03/2020 CZERWIEC

NEWSLETTER

IT-TECH/PZP LAW

W NUMERZE:

Traple
Konarski
Podrecki
& Wspólnicy

TKP

IOT (INTERNET RZECZY)

#akty prawne #prawo i biznes

Internet Rzeczy – najważniejsze regulacje prawne w Polsce

Internet Rzeczy (Internet of Things, IoT) to sieć różnego rodzaju fizycznych urządzeń, wyposażonych we wbudowaną technologię (np. RFID) umożliwiającą komunikację, wymianę danych oraz interakcję – zarówno wewnątrz sieci, jak i ze środowiskiem zewnętrznym. Istotą koncepcji Internetu Rzeczy jest możliwość połączenia i komunikacji z fizycznymi obiektami, wcześniej niezdolnymi do samodzielnego generowania, transmisji i odbioru danych. Dzięki temu obiekty te są w stanie samodzielnie rozpoznać zdarzenia i zmiany zachodzące w otoczeniu oraz w sposób autonomiczny podjąć odpowiednią akcję i/lub reakcję bez interwencji człowieka.

Powszechność zastosowania rozwiązań IoT czyni zasadnym poddanie analizie najważniejszych przepisów prawnych znajdujących zastosowanie do tego rodzaju innowacji.

IoT – obszary regulacyjne

Obecnie ani w Polsce, ani na świecie nie ma aktu prawnego całościowo (horyzontalnie) regulującego Internet Rzeczy, nie planuje się również uchwalenia przepisów tego rodzaju. Przyjmowane są natomiast regulacje wertykalne dotyczące wybranych tylko obszarów funkcjonowania IoT. Przykładem jest obowiązujący od 1 stycznia 2020 r. California IoT Act, w ramach którego dokonano nowelizacji stanowego kodeksu cywilnego. Istotą tej regulacji jest nałożenie na producentów urządzeń podłączonych do Internetu dodatkowych obowiązków w zakresie zapewnienia bezpieczeństwa tych urządzeń, a także informacji w nich przechowywanych.

Polskie przepisy regulujące korzystanie z Internetu Rzeczy podzielić można na cztery podstawowe grupy: przepisy prawne dotyczące cyberbezpieczeństwa, przepisy o ochronie danych osobowych i prywatności, przepisy prawa cywilnego oraz odpowiedzialności za szkodę wywołaną przez produkt niebezpieczny, przepisy dotyczące praw własności intelektualnej.

IoT a cyberbezpieczeństwo

Cyberbezpieczeństwo jest wskazywane jako główne źródło zagrożeń Internetu Rzeczy. Podstawowe znaczenie w tym zakresie odgrywają regulacje składające się na tzw. pakiet cyberbezpieczeństwa:

- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (ustawa o KSC)[1];
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)[2].

Ustawa o KSC nie odnosi się wprost do Internetu Rzeczy, niewątpliwie jednak podmioty korzystające z rozwiązań IoT oraz podmioty świadczące usługi związane z IoT mogą być adresatami określonych w niej obowiązków. Dotyczy to zarówno operatorów usług kluczowych (np. przedsiębiorstwo energetyczne), jak i dostawców usług cyfrowych (np. dostawca usługi chmury obliczeniowej, w której przechowywane są dane zebrane przez urządzenia IoT).

Znaczenie aktu o cyberbezpieczeństwie dla Internetu Rzeczy wyraża się z kolei w stworzeniu ram prawnych, zgodnie z którymi wykonywana będzie certyfikacja cyberbezpieczeństwa produktów, usług i procesów. Warto w związku z tym zaznaczyć, że choć ma ona w zasadzie być dobrowolna, to w akcie o cyberbezpieczeństwie zastrzeżono możliwość wprowadzenia obligatoryjnej certyfikacji określonych produktów czy usług, zarówno w przepisach prawa unijnego, jak i prawa krajowego. W przyszłości nie jest więc wykluczone, że dla wprowadzenia do obrotu wybranych produktów czy usług IoT konieczne będzie uzyskanie odpowiedniego certyfikatu cyberbezpieczeństwa.

IoT a ochrona danych osobowych i prywatności

Internet Rzeczy nie został wprost wymieniony w RODO, niemniej w motywie nr 30 wśród identyfikatorów internetowych, które mogą doprowadzić do identyfikacji danej osoby fizycznej, wymieniono m.in. etykiety RFID. Nie ulega więc

[1] Dz.U. z 2018 r., poz. 1560 z późn. zm.
[2] Dz.U.UE.L.2019.151.15.

wątpliwości, że szczególnie w przypadku „konsumenckiego" Internetu Rzeczy, a więc sytuacji gdy urządzenia te są wykorzystywane przez osoby fizyczne (np. urządzenia „do mierzenia siebie"), dochodzi do przetwarzania danych osobowych.

Przy ocenie dopuszczalności przetwarzania danych osobowych w związku z Internetem Rzeczy szczególne znaczenie mają wytyczne Grupy Roboczej art. 29, zastąpionej obecnie Europejską Radą Ochrony Danych (EROD). Wymienić należy w szczególności następujące opinie:

- opinia Europejskiej Rady Ochrony Danych nr 1/2020 dotycząca przetwarzania danych osobowych w kontekście pojazdów połączonych i aplikacji związanych z mobilnością;
- opinia Grupy Roboczej art. 29 nr 8/2014 w sprawie najnowszych osiągnięć w zakresie Internetu przedmiotów przyjęta w dniu 16 września 2014 r. (WP 223).

Do najważniejszych problemów związanych z ochroną danych osobowych i IoT zaliczyć należy:

- brak kontroli podmiotu danych nad rozpowszechnianiem dotyczących go informacji (np. w przypadku komunikacji między przedmiotami, która może zostać wywołana automatycznie, jak i domyślnie, bez wiedzy danej osoby);
- niską „jakość" zgód na przetwarzanie danych osobowych, uzyskiwanych od użytkowników IoT;
- ograniczenia możliwości zachowania anonimowości przez użytkowników IoT;
- niższe bezpieczeństwo urządzeń IoT z uwagi na konieczność utrzymania równowagi między wydajnością a bezpieczeństwem urządzenia IoT.

Niezależnie od ochrony określonej w RODO na podstawie odrębnych przepisów chroniona jest również prywatność użytkowników urządzeń IoT. Zastosowanie znajduje w szczególności przepis art. 173 Ustawy z dnia 16 lipca 2004 r. – Prawo Telekomunikacyjne[3], określający zasady, na podstawie których dopuszczalne jest „przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym". Podłączone do sieci urządzenia IoT niewątpliwie kwalifikować należy jako „telekomunikacyjne urządzenia końcowe" w rozumieniu tego przepisu.

IoT a przepisy prawa cywilnego i odpowiedzialność za szkody

Z cywilnoprawnego punktu widzenia korzystanie z IoT obejmuje korzystanie z:

- rzeczy (urządzenie podłączone do sieci);
- oprogramowania (aplikacje i systemy IoT);
- usługi (np. dostęp do sieci, dostarczanie danych).

Rozróżnienie to ma kluczowe znaczenie dla kształtowania treści umów oraz – uzupełniających je – przepisów kodeksu cywilnego.

Dla dostawców rozwiązań IoT szczególnie istotne znaczenie mają przepisy o odpowiedzialności za szkody wywołane w związku z ich stosowaniem. Powstaje zatem pytanie o stosowanie się regulacji o odpowiedzialności za szkodę wywołaną przez produkt niebezpieczny (art. 4491 Ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny, dalej: k.c.). Warto pamiętać, że „produktem niebezpiecznym" w rozumieniu tych przepisów jest w zasadzie tylko rzecz ruchoma (art. 4491 § 2 k.c.). Z tego reżimu odpowiedzialności wyłączeni są więc np. dostawcy aplikacji czy usług IoT. Należy również podkreślić, że odpowiedzialność za produkt niebezpieczny dotyczy tylko relacji z konsumentem, a także że ograniczenie odpowiedzialności dotyczy tylko szkody na mieniu (art. 4492 k.c.). Nie obejmuje więc np. szkody związanej z naruszeniem prywatności powstałej w wyniku naruszenia bezpieczeństwa informacji przechowywanych w urządzeniu IoT. Z punktu widzenia Internetu Rzeczy szczególne znaczenie może mieć także przepis, zgodnie z którym producent nie odpowiada wtedy, gdy „nie można było przewidzieć niebezpiecznych właściwości produktu, uwzględniając stan nauki i techniki w chwili wprowadzenia produktu do obrotu" (art. 4493 § 2 k.c.). Ta przesłanka zwalniająca z odpowiedzialności może znaleźć zastosowanie np. w razie różnego rodzaju szkód wywołanych nowymi postaciami cyberataków.

IoT a prawa własności intelektualnej

Z punktu widzenia przepisów prawa własności intelektualnej dla nabywców urządzeń IoT szczególne znaczenie prawne ma odpowiedź na pytanie o tytuł prawny do eksploatacji zainstalowanych w tych urządzeniach programów komputerowych oraz o możliwość rozporządzania taką rzeczą lub udostępnienia jej do korzystania przez osoby trzecie. W doktrynie przyjmuje się, że korzystanie przez nabywcę rzeczy (urządzenia IoT) z programu komputerowego zainstalowanego w zbywanej rzeczy następuje na podstawie ustawowej licencji w związku z wyczerpaniem prawa do rozpowszechniania kopii programu komputerowego. Nabywca rzeczy uzyskuje bowiem możliwość korzystania z programu, który jest już zainstalowany przez uprawniony podmiot (producenta rzeczy, który uzyskał licencję od podmiotu praw do programu komputerowego), a więc nabywa kopię programu na nośniku materialnym. W konsekwencji nabywca może również dokonać jej dalszego zbycia wraz z zainstalowanym w niej programem komputerowym[4].

[3] Dz.U. z 2004 r. Nr 171, poz. 1800.

[4] J. Pisuliński, Licencja na oprogramowanie a rozporządzanie rzeczą, [w:] „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 2018/2, s. 74–84.

Internet Rzeczy – korzyści i trendy

Rynek IoT

745 miliardów dolarów tyle wyniosą wydatki na Internet Rzeczy (IoT) w 2019 r. Wydatki utrzymają dwucyfrową roczną stopę wzrostu w całym okresie prognozy (2017–2022 r.) i przekroczą bilion dolarów w 2022 r.[1]. (Raport IDC)

Powody wdrożeń IoT

Ponad połowa (56%) przedsiębiorstw stwierdziła, że celem wdrożenia IoT była poprawa wydajności i produktywności, 49% chciało uzyskać lepszą jakość produktów lub usług, a 37% oszczędność kosztów[2].

Funkcje biznesowe, które najbardziej korzystają z rozwiązań IoT[3]:

- zarządzanie danymi i analityka – **38%**;
- usługi / wsparcie klienta – **37%**;
- produkty lub usługi (B2B lub B2C) – **36%**;
- produktywność pracowników – **32%**;
- zarządzanie łańcuchem dostaw / logistyka – **28%**;
- zarządzanie infrastrukturą technologiczną – **24%**;
- zarządzanie zasobami – **14%**;
- zarządzanie energią – **11%**.

IoT i bezpieczeństwo

Wdrażanie IoT w fabrykach niesie za sobą istotne zagrożenia związane z bezpieczeństwem. Wraz ze wzrostem liczby urządzeń podłączonych do sieci, częstotliwości połączeń z Internetem, liczby hotspotów Wi-Fi czy przetwarzania danych w chmurze zwiększa się także prawdopodobieństwo cyberataków na przedsiębiorstwa. **Jak wynika z biuletynu organizacji ICS-CERT, najbardziej zagrożonymi sektorami w przemyśle nadal są: energetyka (blisko 20% ataków), gospodarka wodna (ok. 40%) oraz firmy wielosektorowe (25%).**

Niezaszyfrowane jest 98% całego ruchu IoT, co naraża dane osobowe i poufne w sieci. Podatnych na ataki o średniej lub dużej skali jest 57% urządzeń Internetu Rzeczy, 41% ataków wykorzystuje luki w zabezpieczeniach urządzeń, ponieważ ataki oparte na technologiach informatycznych przeszukują urządzenia podłączone do sieci, próbując wykorzystać znane słabości[4].

[1] Przemysłowy Internet Rzeczy (IIoT). Fabryki przyszłości w dobie rewolucji przemysłowej, raport Instytutu Innowacyjnej Gospodarki na zlecenie Emerson Polska, Warszawa 2019.
[2] IoT Enterprise Survey 2019/2020, raport Ovum.
[3] The IoT Business Index 2020, raport The Economist Intelligence Unit.
[4] 2020 Unit 42 IoT Threat Report, raport Palo Alto Networks.

IoT sposobem na wykrywanie ognisk koronawirusa

Internet Rzeczy znajduje coraz szersze zastosowanie i zaczyna być wykorzystywany do walki z koronawirusem. Jedna ze szwajcarskich firm pracuje nad rozwiązaniem opartym na architekturze Internetu Rzeczy, będącym połączeniem sensora temperatury, beacona Bluetooth oraz układu odpowiedzialnego za szyfrowanie przesyłanych danych. Za pomocą sensorów system będzie automatycznie identyfikować ogniska infekcji oraz określać obszar konieczny do odizolowania w celu uniemożliwienia dalszego rozprzestrzeniania się wirusa. System ten miałby wykorzystywać miliardy czujników różnego typu, głównie mierzących temperaturę ciała, połączonych w jedną sieć stale skanującą informacje pozyskane z sensorów. Zebrane dane miałyby być przekazywane za pośrednictwem sieci 5G do instalowanych lokalnie bramek (np. w domu użytkownika) oraz na serwer odpowiedniej organizacji zarządzającej walką z pandemią. Wszystkie dane przekazywane za pośrednictwem systemu mają być domyślnie szyfrowane, anonimizowane i udostępniane do analizy z wykorzystaniem technologii blockchain. Takie rozwiązanie pozwalałoby wykrywać nowe przypadki zakażeń w czasie rzeczywistym i niezwłocznie rekomendować izolacje konkretnych osób czy wskazanych obszarów.

Włochy z kolei, z dniem 8 czerwca br., po uzyskaniu zgody regionalnego Rzecznika Praw Obywatelskich, wprowadziły w części północnych regionów testową Immuni contact-tracing app – aplikację zaprojektowaną do pomocy w zarządzaniu drugą fazą epidemii koronawirusa. Aplikacja używa Bluetootha i działa na podstawie automatycznie generowanych kodów. Kiedy dwa smartfony z zainstalowaną Immuni app znajdują się w odległości mniej niż jednego metra od siebie, dochodzi do automatycznej wymiany generowanych przez aplikacje kodów, które z kolei umożliwiają śledzenie poprzednich kontaktów użytkowników na wypadek, gdyby któryś z nich został zdiagnozowany jako zakażony wirusem. Z kolei służba zdrowia, rejestrując nowy przypadek zakażenia, może za zgodą pacjenta dodać do systemu kod wygenerowany dla danego pacjenta. Na tej podstawie system przesyła ostrzeżenia do użytkowników aplikacji, którzy mieli kontakt z osobą zakażoną. Twórcy zapewniają, że generowane kody są anonimowe i nie zawierają danych osobowych użytkowników aplikacji, a sama jej instalacja jest oczywiście dobrowolna.

W obu powyższych przypadkach pojawia się kluczowe pytanie o ochronę prywatności i danych osobowych użytkowników oraz bezpieczeństwo IoT. Twórcy Immuni app zapewniają o zgodności rozwiązania z włoskim i europejskim prawem dotyczącym ochrony danych osobowych (jego założeniem jest przechowywanie danych użytkowników w ich urządzeniach, a nie w centralnym serwerze). Aplikacja nie ma też funkcji lokalizowania użytkownika. Szwajcarzy zapewniają z kolei, że projektowane rozwiązanie, nieco bardziej inwazyjne z punktu widzenia gromadzenia danych użytkowników i konieczności zapewnienia ich bezpieczeństwa, ma być w pełni anonimowe i nie naruszać prywatności użytkowników.

AI (SZTUCZNA INTELIGENCJA)

#rekomendacje_i_wytyczne

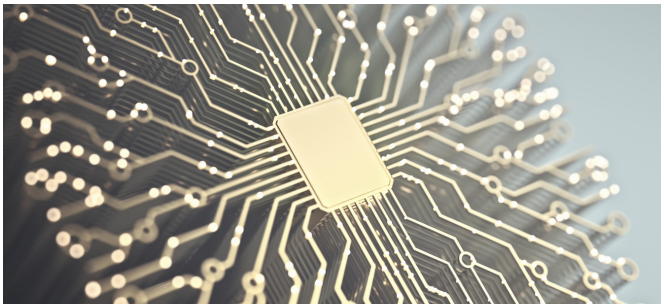
Unijna propozycja przepisów regulujących odpowiedzialność za działania sztucznej inteligencji

W dniu 4 maja 2020 r. komitet ds. prawnych Parlamentu Europejskiego przedstawił propozycje przepisów regulujących zasady odpowiedzialności za szkody wyrządzone przez sztuczną inteligencję (ang. artificial intelligence, dalej: AI). Przepisy mają w przyszłości przybrać kształt aktu prawnego o randze rozporządzenia. Zaprezentowany projekt nie wprowadza znaczącej rewolucji w zakresie, rekonstruowanej już z obecnych przepisów, odpowiedzialności podmiotów posługujących się AI, jednak znacząco ułatwia dochodzenie roszczeń osobom poszkodowanym, przy okazji nakładając nowe obowiązki, np. obligatoryjne ubezpieczenia. Projektowane przepisy są ograniczone zarówno przedmiotowo, jak i podmiotowo, a pozostały poza projektem rozporządzenia zakres odpowiedzialności ma zostać uregulowany poprzez nowelizację dyrektywy o produktach wadliwych – jako odpowiedzialność za produkt niebezpieczny. Poniżej przedstawiamy najważniejsze zagadnienia projektu, a więcej na ten temat można przeczytać na naszym blogu.

Zakres stosowania

Zakres przedmiotowy przedstawionych przepisów został zawężony jedynie do szkód związanych ze zdrowiem i życiem poszkodowanego oraz szkód na mieniu wyrządzonych przez AI. Zgodnie z propozycją rozporządzeniem nie zostałyby objęte zatem problemy odpowiedzialności kontraktowej, np. z tytułu niewykonania zobowiązania. Zakres podmiotowy planowanych przepisów również jest wąski i obejmuje jedynie tzw. wdrażających. W projekcie przewidziana została definicja legalna wdrażającego, zgodnie z którą za wdrażającego należy uznać podmiot, który:

- decyduje o użyciu AI;
- sprawuje kontrolę nad powiązanym ryzykiem;
- czerpie korzyści z działania AI.



Definicja ta nie jest jasna i obecnie trudno jednoznacznie określić katalog podmiotów wyczerpujących wskazane przesłanki. Z całą pewnością – na co również wskazują projektodawcy – dochodzić może do sytuacji, w których także użytkownik danego urządzenia może zostać uznany za wdrażającego. Wdrażającymi będą zapewne również podmioty oferujące określone produkty, które zostały przez nich wyposażone w systemy AI. Z kolei odnośnie do odpowiedzialności producentów oprogramowania, programistów, wytwórców zarekomendowano nowelizację dyrektywy o produktach niebezpiecznych, która miałaby swoim zakresem objąć produkty AI.

Definicja AI

W projekcie zdecydowano się na wprowadzenie definicji legalnej AI, co wydaje się krokiem w dobrym kierunku, ułatwia bowiem stosowanie proponowanych przepisów. Niemniej jednak specyfika systemów AI powoduje, że utworzenie wyczerpującej definicji AI jest bardzo trudne lub wręcz niemożliwe. Niestety także zaproponowana regulacja nie jest w tym zakresie doskonała. Zgodnie z brzmieniem definicji:

- **System AI** – oznacza system, który wykazuje inteligentne zachowanie poprzez analizę pewnych danych wejściowych i podejmowanie działań, z pewną dozą autonomii, w celu osiągnięcia określonych celów. Systemy AI mogą być oparte wyłącznie na oprogramowaniu, działając w wirtualnym świecie, lub mogą być osadzone w urządzeniach sprzętowych.
- **Autonomiczny** – oznacza system AI, który działa poprzez postrzeganie określonych danych wejściowych i bez konieczności postępowania zgodnie z zestawem wcześniej ustalonych instrukcji, pomimo swojego zachowania będąc ograniczonym przez cel, który został wyznaczony, i inne istotne wybory projektowe dokonane przez jej dewelopera

Największe zalety definicji to wskazanie na najistotniejsze cechy systemów AI: autonomię, wykazywanie inteligentnego zachowania i przetwarzanie danych wejściowych, ponadto objęcie zakresem definicji zarówno samodzielnego oprogramowania, jak i konkretnych produktów wyposażonych w oprogramowanie AI. Wadą jest uzależnienie systemu AI od działania w celu osiągnięcia określonego celu, co nie zawsze

ma miejsce, zwłaszcza w przypadku uczenia nienadzorowanego, w którym cel nie jest z góry określony. Te AI są szczególnie niebezpieczne, bardzo trudno jest bowiem ocenić ich potencjalne możliwości, a w konsekwencji ryzyko, jakie niesie za sobą ich używanie.

Dwa reżimy odpowiedzialności

Projekt zakłada podział systemów AI na dwa rodzaje, co w konsekwencji wprowadza także dwa reżimy odpowiedzialności – **na zasadzie ryzyka i na zasadzie winy.**

Odpowiedzialność **na zasadzie ryzyka** przewidziana została dla **tzw. systemów AI wysokiego ryzyka**. Chociaż projekt wprowadza definicję wysokiego ryzyka, to należy stwierdzić, że w tym zakresie posługuje się wieloma pojęciami nieostrymi, co znacznie utrudnia jej stosowanie. Uzupełnieniem dla tej definicji jest tabela, stanowiąca załącznik do projektu. Wskazuje się w niej sektor gospodarki oraz rodzaj systemu AI, które będą określane mianem tych wysokiego ryzyka. Tabela taka ma być aktualizowana co 6 miesięcy, a obecnie prezentuje się następująco:

System AI	Sektor krytyczny
Bezzałogowe statki powietrzne	transport
Pojazdy autonomiczne o poziomach 4 i 5	transport
Autonomiczne systemy zarządzania ruchem	transport
Roboty autonomiczne	wsparcie
Autonomiczne urządzenia do czyszczenia miejsc publicznych	wsparcie

Jak widać, proponowana regulacja w obecnym kształcie najbardziej dotyczy sektora transportu – autonomicznych pojazdów i systemów sterowania ruchem drogowym, a także autonomicznych robotów i urządzeń wspierających. Wszystkie te systemy mają potencjalnie kontakt z dużą liczbą osób, co przekłada się na poziom stwarzanego ryzyka. Odpowiedzialność zostanie wyłączona jedynie wtedy, kiedy zdarzenie powodujące szkodę powstanie na skutek siły wyższej.

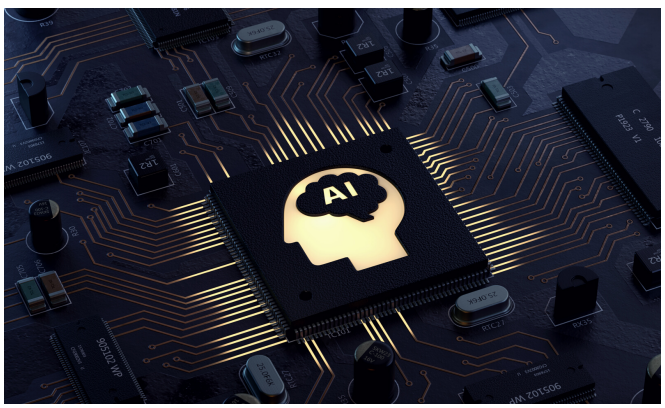
Odpowiedzialność **na zasadzie winy** dotyczy **wszystkich innych**, niewymienionych powyżej, systemów AI. Oprócz możliwości uwolnienia się od odpowiedzialności z powodu działania siły wyższej możliwe będzie właściwie dowolnie wykazywanie braku swojej winy, z tym wyjątkiem, że w wypadku ingerencji w system AI osoby trzeciej, której nie da się namierzyć lub która nie ma środków na pokrycie szkody, nadal odpowiedzialnym będzie wdrażający system AI. Jest to istotne odstępstwo w kierunku odpowiedzialności na zasadzie ryzyka. Ponadto nie można powoływać się na fakt, że system zadziałał autonomicznie, jest to bowiem immanentna cecha systemów AI.

Obowiązkowe ubezpieczenie

Podmioty wdrażające systemy AI wysokiego ryzyka będą musiały mieć obowiązkowe ubezpieczenia, których kwoty powinny odpowiadać zakresowi odpowiedzialności – w wypadku śmierci i naruszenia zdrowia jest to 10 mln euro, a w wypadku szkód na mieniu 2 mln euro. Ubezpieczenia nie byłyby obowiązkowe, jeżeli określone podmioty objęte byłyby innymi ubezpieczeniami wymaganymi dla prowadzenia określonej działalności, a ich zakres pozwalałby na pokrycie wymienionych powyżej kwot.

Dla kogo ma to znaczenie?

Projektowane przepisy mają szczególne znaczenie dla wszystkich podmiotów, które chcą wdrażać w swoich przedsiębiorstwach urządzenia wyposażone w systemy AI, w szczególności te określone mianem systemów AI wysokiego ryzyka. Wprowadzenie odpowiedzialności na zasadzie ryzyka pozostawia bowiem dla takich podmiotów bardzo niewielki margines błędu – w zdecydowanej większości przypadków w razie powstania szkody podmioty będą za nią odpowiedzialne. Takie ukształtowanie odpowiedzialności ma ułatwić poszkodowanym, niezwiązanym z danym urządzeniem, przedsiębiorstwem czy wdrażającym, dochodzenie swoich praw, zwłaszcza w przypadku konieczności pokrycia kosztów leczenia.



Incydenty i ich koszty – co pokryje cyberpolisa?

Ostatnie miesiące to czas wdrażania na dużą skalę narzędzi umożliwiających pracę zdalną i świadczenie usług w sieci. Konieczność przeniesienia działalności do świata online przyspieszyła niewątpliwie transformację cyfrową przedsiębiorstw, przyczyniając się także do zweryfikowania wdrożonych procedur i zabezpieczeń przed różnego rodzaju ryzykami cybernetycznymi.

W wielu przypadkach takie procedury i zabezpieczenia są dopiero projektowane i przyjmowane, a przedsiębiorcy szukają dróg ochrony przed stratami wynikającymi z ryzyk cybernetycznych.

„Koszty" incydentu cyberbezpieczeństwa

Statystyki jasno pokazują, że liczba różnego rodzaju cyberataków (w tym kampanii ransomware, ataków DDoS czy phishingu) rokrocznie rośnie, a szczególnie wzmożona aktywność cyberprzestępców jest obserwowana również w okresie pandemii[1].

W efekcie, jeśli atak został przeprowadzony skutecznie (np. doprowadził do przełamania zabezpieczeń lub paraliżu działalności przedsiębiorcy), zaatakowany musi liczyć się z różnego rodzaju stratami, takimi jak koszty:

- reakcji na incydent, zabezpieczenia dowodów i informatyki śledczej celem ustalenia przyczyn i zakresu incydentu (co może wymagać zaangażowania specjalistów);
- zapłaty okupu – w razie ataku ransomware;
- przywrócenia działania systemu, którego dotyczył incydent, i danych przetwarzanych w tym systemie;
- przerwy w działalności przedsiębiorcy spowodowanej incydentem, przekładającej się na utratę lub ograniczenie zysków;
- ochrony reputacji, zwłaszcza kiedy incydent wiąże się z wyciekiem dużej ilości danych mogących stanowić tajemnicę przedsiębiorstwa lub danych osobowych klientów.

Odpowiedzialność prawna

Nie można przy tym zapominać, że brak odpowiednich, dostosowanych do oszacowanego poziomu ryzyka zabezpieczeń może również doprowadzić do odpowiedzialności prawnej przedsiębiorcy objętego atakiem – administracyjnej oraz cywilnej, **co może wiązać się z wysokimi karami oraz odszkodowaniami.**

Trzeba pamiętać, że incydenty cyberbezpieczeństwa często wiążą z **ujawnieniem lub dostępem osób nieuprawnionych do danych przetwarzanych w systemie, w tym danych osobowych.** Świadczą o tym przykłady naruszeń opisane przez zespół RODO na str. 13–14 w najnowszym wydaniu newslettera, dostępnym tutaj. W takich przypadkach **Prezes Urzędu Ochrony Danych Osobowych może wszcząć postępowanie zmierzające do weryfikacji, czy dane osobowe były odpowiednio** (tj. proporcjonalnie do oszacowanego ryzyka) **zabezpieczone**, czy też administrator lub przetwarzający nie spełnił wymogów określonych w RODO. To z kolei otwiera drogę do nałożenia kar administracyjnych, które mogą okazać się dotkliwe dla przedsiębiorców.

Kary administracyjne zostały przewidziane także w **ustawie o krajowym systemie cyberbezpieczeństwa**[2], której podlegają nie tylko **operatorzy usług kluczowych** (podmioty wyznaczone w drodze decyzji administracyjnej), lecz także **dostawcy usług** (dostawcy usług chmurowych, internetowe platformy handlowe oraz wyszukiwarki internetowe – z wyłączeniem mikroprzedsiębiorców i małych przedsiębiorców).

Incydenty cyberbezpieczeństwa mogą także skutkować **odpowiedzialnością cywilnoprawną i koniecznością zapłaty kar umownych lub odszkodowań dla klientów**. W tym kontekście najważniejsze są postanowienia zawartych z kontrahentem umów, które wyznaczą zakres i zasady odpowiedzialności, w tym przesądzą zwłaszcza, czy można dostawcy przypisać odpowiedzialność za incydent, czy też na gruncie umowy i przepisów prawa swoje obowiązki wykonał należycie.

[1] Por. https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance; https://www.cyberdefence24.pl/zagrozenia/wzrost-liczby-atakow-ransomware-oraz-zadan-hakerow-w-2019-roku; https://www.kaspersky.pl/o-nas/informacje-prasowe/3262/trzykrotny-wzrost-liczby-atakow-ddos-na-edukacje-i-administracje-podczas-pandemii-koronawirusa.
[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560 z późn. zm.).

Cyberpolisy – przyszłość rynku ubezpieczeń?

Mając na uwadze, że uprzednie określenie kosztów, które będzie musiał ponieść przedsiębiorca w razie incydentu, jest w praktyce niemożliwe i wymaga założenia sporego marginesu na nieprzewidziane okoliczności, przedsiębiorcy coraz częściej decydują się na zawarcie umowy ubezpieczenia ryzyk cybernetycznych. Nierzadką obecnie sytuacją jest też wymaganie przez kontrahentów przedstawienia polisy obejmującej ryzyka cybernetyczne. Oferta rynku ubezpieczeń stale się poszerza, a polisy w zdecydowanej większości obejmują koszty opisane w artykule – w tym także koszty kar administracyjnych.

Ubezpieczenia w tym zakresie pozostają wciąż dobrą praktyką, a nie obowiązkiem przedsiębiorców. To jednak ma szanse się zmienić w niedalekiej przyszłości – przynajmniej w przypadku niektórych technologii. Warto zwrócić uwagę na rekomendacje dotyczące uregulowania zasad odpowiedzialności sztucznej inteligencji, zaprezentowane przez komitet ds. prawnych dla Komisji Europejskiej, opublikowane w dniu 4 maja 2020 r. Przewidują one obowiązkowe ubezpieczenia dla niektórych sektorów oraz niektórych systemów wykorzystujących sztuczną inteligencję. Więcej piszemy o tym w artykule pt. Unijna propozycja przepisów regulujących odpowiedzialność sztucznej inteligencji.

Nie jest przy tym wykluczone, że unijny lub polski ustawodawca zdecydują się wprowadzić analogiczne rozwiązania także dla innych disruptive technologies, takich jak Internet Rzeczy czy chmura obliczeniowa. Są one coraz powszechniejsze, a co za tym idzie, technologie te umożliwiają gromadzenie dużej ilości danych, których wykorzystanie może przynieść znaczne straty zarówno usługodawcom, jak i ich klientom. Niezależnie jednak od konkretnych regulacji prawnych, które mogą zostać przyjęte w przyszłości, warto rozważyć ubezpieczenie ryzyk cybernetycznych i wybrać konkretny produkt ubezpieczeniowy adekwatny do prowadzonej działalności.

CHMURA OBLICZENIOWA

#aktualności #akty_prawne

Cyberbezpieczna chmura obliczeniowa – przepisy ustawy o krajowym systemie cyberbezpieczeństwa

W ostatnich latach zainteresowanie chmurą obliczeniową niewątpliwie wzrasta. Zwiększenie tego zainteresowania widoczne jest w raporcie Chmura publiczna w Polsce 2019. Wykorzystanie, bezpieczeństwo, plany rozwoju, który został przygotowany przez IDG we współpracy z Oktawave pośród podmiotów, które korzystają lub planują korzystać z rozwiązań cloud computingu. Z raportu wynika, że prawie jedna trzecia (30%) przedsiębiorstw planuje wzrost wydatków na usługi IaaS na poziomie około 11–29%, natomiast kolejne 23% indagowanych zamierza zwiększyć nakłady o około 30–49%. Co więcej, według danych raportu Computerworld TOP200 edycja 2019, przychody działających na polskim rynku dostawców chmury przekroczyły w 2018 r. miliard złotych, przy wzroście o 23% w stosunku do roku poprzedniego.

Oprócz wymiernych korzyści z inwestowania w chmurę obliczeniową, takich jak poprawa elastyczności i zwiększona skalowalność zasobów, poprawa dostępności i ciągłości biznesu, przesunięcie wydatków na IT z modelu CAPEX na OPEX[1], na uwagę zasługuje również rola, jaką odegrała chmura obliczeniowa podczas pandemii COVID-19, o czym pisaliśmy w majowym wydaniu newslettera IT-TECH/PZP LAW (dostępnym pod tym linkiem).

Warto przy tym zwrócić uwagę na ramy prawne, które regulują cloud computing. Obok wielu regulacji tzw. soft law, przepisów o ochronie danych osobowych, przepisów sektorowych (finansowych, life science, public), w istotnym zakresie świadczenie usług chmurowych zostało uregulowane przez ustawodawcę w ustawie o krajowym systemie cyberbezpieczeństwa[2]. Kształtuje ona status dostawców usług cyfrowych i obowiązków nałożonych na takie podmioty.

Status dostawcy usług cyfrowych

Ustawa o krajowym systemie cyberbezpieczeństwa nakłada obowiązki w zakresie cyberbezpieczeństwa na dostawców usług cyfrowych. Rodzaje usług cyfrowych zostały określone w załączniku nr 2 do ustawy, w którym pośród usługi internetowej platformy handlowej i usługi wyszukiwarki internetowej została wskazana również usługa przetwarzania w chmurze. Przez usługę przetwarzania w chmurze należy rozumieć „usługę umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników".

Zgodnie z art. 17 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa dostawcą usługi cyfrowej jest natomiast osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową, z wyjątkiem mikroprzedsiębiorców i małych przedsiębiorców, o których mowa w ustawie – Prawo przedsiębiorców .

Zgodnie zatem z intencją ustawodawcy statusu dostawcy usług cyfrowych nie posiadają mikroprzedsiębiorcy i mali przedsiębiorcy, a w tym zakresie ustawa o krajowym systemie cyberbezpieczeństwa odwołuje się do definicji ustawowych określonych w ustawie – Prawo przedsiębiorców[3].

[1] Chmura obliczeniowa w Polsce 2020, badanie „Computerworld".
[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560 z późn. zm.), która w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6
lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1).
[3] Art. 7 ust. 1 pkt 1 i 2 Ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (t.j. Dz. U. z 2019 r., poz. 1292 z późn. zm.).

Zgodnie zatem z intencją ustawodawcy statusu dostawcy usług cyfrowych nie posiadają mikroprzedsiębiorcy i mali przedsiębiorcy, a w tym zakresie ustawa o krajowym systemie cyberbezpieczeństwa odwołuje się do definicji ustawowych określonych w ustawie – Prawo przedsiębiorców. Poniżej prezentujemy w formie tabelarycznej przesłanki stwierdzenia, jaki status posiada dany przedsiębiorca:

Wielkość przedsiębiorcy	Liczba zatrudnionych pracowników	Roczny obrót	Roczna suma bilansowa
Duży przedsiębiorca	co najmniej 250 **ORAZ**	ponad 50 mln euro **LUB**	ponad 43 mln euro
Średni przedsiębiorca	max. 249 **ORAZ**	max. 50 mln euro **LUB**	max. 43 mln euro
Mały przedsiębiorca	max. 49 **ORAZ**	max. 10 mln euro **LUB**	max. 10 mln euro
Mikroprzedsiębiorca	max. 9 **ORAZ**	max. 2 mln euro **LUB**	max. 2 mln euro

W kontekście uznania danego podmiotu za mikroprzedsiębiorcę lub małego czy też średniego przedsiębiorcę, a w konsekwencji za dostawcę usługi cyfrowej, istotne jest zwrócenie uwagi, że powyższe wartości są odnoszone do jednego z dwóch ostatnich lat obrotowych – a więc zmiana statusu (np. z małego na średniego przedsiębiorcę) może nastąpić po zakończeniu roku obrotowego.

Obowiązki dostawcy usługi cyfrowej

Ustawa o krajowym systemie cyberbezpieczeństwa nakłada na dostawców usług cyfrowych obowiązki w zakresie cyberbezpieczeństwa.

Do obowiązków nałożonych przez ustawodawcę na dostawców usług cyfrowych należy przede wszystkim podjęcie właściwych i proporcjonalnych środków technicznych i organizacyjnych określonych w rozporządzeniu wykonawczym 2018/151[4] w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej (art. 17 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa).

Środki te mają zapewnić cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz mają uwzględniać:

- bezpieczeństwo systemów informacyjnych i obiektów;
- postępowanie w przypadku obsługi incydentu;
- zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej;
- monitorowanie, audyt i testowanie;
- najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi, o których mowa w rozporządzeniu wykonawczym 2018/151.

Do dostawcy usługi cyfrowej należy również obowiązek podjęcia środków zapobiegających i minimalizujących wpływ incydentów na usługę cyfrową w celu zapewnienia ciągłości świadczenia tej usługi (art. 17 ust. 3 ustawy o krajowym systemie cyberbezpieczeństwa), a także szczegółowe obowiązki w zakresie wykrywania, rejestrowania, analizowania oraz klasyfikowania incydentów (opisane w art. 18–20 ustawy o krajowym systemie cyberbezpieczeństwa). W tym zakresie dostawca usługi cyfrowej m.in.:

- przeprowadza czynności umożliwiające wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów;
- zgłasza incydent istotny niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
- zapewnia obsługę incydentu istotnego i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;
- przekazuje operatorowi usługi kluczowej, który świadczy usługę kluczową za pośrednictwem dostawcy usług, informacje dotyczące incydentu mającego wpływ na ciągłość świadczenia usługi kluczowej tego operatora.

Polecamy Państwa uwadze lekturę rozporządzenia wykonawczego 2018/151, które precyzuje elementy, jakie mają zostać uwzględnione przez dostawców usług cyfrowych przy określaniu i przedsiębraniu środków mających na celu zapewnienie poziomu bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez dostawców w kontekście oferowania usług, jak również parametry, które należy wziąć pod uwagę w celu ustalenia, czy incydent ma istotny wpływ na świadczenie tych usług.

[4] Rozporządzenie wykonawcze Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz.U.UE.L.2018.26.48 z 31.01.2018).

Zmiany w ustawie o krajowym systemie cyberbezpieczeństwa

Przy okazji prac Ministerstwa Cyfryzacji nad rozporządzeniem dotyczącym bezpieczeństwa sieci piątej generacji (5G)[5] pojawiły się doniesienia o nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa dotyczącej nie tylko sieci 5G, ale również o znacznie szerszym zakresie.

Obecnie nie ma jednak projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. W wykazie prac legislacyjnych i programowych Rady Ministrów znajduje się jednak informacja o projekcie zarejestrowanym pod numerem UD68 i dotyczącym projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, ustawy – Prawo telekomunikacyjne oraz ustawy – Ordynacja podatkowa, z planowanym terminem przyjęcia tego projektu przez Radę Ministrów określonym na II kwartał 2020 r.

Jako istotne rozwiązania ujęte w projekcie w zakresie ustawy o krajowym systemie cyberbezpieczeństwa wskazano wprowadzenie zamkniętego katalogu dopuszczalnych specjalnych środków ochronnych (takich jak ostrzeżenie, wpis na listę podmiotów stanowiących zagrożenie dla cyberbezpieczeństwa oraz środki zabezpieczające). Na szczegóły musimy jednak poczekać do czasu opublikowania projektu nowelizacji.

[5] Projektowane rozporządzenie Ministra Cyfryzacji w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług.

Prace nad chmurą europejską i projekt Gaia-X

Zgodnie z zapowiedzią, wynikającą z treści komunikatu Komisji Europejskiej (KE) z 19 lutego 2020 r.: A European strategy for data, obecnie trwają prace mające na celu stworzenie infrastrukturalnych, organizacyjnych, a także prawnych ram, które umożliwią powstanie europejskiej chmury (tzn. inicjatywy pozwalającej na większe uniezależnienie się od dostawców amerykańskich czy chińskich).

Dominacja na globalnym rynku usług chmurowych dostawców przede wszystkim amerykańskich (Amazon Web Services, Microsoft Azure, Google, IBM) oraz chińskich (Alibaba), a także fakt, że w czołówce światowych cloud providerów brakuje graczy europejskich, spędza sen z powiek decydentom UE. Rozwiązaniem ma być europejska platforma chmurowa, zapewniająca zgodność ze strategią Jednolitego Rynku Cyfrowego, w której dane będą przetwarzane w zgodzie z unijnymi wartościami, standardami i wymogami prawnymi, a do tego na serwerach nienależących do firm, nad którymi jurysdykcję mają USA czy Chiny, mogące kierować do tych firm żądania wydania danych przechowywanych w chmurze.

Komisja chce wspierać rozwój europejskiej chmury, z naciskiem na synergię pomiędzy inicjatywami ogólnounijnymi oraz krajowymi (np. Gaia-X, co do której współpracę nawiązały obecnie Niemcy i Francja).

Wsparcie od strony organizacyjnej i prawnej ma polegać w szczególności na stworzeniu „cloud rulebook" (takim pojęciem posługuje się A European strategy for data) – czyli przekrojowego instrumentu zbierającego unijne wymogi prawne dotyczące przetwarzania danych w chmurze, wynikające w szczególności z RODO, rozporządzenia Free flow of data, dyrektywy NIS i aktu o cyberbezpieczeństwie.

W ramach strategii KE dla danych zapowiedziano przeznaczenie 6 mld euro na stworzenie jednolitego rynku danych.

Inicjatywa Gaia-X

W trakcie budowy jest obecnie projekt Gaia-X (link), mający realizować powyższe założenia i przewidujący stworzenie europejskiego ekosystemu i infrastruktury dla przetwarzania danych. Start Gaia-X ogłaszał w październiku ubiegłego roku niemiecki minister gospodarki Peter Altmaier, a obecnie projekt ten nabiera dużego rozpędu, mając już na pokładzie oprócz Niemiec również Francję.

Liderzy projektu Gaia-X deklarują, że jest on otwarty dla innych państw członkowskich, których przyłączenie się do budowy tej europejskiej platformy jest mile widziane. Ponadto nie jest ona zamknięta dla dostawców pochodzących spoza UE – pod warunkiem, że spełnią oni zasady i wymogi przetwarzania danych przyjęte w ramach projektu Gaia-X.

Jeżeli chodzi o te ostatnie, to powstał już pierwszy dokument (w maju 2020 r.) – GAIA-X: Policy Rules and Architecture of Standards (link) – określający wspólne standardy w zakresie przechowywania i przetwarzania danych na serwerach zlokalizowanych na terenie UE, wynikające z unijnego prawa, w szczególności dotyczącego ochrony danych osobowych. Akceptacja i wdrożenie tych zasad stanowić będzie warunek wstępny certyfikacji i onboardingu pozwalającego na świadczenie usług przez dostawcę chmurowego w ramach projektu Gaia-X.

Twórcy Gaia-X wskazują jako naczelne przyświecające projektowi zasady:

- Europejska ochrona danych.
- Otwartość i transparentność.
- Autentyczność i zaufanie.
- Suwerenność cyfrowa i samostanowienie.
- Wolny dostęp do rynku i promowanie europejskich wartości.
- Modułowość i interoperacyjność.
- Przyjazność dla użytkownika.

Spośród powyższych, poza kluczową kwestią zgodności z unijnym prawem przetwarzania danych, w oczy rzuca się często powtarzane w kontekście Gaia-X hasło digital sovereignty lub data sovereignty, rozumiane jako uprawnienie do podejmowania decyzji dotyczących struktury, budowy i zarządzania procesami cyfrowymi, infrastrukturami i przepływem danych. Natomiast postulaty otwartości, interoperacyjności, transparentności dają nadzieję m.in. na zapewnienie firmom i podmiotom korzystającym z oferowanych w ramach tej inicjatywy usług chmurowych możliwość łatwej zmiany dostawców.

Mówi się również o tym, że stworzenie europejskiej platformy chmurowej będzie wymagać ustanowienia w tym celu centralnej organizacji na poziomie unijnym, która położyłaby ekonomiczne, organizacyjne i techniczne podstawy pod europejską infrastrukturę danych.

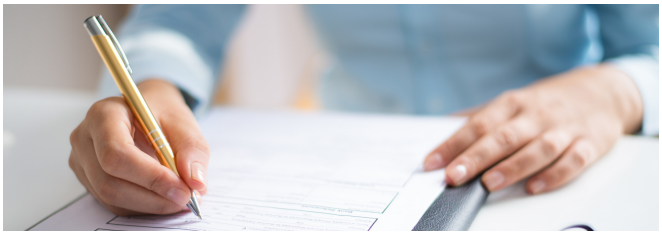
Niemcy i Francja poinformowały, że do końca roku uruchomią platformę chmurową Gaia-X. Pierwsze usługi świadczone publicznie mają być dostępne w 2021 r.

Inicjatywa wydaje się być wspaniała, powstają tylko pytania, czy nie za późno, dlaczego dopiero teraz, oraz obawa, aby wdrożenie europejskiej chmury nie rozbiło się o rozbieżne wizje i zagadnienia polityczne w ramach UE.

Zamówienia publiczne w tarczy 4.0

Rada Ministrów przyjęła w dniu 22 maja 2020 r. projekt ustawy o dopłatach do oprocentowania kredytów bankowych udzielanych na zapewnienie płynności finansowej przedsiębiorcom dotkniętym skutkami COVID-19 oraz o zmianie niektórych innych ustaw. Projekt został uchwalony przez Sejm, a prace nad nim, na moment przygotowania artykułu, prowadzone są przez Senat[1].

Ustawa przewiduje dalsze bardzo istotne zmiany w prawie zamówień publicznych w czasie trwania pandemii COVID-19, korzystne przede wszystkim dla przedsiębiorców (wykonawców) działających na rynku zamówień publicznych. W tym zakresie zmienione zostaną przepisy Ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych.



1. Obowiązek dokonania zmiany umowy o zamówienie publiczne.
Ustawodawca nadał nową treść art. 15r ust. 4. Nowy przepis stanowi, że w wypadku stwierdzenia przez zamawiającego, iż okoliczności związane z wystąpieniem COVID-19 **wpływają** na należyte wykonanie umowy, dokonuje on w uzgodnieniu z wykonawcą zmiany umowy, stosując jako podstawę prawną art. 144 ust. 1 pkt. 3 Ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (PZP). Brzmienie przepisu wskazuje, że wykonawca może w takich okolicznościach mieć roszczenie o zmianę umowy. W pozostałym zakresie przepis się nie zmienia, tj. w wypadku stwierdzenia, że okoliczności związane z wystąpieniem COVID-19 jedynie **mogą wpłynąć** (potencjalnie) na należyte wykonanie umowy, zamawiający może, ale nie musi dokonać zmiany umowy. Warto też zauważyć, że to zamawiający decyduje (stwierdza), czy zaszły okoliczności uprawniające do podjęcia rozmów w sprawie zmiany umowy. Jest to zabezpieczenie przed nadużywaniem nowych przepisów przez wykonawców.

2. Zakaz potrącania kar umownych z wynagrodzenia wykonawcy i zakaz zaspokojenia z zabezpieczenia należytego wykonania umowy.
Wprowadzony zostanie nowy przepis art. 15r (1), z którego wynika zakaz potrącania kar umownych zastrzeżonych na wypadek niewykonania lub nienależytego wykonania umowy z wynagrodzenia wykonawcy lub z innych jego wierzytelności, a także zakaz zaspokojenia tych kar z zabezpieczenia należytego wykonania umowy w okresie ogłoszenia stanu zagrożenia epidemicznego albo stanu epidemii w związku z COVID-19 i przez 90 dni od dnia odwołania stanu, który obowiązywał jako ostatni, o ile zdarzenie, w związku z którym zastrzeżono tę karę, nastąpiło w okresie ogłoszenia stanu zagrożenia epidemicznego albo stanu epidemii (bieg terminu przedawnienia roszczenia zamawiającego oraz terminu ważności zabezpieczenia należytego wykonania umowy nie rozpoczyna się, a rozpoczęty ulega zawieszeniu). Oznacza to znaczną ulgę dla wykonawców, którzy napotkali problemy w realizacji umowy związane z pandemią.

Powyższe nie oznacza jednak, że zamawiający stracą możliwość dochodzenia swoich roszczeń bądź zabezpieczenie należytego wykonania umowy. Ustawa stanowi bowiem również, że w okresie ogłoszenia stanu zagrożenia epidemicznego albo stanu epidemii w związku z COVID-19 i przez 90 dni od dnia odwołania stanu, który obowiązywał jako ostatni, bieg terminu przedawnienia roszczeń zamawiającego oraz terminu ważności zabezpieczenia należytego wykonania umowy nie rozpoczyna się, a rozpoczęty ulega zawieszeniu. Upływ tych terminów może nastąpić nie wcześniej niż po 120 dniach od odwołania tego ze stanów, który obowiązywał jako ostatni.

3. Wadium tylko fakultatywnie.
Zgodnie z proponowanym nowym przepisem art. 15va zniesiony zostanie obowiązek żądania wadium przez zamawiających w postępowaniach o wartości równej progom unijnym i wyższej od nich.

[1] Stan na 18 czerwca 2020 r.

4. Obowiązkowe dokonywanie płatności wynagrodzenia w częściach lub udzielania zaliczek przez zamawiających.
Zgodnie z proponowanym nowym przepisem art. 15vb w wypadku umów w sprawie zamówienia publicznego zawieranych na okres dłuższy niż 12 miesięcy zamawiający mają obowiązek przewidzieć zapłatę wynagrodzenia w częściach po wykonaniu danego etapu umowy lub udzielać zaliczki na poczet realizacji zamówienia. Zamawiający będzie miał obowiązek określić w projekcie umowy z wykonawcą procent wynagrodzenia wypłacanego za wykonanie poszczególnych jej części, przy czym wartość ostatniej części wynagrodzenia nie będzie mogła wynosić więcej niż 50% wysokości wynagrodzenia należnego wykonawcy, a zaliczka nie może być mniejsza niż 5% wysokości tego wynagrodzenia. Obowiązek płatności wynagrodzenia w częściach i udzielania zaliczek nie będzie dotyczył zamówień w dziedzinach obronności i bezpieczeństwa.

5. Zmniejszenie maksymalnej wartości zabezpieczenia należytego wykonania umowy do 5%, częściowy zwrot zabezpieczenia.
Przepis art. 15vb przewiduje, że zabezpieczenie należytego wykonania umowy będzie można ustalić na poziomie maksymalnym 5% ceny całkowitej podanej w ofercie albo maksymalnej wartości nominalnej zobowiązania zamawiającego wynikającego z umowy. Ustalenie zabezpieczenia na poziomie do 10% będzie dalej dopuszczalne, ale jedynie wyjątkowo, jeżeli jest to uzasadnione przedmiotem zamówienia lub wystąpieniem ryzyka związanego z jego realizacją, co zamawiający ma obowiązek wskazać i opisać w specyfikacji istotnych warunków zamówienia. Dodatkowo projekt ustawy uprawnia zamawiającego do częściowego zwrotu zabezpieczenia należytego wykonania umowy po wykonaniu części zamówienia, jeżeli przewidział taką możliwość w specyfikacji istotnych warunków zamówienia.

6. Wszczęcie postępowania w trybie przetargu nieograniczonego będzie następować poprzez zamieszczenie ogłoszenia o zamówieniu na stronie internetowej zamawiającego.
Z ustawy PZP usunięty zostanie obowiązek zamieszczania ogłoszenia o zamówieniu w miejscu publicznie dostępnym w swojej siedzibie.

7. Ponadto w projekcie ustawy przewidziano wyłączenie stosowania ustawy PZP do umów o zarządzanie PPK (Pracownicze Plany Kapitałowe) oraz umów o prowadzenie PPK, jeżeli wartość zamówienia jest mniejsza niż progi unijne.
Warto podkreślić, że zgodnie z projektowanymi przepisami przejściowymi do postępowań o udzielenie zamówienia publicznego, wszczętych i niezakończonych przed dniem wejścia w życie nowych przepisów art. 15va (wadium) i art. 15vb (wynagrodzenie częściowe, zaliczki, zabezpieczenie), stosuje się przepisy dotychczasowe. Podobnie przepisy dotychczasowe stosuje się do umów w sprawie zamówienia publicznego zawartych:

- przed dniem wejścia w życie art. 15vb;
- nie wcześniej niż z dniem wejścia w życie art. 15vb, w następstwie postępowań o udzielenie zamówienia wszczętych przed dniem wejścia w życie tego przepisu.

Oznacza to, że nowe rozwiązania dotyczące wadium i umów o zamówienie publiczne nie będą miały mocy wstecznej.

Jednocześnie warto podkreślić, że zmiany opisane w pkt. 3, 4 i 5 powyżej są przewidziane również w nowej Ustawie z dnia 11 września 2019 r. – Prawo zamówień publicznych, która wejdzie w życie z dniem 1 stycznia 2021 r.

Tarcza 4.0 przeciwko potrącaniu kar w PZP

Potrzeba wsparcia dla sektora prywatnego

Epidemię COVID-19 odczuła zdecydowana większość przedsiębiorców. Wiele firm zmuszonych było nawet do zawieszenia bądź istotnego ograniczenia swojej działalności. Inne z niepewnością spoglądały w przyszłość (i nadal to robią). Powyższe okoliczności dotyczą także realizowanych w trakcie epidemii zamówień publicznych, w tym dotyczących sektora IT.

Chociaż przedstawiciele branży informatycznej dużą część swojej pracy mogą z powodzeniem wykonywać z domu, to jednak nie wszystkie czynności da się przeprowadzić w ten sposób. W przypadku wdrożenia oprogramowania prawidłowe wykonanie prac może wymagać podjęcia pewnych czynności w siedzibie zamawiającego, co z uwagi na pandemię, może być co najmniej utrudnione. W przypadku dostawy sprzętu IT na rynku wciąż dostrzegalne są braki niektórych produktów (np. laptopów, które spełniają specyficzne wymagania). Ponadto wymóg bardzo szybkiego przejścia na pracę zdalną spowodował pewne trudności związane z organizacją działań, a także, w wyniku masowości całego zjawiska, znacząco wpłynął na przepustowość sieci internetowych.

Wszystkie te czynniki mogą prowadzić do opóźnień w realizacji zamówień, a w konsekwencji – do naliczenia przez zamawiających kar umownych z tytułu niewykonania lub nienależytego wykonania umowy. W takich sytuacjach, z uwagi na wysokie koszty prowadzenia sporów sądowych oraz ich przewlekłość, wielu zamawiających decyduje się potrącić naliczone kary umowne z wynagrodzenia dla wykonawcy. Nowelizacja przepisów projektowana przez ustawodawcę ma temu zapobiec.

Projekt nowelizacji

Projektowany przepis Tarczy 4.0[1] brzmi następująco *„art. 15r1 1. W okresie ogłoszenia stanu zagrożenia epidemicznego albo stanu epidemii w związku z COVID-19, i przez 90 dni od dnia odwołania stanu, który obowiązywał jako ostatni, zamawiający nie może potrącić kary umownej zastrzeżonej na wypadek niewykonania lub nienależytego wykonania umowy, o której mowa w art. 15r ust. 1, z wynagrodzenia wykonawcy lub z innych jego wierzytelności, a także nie może dochodzić zaspokojenia z zabezpieczenia należytego wykonania tej umowy, o ile zdarzenie, w związku z którym zastrzeżono tę karę, nastąpiło w okresie ogłoszenia stanu zagrożenia epidemicznego albo stanu epidemii”*. Sejm w dniu 4 czerwca 2020 r. uchwalił ustawę, która na moment przygotowywania niniejszego artykułu jest przedmiotem prac Senatu.

W uzasadnieniu projektu[2] wskazano, że „proponowane rozwiązanie przyczyni się do ograniczenia obciążeń finansowych wykonawców w okresie walki ze skutkami epidemii COVID-19, a w konsekwencji do zwiększenia ich zasobów finansowych”.

Rzeczywiście wprowadzenie powyższego przepisu doprowadzi do ograniczenia możliwości potrącania kar umownych z wynagrodzenia wykonawcy lub zabezpieczenia należytego wykonania umowy, co może poprawić płynność finansową niektórych wykonawców. Nie powinno to spowodować pokrzywdzenia zamawiających, którzy będą mogli dochodzić swoich roszczeń przed sądem. Należy jednak pamiętać, że ograniczenia w tym zakresie odnoszą się do umów zawartych w reżimie Prawa zamówień publicznych. Nie mają więc zastosowania w przypadku umów zawartych na rynku prywatnym.

Ponadto zakaz naliczania kar umownych nie ma charakteru absolutnego i jest ograniczony przez dwa czynniki. Pierwszy czynnik ma charakter przedmiotowy – zakaz dotyczy jedynie kar umownych naliczonych w wyniku zdarzenia mającego miejsce w „okresie ogłoszenia stanu zagrożenia epidemicznego albo stanu epidemii”. Pewną wątpliwość może budzić to, czy zdarzenie uzasadniające naliczenie kar umownych ma być spowodowane epidemią COVID-19, czy też wystar-czy, aby wystąpiło w czasie określonym w ustawie (bo nie wszystkie błędy w realizacji kontraktów w czasie epidemii COVID-19 muszą być jej skutkiem). Wydaje się, że pomiędzy zdarzeniem a epidemią powinien zachodzić związek przyczynowy, chociaż może on być pośredni.

Drugi czynnik ma charakter czasowy – zakaz obowiązuje jedynie „w okresie ogłoszenia stanu zagrożenia epidemicznego albo stanu epidemii w związku z COVID-19, i przez 90 dni od dnia odwołania stanu, który obowiązywał jako ostatni”. Po upływie tego okresu potrącenie kar umownych będzie możliwe w dotychczasowym zakresie. Nie można wykluczyć, że w niektórych przypadkach zamawiający mogą celowo zwlekać z wypłatą wynagrodzenia wykonawcy, aby potrącić kary umowne po upływie powyższego okresu. Ponadto trudno obecnie ustalić, czy okres 90 dni od daty zakończenia stanu epidemii lub ustania zagrożenia epidemicznego jest wystarczający dla ochrony wykonawców. Będzie można to określić dopiero w przyszłości, w zależności od czasu trwania epidemii i jej finalnego wpływu na gospodarkę.

Niezależnie od pewnych wątpliwości powyższą propozycję legislacyjną należy potraktować jako działanie, które może przyczynić się do poprawy płynności finansowej niektórych wykonawców. Wypłata wynagrodzenia za zrealizowaną umowę, chociażby w części, jest kluczowa dla możliwości zapłaty za nakłady i zobowiązania powstałe w wyniku wywiązywania się z niej. Jednocześnie nie dochodzi do pokrzywdzenia zamawiających, którzy nadal będą uprawnieni do dochodzenia swoich roszczeń. Wydaje się więc, że zaproponowane rozwiązanie stanowi kompromis pomiędzy interesem wykonawców, którzy w obecnej sytuacji mogą mieć poważne trudności z wykonywaniem umów, a interesem zamawiających, którzy oczekują należytego wywiązania się z umowy. Rozwiązanie to jest właściwe także ze względów słusznościowych, epidemia stanowi bowiem sytuację zaskakującą i groźną dla całego obrotu.

[1] Art. 58 pkt. 12) Tarczy 4.0 - rządowego projektu ustawy o dopłatach do oprocentowania kredytów bankowych udzielanych na zapewnienie płynności finansowej przedsiębiorcom dotkniętym skutkami COVID-19 oraz o zmianie niektórych innych ustaw.

[2] Uzasadnienie do rządowego projektu ustawy o dopłatach do oprocentowania kredytów bankowych udzielanych na zapewnienie płynności finansowej przedsiębiorcom dotkniętym skutkami COVID-19 oraz o zmianie niektórych innych ustaw, s. 61; uzasadnienie dostępne jest pod adresem https://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=382.

Rebus sic stantibus w umowach IT

Klauzula *rebus sic stantibus* (z łac. skoro sprawy przybrały taki obrót) została wprowadzona do polskiego kodeksu cywilnego (dalej: k.c.) w 1990 r. wraz z wejściem w życie art. 3571. Stanowi ona wyjątek od ogólnej zasady pacta sunt servanda i daje sądom powszechnym kompetencję do ingerencji w zawarte umowy na wypadek zaistnienia „nadzwyczajnej zmiany stosunków". Czy wobec tego pandemia COVID-19 umożliwia powoływanie się przed sądem na klauzulę *rebus sic stantibus*?

Jeszcze do niedawna klauzula *rebus sic stantibus* stosowana była w praktyce najczęściej do umów kredytu zaciągniętych w walutach obcych. W tym wypadku „nadzwyczajna zmiana stosunków" odnosiła się do dużych wahań kursów walut. Nie mieliśmy bowiem w Polsce od 1990 r. do czynienia z sytuacją porównywalną do tej spowodowanej wirusem SARS-CoV-2. Pojawiają się w związku z tym uzasadnione pytania o możliwość zastosowania *rebus sic stantibus* do umów realizowanych w warunkach pandemii.

Podstawową przesłanką powołania się na klauzulę *rebus sic stantibus* jest wystąpienie „nadzwyczajnej zmiany stosunków" rozumianej jako rzadko zachodzące, niezwykłe, wyjątkowe, normalnie niespotykane zdarzenie, które może mieć tło przyrodnicze lub społeczne[1]. W orzecznictwie Sądu Najwyższego epidemia wskazywana jest wprost jako powszechnie występujące zdarzenie mogące powodować nadzwyczajną zmianę stosunków[2]. Zmiana ta może objawiać się występowaniem zjawisk takich jak kryzys gospodarczy, gwałtowna zmiana poziomu cen czy długotrwały paraliż ż środków transportu[3]. Wydaje się, że z taką właśnie sytuacją mamy obecnie do czynienia. Co więcej, nadzwyczajna zmiana stosunków musi być nieprzewidywalna, czyli niemożliwa do przewidzenia przez strony umowy w momencie jej zawarcia przy dochowaniu należytej staranności. W tej kwestii wątpliwości może budzić ustalenie, od którego momentu wystąpienie pandemii COVID-19 na terenie Polski można było przewidzieć. Czy za moment ten należy przyjąć zdiagnozowanie pierwszego przypadku koronawirusa poza terenem Chin (13 stycznia), czy na przykład wystąpienie choroby na terytorium Unii Europejskiej (24 stycznia)? O ile odpowiedź na to pytanie jest trudna, o tyle można stwierdzić, że z pewnością wystąpienie nadzwyczajnej zmiany stosunków stało się w jakimś stopniu przewidywalne, zanim zdiagnozowano w Polsce tzw. pacjenta zero.

Aby zastosować klauzulę *rebus sic stantibus*, dalsza realizacja umowy wskutek wystąpienia nadzwyczajnej zmiany okoliczności musi się dodatkowo wiązać z nadmierną trudnością dla stron lub grozić którejkolwiek z nich rażącą stratą. Nadmierną trudność w umowach IT może na przykład stanowić konieczność dostarczenia komponentów lub urządzeń, które wskutek pandemii stały się trudno dostępne ze względu na wstrzymanie pracy fabryk, czy obowiązek zapewnienia udziału w realizacji zlecenia oddelegowanego personelu, podczas gdy znaczna część pracowników wykonawcy jest chora na COVID-19 lub przebywa w obowiązkowej kwarantannie. Znaczący wzrost cen określonych komponentów lub urządzeń oraz kosztów usług podwykonawców w związku z wystąpieniem epidemii może z kolei grozić jednej ze stron poniesieniem rażącej straty. Powyższe okoliczności muszą zostać powiązane z wystąpieniem nadzwyczajnej zmiany okoliczności – powołując się na klauzulę *rebus sic stantibus*, należy jasno wykazać, że wzrost cen jest spowodowany pandemią COVID-19 (np. poprzez konieczność zapewnienia dodatkowych środków ochrony osobistej, czy ograniczenia w transporcie), a nie innymi zdarzeniami (na przykład powtarzającym się, okresowym wzrostem cen).

[1] Wyrok Sądu Apelacyjnego w Katowicach z dnia 7 grudnia 2018 r., sygn. I ACa 644/18.
[2] Wyrok Sądu Najwyższego z dnia 8 marca 2018 r., sygn. II CSK 303/17.
[3] Wyrok Sądu Apelacyjnego w Katowicach z dnia 7 grudnia 2018 r., sygn. I ACa 644/18.

Do ingerencji w umowę na podstawie art. 3571 k.c. upoważniony jest wyłącznie sąd, który może zmienić sposób jej wykonania czy wysokość wynagrodzenia, a nawet orzec o jej rozwiązaniu, przy czym rozwiązanie umowy powinno następować jedynie w sytuacjach wyjątkowych[4], a sąd nie jest przy orzekaniu związany żądaniem osoby powołującej się na klauzulę *rebus sic stantibus.*

Warto wskazać, że w przypadku umów zawartych w trybie postępowania o udzielenie zamówienia publicznego nie należy – co do zasady – wykluczać możliwości powoływania się na art. 3571 k.c. W orzecznictwie dominuje pogląd, że art. 144 ust. 1 Ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych nie pozbawia możliwości sądowej zmiany takiej umowy w przypadku zastosowania klauzuli *rebus sic stantibus*. Należy mieć jednak na względzie, że przepisy szczególne tzw. ustawy antycovidowej[5] dopuszczają możliwość zmiany umowy zawartej w reżimie zamówień publicznych z uwagi na okoliczności związane z wystąpieniem COVID-19 – szersze omówienie tych kwestii znajduje się w artykule „Zamówienia publiczne w tarczy 4.0". Wydaje się zatem, że z uwagi na szczególny charakter klauzuli *rebus sic stantibus*, która powinna być stosowana jedynie w wyjątkowych przypadkach, podmioty sektora publicznego powinny w pierwszej kolejności korzystać z uprawnień do zmiany umowy przyznanych im przez przepisy szczególne, a dopiero w razie braku możliwości osiągnięcia porozumienia z wykonawcą powoływać się na art. 3571 k.c.

Pandemia COVID-19 może stanowić uzasadnienie dla zastosowania przez sąd klauzuli *rebus sic stantibus* dla kontraktów IT. Należy jednak pamiętać, że podmiot powołujący się na zaistnienie nadzwyczajnych okoliczności powinien wykazać powstanie nadmiernych trudności lub groźby poniesienia rażącej straty w związku z realizacją umowy, wywołanych rozprzestrzenianiem się wirusa SARS-CoV-2. Warto również przewidzieć odpowiednie postanowienia zabezpieczające interesy stron na wypadek okoliczności wywołanych COVID-19 w umowach zawieranych obecnie, ponieważ możliwość powoływania się przy ich realizacji na klauzulę *rebus sic stantibus* będzie bardzo utrudniona[6].

[4] Wyrok Sądu Najwyższego z dnia 8 marca 2018 r., sygn. II CSK 303/17.
[5] Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. 2020, poz. 374 z późn. zm.).
[6] Por. wyrok Sądu Najwyższego z dnia 10 maja 2006 r., sygn. III CK 336/05.

ARTYKUŁY

#czasopisma

"Organizacja wewnętrznych struktur" - artykuł autorstwa Agnieszki Wachowskiej i Joanny Jastrząb ukazał się w majowym numerze "IT Professional".

„Wykonanie zastępcze w umowach IT” - artykuł autorstwa Agnieszki Wachowskiej i Karoliny Grocheckiej-Goljan ukaże się w lipcowym numerze „IT Professional”.

„IP Box w branży IT” - artykuł autorstwa Agnieszki Wachowskiej i Joanny Jastrząb ukaże się w lipcowym numerze „IT Professional”.

„Analiza potrzeb i wymagań w nowym PZP” - artykuł autorstwa Tomasza Krzyżanowskiego i Wojciecha Karwackiego ukazał się w czerwcowym dodatku do wydania czasopisma „Zamówienia Publiczne Doradca”.

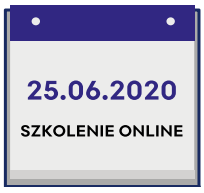
„Jawność otwarcia ofert elektronicznych transmitowanego online” - artykuł autorstwa Wojciecha Karwackiego ukazał się w majowym wydaniu czasopisma „Zamówienia Publiczne Doradca”.

„Komunikacja zamawiającego z wykonawcami w nowym Pzp” - artykuł autorstwa Tomasza Krzyżanowskiego ukazał się w majowym dodatku do wydania czasopisma „Zamówienia Publiczne Doradca”.

03/2020 CZERWIEC

NADCHODZĄCE WYDARZENIA

#szkolenia #konferencje #warsztaty



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

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

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 >>

"Umowy wdrożeniowe na systemy IT"

Prelekcja "Wdrożenie IT – jak przygotować dobrą umowę?"
- r. pr. Agnieszka Wachowska

Prelekcja "Odpowiedzialność dostawców usług IT za nienależyte wykonywanie umowy" - adw. Xawery Konarski

Podsumowanie: "Jak zrealizować wdrożenie IT zgodnie z budżetem, harmonogramem i przyjętymi wymaganiami – checklista Dostawców i Zamawiających"
- adw. Xawery Konarski, r. pr. Agnieszka Wachowska

Więcej informacji >>

"Internet Rzeczy (problematyka prawna)"

adw. Xawery Konarski

Szczegóły wkrótce

"Wykonanie umów ICT i COVID-19"

adw. Xawery Konarski, r. pr. Agnieszka Wachowska

Szczegóły wkrótce

"Umowy na utrzymanie, serwis i rozwój systemów IT - najlepsze praktyki i sporne kwestie"

r. pr. Agnieszka Wachowska

Więcej informacji >>

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

adw. Xawery Konarski, r. pr. Agnieszka Wachowska

Więcej informacji >>

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
Stażysta
aleksander.elmerych@traple.pl

Michał Kalinowski
Stażysta
michal.kalinowski@traple.pl

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