktu widzenia budowy Platformy e-Zamówienia jest 1 stycznia 2021 r., tj. data wejścia w życie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019, dalej: „Nowe PZP". Nowe PZP przewiduje obowiązek prowadzenia wszystkich postępowań elektronicznie (zarówno o wartości równej lub przekraczającej progi unijne, jak i postępowań o wartości niższej niż progi unijne) – art. 61 i n. Nowego PZP. W porównaniu do obecnego stanu prawnego Nowe PZP obejmuje więc elektronizację postępowań o wartości niższej niż progi unijne.

Jak wynika z harmonogramu realizacji umowy na budowę Platformy e-Zamówienia, nie wszystkie funkcjonalności, Platformy e-Zamówienia mają być gotowe do dnia 1 stycznia 2021 r. Przykładowo Moduł Ofert/Wniosków Komponent Kryptograficzny, Zarządca Kluczy ma być dostępny w I kwartale 2021 r. Aby możliwe było składanie ofert za pośrednictwem Platformy e-Zamówienia przed wejściem w życie Nowego PZP, moduł ten powinien być gotowy nie później niż w IV kwartale 2020 r. Zamieszczenie harmonogramu realizacji umowy nie wyklucza jednak wykonania modułu we wcześniejszym terminie

Niezależnie od powyższego nie ulega wątpliwości, że UZP bardzo zależy na udostępnieniu Platformy e-Zamówienia w zakresie umożliwiającym przeprowadzenie postępowania o udzielenie zamówienia publicznego przed dniem 1 stycznia 2021 r. Prezes UZP podkreślał to w swych publicznych wystąpieniach. Wynika to z tego, że w Nowym PZP nałożono na zamawiających obowiązek prowadzenia postępowań o wartości niższej niż progi unijne przy wykorzystaniu narzędzi elektronicznych. Skoro taki obowiązek został przez ustawodawcę nałożony, to powinny istnieć ogólnodostępne, bezpłatne narzędzia umożliwiające realizację tego obowiązku. W przeciwnym wypadku mniejsi zamawiający, jak przykładowo jednostki samorządu terytorialnego, będą musieli korzystać z platform prywatnych i ponosić koszty nabycia dostępu do tych platform.

W przypadku, gdyby platforma e-Zamówienia nie była gotowa do dnia 1 stycznia 2021 r., możliwe jest również wykorzystywanie miniPortalu. Platforma ta posiada jednak ograniczone funkcjonalności i nie jest rozwiązaniem idealnym. W świetle wielokrotnie przesuwanych terminów pełnej elektronizacji, dotrzymanie terminu 1 stycznia 2021 wydaje się być kluczowe dla UZP z punktu widzenia wizerunkowego.

NADCHODZĄCE WYDARZENIA

#szkolenia #konferencje #warsztaty

"Nowa ustawa - prawo zamówień publicznych obowiązująca od 1 stycznia 2021 oraz szczególnie regulacje w zakresie PZP dot. sytuacji epidemicznej COVID-19"

Zespół IT-Telco

Rejestracja wkrótce

"Umowy ICT w okresie pandemii COVID-19"

adw. Xawery Konarski, r.pr. Agnieszka Wachowska

Więcej informacji >>

"Licencjonowanie oraz prawo autorskie w obszarze IT i środowisku cyfrowym"

„Umowy wdrożeniowe i utrzymaniowe na systemy IT – problematyka" - adw. Xawery Konarski

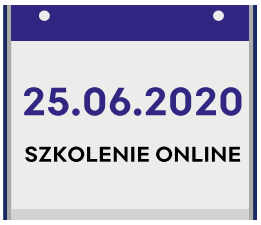
„Spory z branży IT i koncyliacyjne metody ich rozwiazywania" - r. pr. Joanna Stecyk

Więcej informacji >>

"Zwinne wdrożenia w umowach IT (Agile, Prince2 Agile) - przygotowanie i negocjowanie umów w projektach IT przy zwinnym podejściu"

r.pr. Agnieszka Wachowska

Więcej informacji >>



"Zmiana i rozwiązanie umowy IT za szczególnym uwzględnieniem umów zawieranych w sektorze publicznym"

r.pr. Joanna Stecyk, r.pr. Piotr Nepelski

Więcej informacji >>

ARTYKUŁY

#czasopisma

„Prawidłowe postawienie zarzutu warunkiem skutecznego odwołania do KIO"
- artykuł autorstwa Piotra Nepelskiego ukazał się w kwietniowym numerze „Zamówienia Publiczne. Doradca"

„Nowe zasady udzielania zamówień wspólnych"
- artykuł autorstwa Tomasza Krzyżanowskiego ukazał się w kwietniowym dodatku do wydania czasopisma „Zamówienia Publiczne Doradca"

„Umowa na świadczenie zewnętrznych usług z zakresu cyberbezpieczeństwa"
- artykuł autorstwa Agnieszki Wachowskiej i Joanny Jastrząb ukazał się w kwietniowym numerze „IT Professional"

„Outsourcing usług bezpieczeństwa"
– artykuł autorstwa Joanny Jastrząb ukazał się w kwietniowym numerze czasopisma „IT w Administracji"

ZESPÓŁ IT-TELCO/PZP

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

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

Piotr Nepelski
Radca prawny
piotr.nepelski@traple.pl

Tomasz Krzyżanowski
Radca prawny
tomasz.krzyżanowski@traple.pl

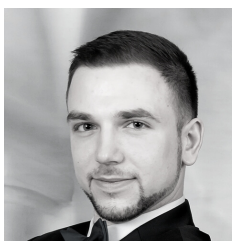
Joanna Stecyk
Radca prawny
joanna.stecyk@traple.pl

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

Joanna Jastrząb
Radca prawny
joanna.jastrzab@traple.pl

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

Wojciech Karwacki
Aplikant radcowski
wojciech.karwacki@traple.pl



Aleksander Elmerych
Prawnik
aleksander.elmerych@traple.pl

Michał Kalinowski
Prawnik
michal.kalinowski@traple.pl

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