NR 5 - SIERPIEŃ 2020

NEWSLETTER

IT-TECH

W NUMERZE:

Traple
Konarski
Podrecki
& Wspólnicy

TKP

Rozpoczęły się publiczne konsultacje projektu ustawy Prawo komunikacji elektronicznej (PKE)

Rozpoczęły się publiczne konsultacje projektu ustawy Prawo komunikacji elektronicznej (PKE) i ustawy ją wprowadzającej. PKE będzie przede wszystkim stanowić wdrożenie unijnej dyrektywy Europejski kodeks łączności elektronicznej z dnia 11 grudnia 2018 r.[1]. **Państwa członkowskie mają obowiązek wdrożyć ją do 21 grudnia 2020r.**

Polski ustawodawca zdecydował się na kompleksowe podejście – przygotowywany przez Ministerstwo Cyfryzacji od początku roku i przekazany właśnie do publicznych konsultacji projekt **PKE ma w całości zastąpić dotychczasową ustawę Prawo telekomunikacyjne[2]**. Zakres regulacji PKE jest nawet szerszy niż dotychczasowej ustawy Prawo telekomunikacyjne (tj. rynek telekomunikacyjny), gdyż PKE w sposób kompleksowy regulować ma cały rynek usług łączności elektronicznej.

Oznacza to, że jedną z podstawowych konsekwencji dla rynku jest objęcie częścią obowiązków dotychczas spoczywających wyłącznie na przedsiębiorcach telekomunikacyjnych również dostawców tzw. usług OTT (over-the-top) pozwalających na komunikację między indywidualnymi osobami poprzez wiadomości tekstowe lub głosowo (VoIP), także poprzez pocztę elektroniczną, czyli bez wykorzystania numerów z krajowego czy międzynarodowego planu numeracji. Nowe wymogi wobec dostawców takich usług (które PKE nazywa usługami komunikacji interpersonalnej) dotyczą obowiązków informacyjnych wobec konsumentów, obowiązków związanych z bezpieczeństwem usług i przeciwdziałaniem zagrożeniom, obowiązków zapewnienia interoperacyjności usług i in.

W obszarze praw użytkowników końcowych pojawiają się istotne zmiany, co ma wyraz przede wszystkim w **obowiązkach informacyjnych dostawców usług komunikacji elektronicznej** (czyli telekomunikacyjnych, ale też niewykorzystujących numerów) **wobec konsumentów**, w tym obowiązku dostarczenia konsumentowi przed zawarciem umowy informacji przedumownych na trwałym nośniku. Zmiany dotyczą także **zasad przedterminowego rozwiązywania umów i zasad ustalania odszkodowania dostawcy usług z tym związanego**, zmian treści umowy z abonentem, usługi tzw. direct billingu i in.

PKE jest bardzo obszerną i kompleksową regulacją, wiążącą się z ogromnym nakładem pracy legislacyjnej. Większość gruntownych zmian wprowadzanych w PKE wynika bezpośrednio z wymogów dyrektywy Europejski kodeks łączności elektronicznej jednocześnie w zakresie części propozycji postanowień, PKE idzie dalej niż wymaga tego dyrektywa. Takie podejście spotyka się z negatywnym odbiorem ze strony części przedstawicieli rynku telekomunikacyjnego jako nadmiernie ograniczające działalność dostawców usług lub zbyt dla nich dotkliwe . Warto przy tym zaznaczyć, że w odniesieniu do przepisów dotyczących praw użytkowników końcowych, co do których dyrektywa wyraźnie wprowadza zasadę maksymalnej harmonizacji (czyli ustawodawca krajowy nie może wprowadzać przepi-sów ani bardziej, ani mniej restrykcyjnych w stosunku do dyrektywy), takie podejście - zwiększające obowiązki dostaw-ców usług telekomunikacyjnych - w szczególności nie powin-no mieć miejsca. Tymczasem, np. w odniesieniu do przepisów dot. usługi direct billingu, polegającej na doliczaniu do rachunku abonenta opłat za inne usługi, którą w projekcie PKE nazwano usługą dodatkowego obciążania rachunku, art. 308 PKE.

Z prowadzonych dotychczas konsultacji wcześniejszych wersji projektu PKE z organizacjami branżowymi, w tym PIIT, wynika, że uczestnicy rynku obawiają się też problemów wynikających z konieczności dostosowania istniejących umów z abonentami do nowych przepisów, gdyż projekt ustawy wprowadzającej obecnie przewiduje przepisy przejściowe oceniane przez wielu przedsiębiorców telekomunikacyjnych jako niekorzystne i mogące powodować straty po ich stronie, wynikające np. z konieczności skrócenia okresu niektórych istniejących umów.

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej.
[2] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne.

Obawy są wyrażane również w związku z opublikowaniem niedawno (29 czerwca 2020 r.), na podstawie obowiązujących przepisów Prawa telekomunikacyjnego, nowego rozporządzenia Ministra Cyfryzacji w sprawie bezpieczeństwa sieci i usług, które ma wejść w życie 29 grudnia 2020 r. Przedsiębiorcy pytają bowiem o to, czy nowe rozporządzenie ulegnie zmianie po wprowadzeniu PKE, stawiając pod znakiem zapytania sens wdrażania rozporządzenia w działalności przedsiębiorców.

Obecne konsultacje projektu PKE potrwać mają około miesiąca, zaś Ministerstwo Cyfryzacji nie wyklucza przeprowadzenia więcej niż jednej rundy konsultacji, jeżeli okaże się to konieczne. Wdrożenie nowego PKE powinno nastąpić w terminie do 21.12.2020 r.

Rozporządzenie w sprawie bezpieczeństwa sieci telekomunikacyjnych oraz raport KE z wdrożenia w krajach UE tzw. Toolboxa 5G

29 czerwca 2020 r. opublikowane zostało 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[1]. Jest ono powszechnie nazywane rozporządzeniem o sieci 5G lub rozporządzeniem w sprawie cyberbezpieczeństwa sieci telekomunikacyjnych, a określa środki (o których mowa w art. 175a ust. 1 i art. 175c ust. 1 Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne), jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług.

Wynikające z rozporządzenia obowiązki przedsiębiorcy telekomunikacyjnego dzielą się na takie, które mają zastosowanie do wszystkich przedsiębiorców telekomunikacyjnych, oraz na dodatkowe – mające zastosowanie do dostawców sieci 5G.

Jeżeli chodzi o pierwszą, tj. „ogólną" grupę obowiązków przedsiębiorców telekomunikacyjnych, to dotyczą one m.in.:

- prowadzenia dokumentacji dotyczącej bezpieczeństwa i integralności sieci i usług, a także wykazu tzw. infrastruktury kluczowej, czyli urządzeń i systemów istotnych dla funkcjonowania sieci;
- identyfikacji i oceny prawdopodobieństwa zagrożeń bezpieczeństwa lub integralności sieci lub usług, a także monitorowania funkcjonowania sieci i usług pod kątem naruszeń bezpieczeństwa lub integralności sieci lub usług i minimalizowanie skutków zagrożeń;
- dostępu do kluczowej infrastruktury i przetwarzanych danych, ustanowienia zasad, procedur i zabezpieczeń dostępu, monitorowania i reagowania na próby ich naruszenia;
- identyfikowania zagrożenia dla bezpieczeństwa w związku z zawieranymi umowami wpływającymi na funkcjonowanie sieci lub usług;
- przeprowadzania oceny bezpieczeństwa sieci i usług telekomunikacyjnych co najmniej raz na dwa lata lub w każdym przypadku stwierdzenia naruszenia bezpieczeństwa o istotnym wpływie na funkcjonowanie sieci lub usług, albo w razie wykrycia podatności zwiększającej poziom ryzyka wystąpienia naruszenia bezpieczeństwa.

Natomiast w grupie dodatkowych obowiązków określonych w rozporządzeniu, dotyczących dostawców sieci 5G (rozporządzenie odnosi się do normy ETSI TR 121 915 V.15.0.0[2], zgodnie z którą obecnie przedmiotem definicji i regulacji jest Faza 1 5G), znajdują się trzy wymogi. Dostawcy 5G:

- podlegać mają rekomendacjom, które mogą być wydane przez pełnomocnika ds. cyberbezpieczeństwa działającego na podstawie ustawy o krajowym systemie cyberbezpieczeństwa;
- mają stosować strategię niedopuszczającą do uzależnienia od jednego dostawcy poszczególnych rodzajów elementów infrastruktury;
- mają zapewniać podwyższanie odporności na zakłócenia sieci i usług telekomunikacyjnych.

[1] Zob. http://www.dziennikustaw.gov.pl/D2020000113001.pdf (dostęp: 6.08.2020).
[2] Zob. https://www.etsi.org/deliver/etsi_tr/121900_121999/121915/15.00.00_60/tr_121915v150000p.pdf (dostęp: 6.08.2020).

Rozporządzenie stanowi polską implementację unijnego Toolboxa 5G[3], dokumentu wydanego w styczniu 2020 r. przez NIS Cooperation Group, zawierającego zalecenia skierowane do państw członkowskich w zakresie przeciwdziałania ryzykom dla integralności i bezpieczeństwa sieci nowej generacji w Europie.

Wdrożenie Toolboxa 5G w państwach członkowskich jest monitorowane przez Komisję Europejską (KE) – 24 lipca br. opublikowany został w tym zakresie raport KE[4]. Wynika z niego, że państwa członkowskie podjęły działania implementujące Toolbox – od analizy istniejącej sytuacji, poprzez przeglądy i plany aktualizacji istniejących środków cyberbezpieczeństwa, po zaawansowany etap wdrożenia odpowiednich środków bezpieczeństwa sieci i usług. W wielu krajach prace są jednak na etapie definiowania zakresu i kształtu właściwych środków, spowalnianego dodatkowo koniecznością podjęcia politycznych decyzji.

Polskie rozporządzenie wprowadza w życie część zaleceń Toolboxa, lecz – co bardzo widoczne – robi to w sposób ogólny, elastyczny, pozbawiony konkretów. Co ciekawe, zwłaszcza w kontekście panujących obecnie na arenie międzynarodowej wątpliwości i obaw o bezpieczeństwo strategiczne, dotyczących wykorzystywania urządzeń sieciowych chińskiego Huawei, rozporządzenie nie wprowadza ani nie daje podstaw do wprowadzenia żadnych ograniczeń dotyczących konkretnych dostawców infrastruktury 5G, pomimo że Toolbox zaleca ocenę i wykluczenie ryzykownych dostawców urządzeń w przypadku najważniejszych elementów infrastruktury.

Polskie rozporządzenie wejdzie w życie 29 grudnia 2020 r.

[3] Zob. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468 (dostęp: 6.08.2020).
[4] Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity July 2020, https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity (dostęp: 6.08.2020).

Europejskie programy certyfikacji cyberbezpieczeństwa – chmura i produkty ICT

Ponad rok temu – 27 czerwca 2019 r. – weszło w życie unijne rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881[1], znane szerzej jako **akt o cyberbezpieczeństwie**. Z jednej strony jego rolą było wzmocnienie mandatu unijnej agencji ds. cyberbezpieczeństwa (ENISA), a z drugiej – **ustanowienie europejskich ram certyfikacji produktów, usług i procesów ICT**. Więcej o akcie o cyberbezpieczeństwie pisaliśmy na blogu – tekst dostępny jest pod tym linkiem.

Wspomniane ramy certyfikacji ustanowione w akcie o cyberbezpieczeństwie mają być podstawą do opracowania i przyjęcia konkretnych programów certyfikacji dla poszczególnych produktów, usług i procesów. Warto przy tym wyraźnie podkreślić, że programy certyfikacji będą miały charakter unijny, co oznacza zwłaszcza, że **zapewnią wdrożenie unijnych standardów certyfikacji i stworzenie jednolitych zasad uznawania, że dane produkty czy usługi i spełniają ustalone wymogi. Tym samym ułatwią działanie dostawców produktów i usług ICT na wspólnym rynku.**

W ostatnich miesiącach **działania w zakresie certyfikacji zostały zintensyfikowane** – ENISA poinformowała o postępach w pracach nad **dwoma programami** certyfikacji, tj.:

- programie certyfikacji cyberbezpieczeństwa produktów ICT opartym na Common Criteria;
- programie certyfikacji usług chmurowych.

EUCC Scheme

W zakresie pierwszego z programów certyfikacji ENISA opublikowała projekt, który podlegał konsultacjom do końca lipca (link). Program, zatytułowany EUCC scheme (Common Criteria based European candidate cybersecurity certification scheme), zajmuje się certyfikacją cyberbezpieczeństwa produktów ICT na podstawie Common Criteria, wspólnej metodologii oceny bezpieczeństwa informatycznego (Common Methodology for Information Technology Security Evaluation) oraz właściwych norm, odpowiednio: ISO/IEC 15408 i ISO/IEC 18045.

Program ten docelowo ma zastąpić obecnie obowiązujące porozumienie SOG-IS MRA, tj. – w uproszczeniu – umowę zawartą między organizacjami rządowymi w sprawie wspólnych kryteriów oceny bezpieczeństwa technologii informacyjnych (Mutual Recognition Agreement – MRA), zatwierdzoną przez Senior Official Group Information System Security (SOG-IS). Polska również uczestniczy w tej umowie – uczestnikiem porozumienia jest Naukowa i Akademicka Sieć Komputerowa (NASK).

Program ma być skierowany do różnego rodzaju produktów:

- zarówno oprogramowania, jak i urządzeń;
- zarówno produktów poświęconych bezpieczeństwu (np. zapory ogniowe, urządzenia szyfrujące, bramy, urządzenia do składania podpisu elektronicznego, środki identyfikacji, takie jak paszporty), jak i wszelkich produktów ICT zawierających funkcje bezpieczeństwa (tj. routerów, smartfonów, kart bankowych, urządzeń medycznych, tachografów do samochodów ciężarowych).

ENISA wskazuje, że beneficjentami programu będą:

- producenci lub dostawcy, którzy chcą ocenić jakość bezpieczeństwa swoich produktów ICT w drodze certyfikacji przez stronę trzecią;
- organy regulacyjne, które w swoich rozporządzeniach i dyrektywach chcą ustanowić wymogi w zakresie bezpieczeństwa i gwarancji dla produktów ICT;
- użytkownicy końcowi, którzy pragną stosować się do przepisów lub uzyskać dowody bezpieczeństwa produktów ICT chroniących wrażliwe aktywa tych użytkowników.

[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).

Co ważne, **program zakłada dwa poziomy zaufania: istotny i wysoki**. Nie uwzględniono w nim poziomu podstawowego, który według aktu o cyberbezpieczeństwie zakładałby deklarację zgodności producenta w zakresie swoich produktów – potwierdzenie spełnienia przez nie wymogów bezpieczeństwa bez udziału strony trzeciej.

Projekt wprowadza również propozycje dotyczące monitorowania certyfikowanych produktów w celu zapewnienia nad nimi nadzoru. W tym zakresie użytkownicy końcowi powinni mieć możliwość zgłaszania podatności wykrytych w toku korzystania z takich produktów, a organy certyfikujące – możliwość żądania odpowiednich informacji dotyczących certyfikowanych produktów.

Co istotne, program certyfikacji nie będzie obowiązkowy, a dobrowolny – zgodnie z ogólną zasadą w tym zakresie przewidzianą przez akt o cyberbezpieczeństwie. W założeniu okres ważności certyfikatu ma wynosić 5 lat i będzie można go przedłużyć, jeśli produkt będzie spełniać stawiane mu wymagania. Ponadto w czasie trwania certyfikatu produkt może zostać wycofany, jeżeli po wykryciu nieprawidłowości nie zostanie on odpowiednio przystosowany.

Dalsze prace nad programami

Biorąc pod uwagę, że proces konsultacji projektu programu EUCC został zakończony, można spodziewać się podjęcia dalszych kroków w celu jego formalnego przyjęcia przez Komisję Europejską. Czas przyjęcia zależeć będzie z pewnością od liczby zgłoszonych sugestii i propozycji zmian.

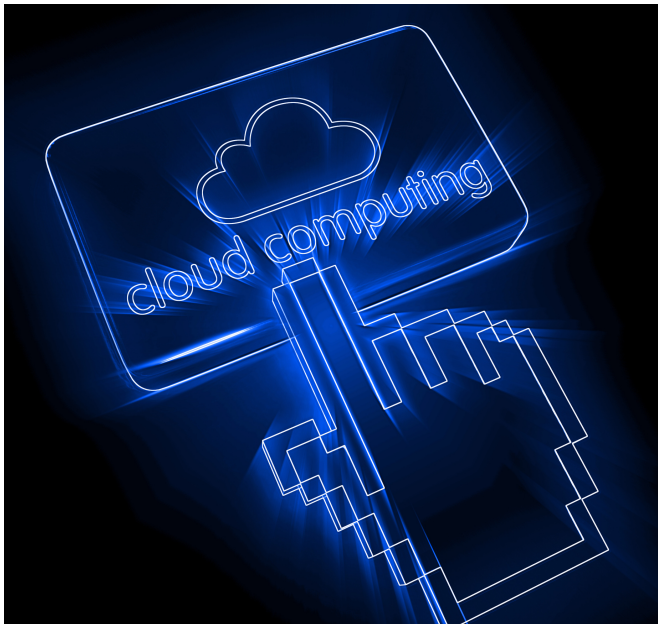
Równocześnie warto śledzić inne prace dotyczące certyfikacji, równolegle prowadzone przez grupy robocze powołane przez ENISA, **zwłaszcza program certyfikacji usług chmurowych**. Prace w tym obszarze również są już na zaawansowanym etapie – w połowie lipca ENISA rozesłała do interesariuszy informację o założeniach certyfikacji cyberbezpieczeństwa usług chmurowych, nad którymi obecnie pracuje, oraz ankietę w tym przedmiocie. Założenia certyfikacji zostały obecnie określone dość ogólnie, a **szczegóły znajdą się w projekcie programu, którego opublikowanie planowane jest na wrzesień br.**

Bezpieczeństwo publicznych chmur obliczeniowych – raport

Chmura obliczeniowa bez wątpienia skorzystała na pandemii COVID-19. Rozwiązanie postrzegane dotąd przez większość firm jako ciekawostka technologiczna i traktowane z pewną dozą nieufności stało się podstawowym narzędziem wykorzystywanym w pracy zdalnej. Badania wskazują, że przedsiębiorstwa, które korzystały z dobrodziejstw cloud computingu jeszcze przed wybuchem pandemii, mogły zapewnić sobie niezakłócone funkcjonowanie podczas lockdownu i tym samym znacznie łagodniej odczuły jego skutki[1]. Mimo zmieniającego się podejścia do chmury obliczeniowej cały czas wiele osób ma obawy dotyczące bezpieczeństwa przechowywania i przetwarzania w ten sposób informacji istotnych z perspektywy prowadzonej działalności – kwestie związane z cyberbezpieczeństwem są wskazywane jako jeden z głównych czynników blokujących podjęcie decyzji o migracji do chmury. Czy słusznie? Pewnych odpowiedzi w tym zakresie dostarcza raport The state of cloud security 2020 opracowany przez firmę Sophos[2].

Raport oparty jest na ankietach przeprowadzonych wśród firm pochodzących z całego świata (w tym także z Polski), korzystających z publicznych chmur obliczeniowych oferowanych przez największych dostawców. Większość ankietowanych stanowiły duże przedsiębiorstwa, zatrudniające ponad 1000 pracowników.

Z raportu wynika, że 70% ankietowanych doświadczyło incydentu bezpieczeństwa związanego z korzystaniem z usług publicznej chmury obliczeniowej w 2019 r. Zauważalna jest przy tym wyraźna tendencja, zgodnie z którą firmy pochodzące z regionu Azji i Pacyfiku doświadczały ataków najczęściej (w Indiach było ich aż 93%). Co ciekawe, firmy znajdujące się w Unii Europejskiej zauważalnie lepiej niż reszta świata radzą sobie z zapobieganiem incydentom bezpieczeństwa w chmurze. Autorzy raportu twierdzą, że jest to zasługa implementacji przepisów RODO, które zapewniają wysoki poziom ochrony informacji. W Polsce jedynie 47% ankietowanych odnotowało w swojej organizacji incydenty bezpieczeństwa w chmurze, co stanowi drugi najniższy wynik zaprezentowany w zestawieniu – niższy odnotowano jedynie we Włoszech.



Raport prezentuje również interesujące wyniki odnoszące się do sposobów, w jakie przestępcy uzyskują dostęp do przechowywanych danych. 66% incydentów było spowodowanych błędną konfiguracją usług i aplikacji, podczas gdy 33% stanowiło rezultat kradzieży informacji o użytkowniku, umożliwiających dostęp do zasobów chmury obliczeniowej (np. identyfikatory, hasła). Szczególnie w zakresie drugiej z wymienionych przyczyn niepokojące są dane przytoczone przez Sophos – zgodnie z przeprowadzonym badaniem aż 91% organizacji przyznawało zbyt duże uprawnienia użytkownikom, podczas gdy 98% nie wdrożyło dwuskładnikowego uwierzytelniania. Powyższe podatności w znacznym stopniu ułatwiają hakerom uzyskanie dostępu do poufnych informacji – przejęcie danych pojedynczego użytkownika stwarza możliwość przeprowadzenia skutecznego ataku na całą organizację. W Polsce natomiast znaczna większość incydentów nie była spowodowana przejęciem konta użytkownika, lecz błędną konfiguracją usług i aplikacji (84%).

Jak wynika z raportu The state of cloud security 2020, bezpieczeństwo usług świadczonych za pośrednictwem publicznej chmury obliczeniowej stanowi realny problem dla

[1] Zob. https://brandsit.pl/chmura-pomogla-firmom-przetrwac-kryzys-czy-praca-zdalna-zwiekszy-popyt-na-cloud-computing/ (dostęp: 5.08.2020).
[2] Raport w pełnej wersji dostępny pod adresem: https://secure2.sophos.com/en-us/content/state-of-cloud-security.aspx (dostęp: 5.08.2020).

firm na całym świecie. Autorzy słusznie wskazują, że przyczyną tego stanu rzeczy może być niewłaściwe zrozumienie roli organizacji w korzystaniu z chmury obliczeniowej i fałszywe przeświadczenie o tym, że za kwestie bezpieczeństwa w całości odpowiada dostawca chmury. O ile w modelu SaaS rzeczywiście to dostawca powinien odpowiednio zabezpieczyć świadczoną usługę (co nie eliminuje całkowicie możliwości wystąpienia incydentów spowodowanych np. przejęciem konta użytkownika), o tyle w modelu PaaS, a w szczególności IaaS, to użytkownik odpowiada za zapewnienie bezpieczeństwa używanych aplikacji i przeprowadzanych procesów.

Warto przy tym pamiętać, że zawierane z dużymi dostawcami umowy nie podlegają co do zasady negocjacjom, a ich postanowienia ograniczają odpowiedzialność dostawców w możliwie największym stopniu. Dlatego też firmy korzystające z usług przetwarzania w chmurze publicznej powinny pamiętać o odpowiednim zabezpieczeniu swoich aplikacji i usług oraz regularnym ich monitorowaniu, a także o wdrożeniu mechanizmów zapobiegających możliwości uzyskania dostępu do kont użytkowników przez nieuprawnione osoby dostępu do kont użytkowników przez nieuprawnione osoby trzecie, np. poprzez ograniczenie przyznawanych uprawnień czy wprowadzenie wieloskładnikowego uwierzytelniania. Niektóre podmioty (np. podlegające nadzorowi KNF[3] czy korzystające z usług chmurowych w ramach inicjatywy WIIP[4]) doczekały się w tym zakresie szczegółowych regulacji – pozostałe muszą natomiast wprowadzić odpowiednie procedury samodzielnie.

Zyskującym na popularności rozwiązaniem jest również zawarcie umowy ubezpieczenia w zakresie ryzyk cybernetycznych. Zainteresowanie tym produktem powoduje, że na rynku pojawiają się nowe oferty, uwzględniające szeroką gamę kosztów: zarówno koszty reakcji na incydent, przywrócenia działania systemu, którego dotyczył incydent, jak i ochrony reputacji i zapłaty kar administracyjnych (np. na gruncie RODO). Więcej pisaliśmy o tym w czerwcowym wydaniu newslettera (artykuł dostępny pod linkiem , str. 8).

[3] Zob. Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej z dnia 23 stycznia 2020 r.
[4] Zob. Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) opublikowane przez Ministerstwo Cyfryzacji, dostępne pod adresem: https://chmura.gov.pl/informacje/scco/ (dostęp: 5.08.2020).

Przyszłość wtórnego rynku oprogramowania w świetle wyroku TSUE dotyczącego e-booków

Prawo zwykle pozostaje o krok w tyle za zmieniającą się rzeczywistością, w tym również za cyfryzacją życia społecznego. Rolą sądów pozostaje wykładnia przepisów w sytuacjach spornych. Jedną z takich sytuacji oceniał niedawno Trybunał Sprawiedliwości UE - w wyroku z dnia 19 grudnia 2019 r. (sprawa C 263/18), stwierdził, że nie można stosować instytucji wyczerpania prawa do e-booków. Pytanie czy, a jeśli tak, to w jakim zakresie wnioski z tego wyroku mają także zastosowanie do obrotu oprogramowaniem, w świetle wcześniej wydanych przez TS UE wyroków np. w sprawie Used Soft?

Wyczerpanie prawa w odniesieniu do oprogramowania i innych utworów

W pierwszej kolejności warto wyjaśnić, że istota wyczerpania prawa stanowi ograniczenie monopolu prawnoautorskiego podmiotu uprawnionego, a dzięki niej, po pierwszym wprowadzeniu do obrotu egzemplarza chronionego utworu autor traci prawo do zezwalania na dalszą odsprzedaż tego egzemplarza, co sprzyja otwartemu rynkowi unijnemu oraz swobodnej wymianie towarów na terytorium UE.

Kwestia ta, istotna z punktu widzenia niniejszej analizy, została uregulowana w dwóch unijnych dyrektywach – 2009/24 – dotyczącej programów komputerowych oraz 2001/29 - dotyczącej utworów innych niż programy komputerowe. Choć przepisy brzmią podobnie, to należy rozpatrywać je odrębnie – mają bowiem zastosowanie do różnych utworów.

TSUE zajmował się tą kwestią dotąd dwukrotnie w stosunku do wyczerpania praw do programów komputerowych. Poniżej przedstawiamy syntetyczne podsumowanie, natomiast szersza analiza tych wyroków znajduje się na naszym blogu.

1. Sprawa UsedSoft (C-128/11) – wyrok z dnia 3 lipca 2012 r.

Producent (Oracle) umożliwiał pobranie z Internetu zakupionego programu na komputer kupującego, udostępniając odpowiednie kody licencyjne dla tego oprogramowania. UsedSoft z kolei odkupował te programy (licencje do tych programów) od klientów Oracle i sprzedawał je następnie innym użytkownikom jako używane programy komputerowe (licencje), udostępniając im również kody licencyjne umożliwiające ponowne pobranie oprogramowania ze stron udostępnianych przez Oracle.

Najważniejsze wnioski:

- Zdaniem Trybunału, skoro licencja na program jest bezterminowa, a licencjodawca pobiera za jej udzielenie jednorazową opłatę, **dochodzi do sytuacji tożsamej ze sprzedażą materialnego nośnika programu komputerowego**.
- Tym samym sprzedaż programu komputerowego na nośniku fizycznym np. w wersji pudełkowej, oraz sprzedaż kopii online, poprzez umożliwienie pobrania programu z serwera, **są do siebie z ekonomicznego punktu widzenia zbliżone**.

[1] Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych
[2] Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym

- Z tych względów, również w przypadku niektórych rodzajów dystrybucji oprogramowania bez fizycznego nośnika, których warunki szczegółowo opisane zostały w wyroku Used Soft może dochodzić do wyczerpania prawa na gruncie art. 4 ust. 2 dyrektywy 2009/24.

2. Sprawa Ranks (C-166/15) –
wyrok z dnia 12 października 2016 r.

Sprawa C-166/15 (Ranks) rozstrzygała problem możliwości odsprzedaży nieoryginalnego egzemplarza nośnika oprogramowania. Uzasadnieniem dla takiego działania było zagubienie lub uszkodzenie oryginalnego nośnika – odsprzedaży podlegała więc kopia zapasowa programu komputerowego (jej wykonanie jest dopuszczalne, gdy taka kopia jest niezbędna do korzystania z programu).

Najważniejsze wnioski:

- Trybunał uznał, że taka odsprzedaż oprogramowania nie jest zgodna z prawem -prawo powielania utworu przysługuje bowiem jedynie uprawnionemu z praw autorskich majątkowych, a możliwość sporządzenia kopii zapasowej jest wyjątkiem od tej zasady.
- Ponadto, samo brzmienie przepisu – obecny art. 4 ust. 2 dyrektywy 2009/24 – mówiąc o wyczerpaniu prawa, wyraźnie odwołuje się do „tej kopii", a więc jedynie oryginalnego nośnika. Wyczerpanie nie dotyczy więc obrotu nieoryginalnym nośnikiem.
- Rozstrzygnięcie TSUE miało charakter pragmatyczny - ciężko bowiem zweryfikować, czy oryginalny nośnik rzeczywiście został zniszczony i odsprzedawana kopia jest jedyną.
- Wyrok potwierdził wnioski płynące z orzeczenia w sprawie UsedSoft, ale wyraźnie rozróżnił wyczerpanie praw w odniesieniu do nośnika oryginalnego i jego kopii – nie ma tu znaczenia fakt, czy nośnik oryginalny przestał istnieć oraz czy nie jest możliwe powielenie ilości egzemplarzy utworu.

Komentowany wyrok – sprawa Tom Kabinet i e-booki (C-263/11) - wyrok z dnia 19 grudnia 2019 r.

Wyrok TSUE dotyczący e-booków mógł być, patrząc z perspektywy powyżej przytoczonych wyroków w sprawie Used Soft i Ranks, pewnego rodzaju zaskoczeniem.

Tom Kabinet zajmowała się skupowaniem używanych e-booków i ich dalszą odsprzedażą. Osoby, od których spółka nabywała e-booki musiały oświadczyć, że nie zachowały ich kopii. Tom Kabinet na nabytych egzemplarzach umieszczała swój znak wodny, aby potwierdzić legalność egzemplarza. Tym samym model biznesowy działania Tom Kabinet był bardzo zbliżony do tego potwierdzonego jako legalny w odniesieniu do programów komputerowych (Used Soft). Nie chodziło bowiem o powielanie (kopiowanie) utworu, a przeniesienie praw do jego cyfrowego, oryginalnego egzemplarza.

Rozpatrując okoliczności prawne sprawy, TSUE uznał że należy zastosować wyłącznie dyrektywę 2001/29, nie uwzględniając dyrektywy 2009/24 dotyczącej programów komputerowych. Zdaniem TSUE, e-book stanowi utwór złożony – składa się z dominującej, twórczej części w postaci treści książki, a w pomocniczej części z programu komputerowego, który umożliwia jej odtworzenie. Zasadnicza wartość tego utworu wynika zatem z treści książki, która programem komputerowym nie jest.

Podkreślając, że na gruncie dyrektywy 2001/29 nie dochodzi do zrównania elektronicznej i fizycznej postaci utworu (co wynika również z uzasadnienia wniosku w sprawie dyrektywy 2001/29[3]), TSUE przyjął, że na gruncie dyrektywy 2001/29 pojęcie oryginału lub kopii utworu może dotyczyć jedynie ich fizycznej, materialnej postaci. Trybunał wskazał, że e-book należy odróżnić od fizycznej książki, inaczej niż miało to miejsce w sprawie egzemplarzy fizycznych i cyfrowych programu komputerowego w sprawie UsedSoft. Książka w formie fizycznej podlega bowiem naturalnemu zużyciu, zniszczeniu w toku jej użytkowania, czego nie można powiedzieć o e-booku, czy też programach komputerowych. W konsekwencji, TSUE uznał że nie doszło do wyczerpania praw, dotyczy ono bowiem „oryginału lub kopii" (art. 4 ust. 2 dyrektywy 2001/29). Tymczasem działalność wykonywana przez Tom Kabinet sprowadzała się do publicznego udostępniania utworów (art. 3 dyrektywy 2001/29), do czego wymagana była zgoda podmiotu uprawnionego.

Konsekwencje wyroku dla branży IT

Wyrok w sprawie Tom Kabinet warto przeanalizować z perspektywy wtórnego rynku odsprzedaży oprogramowania IT, w tym utworów złożonych jak gry komputerowe. Nie jest bowiem wykluczone, że najnowszy wyrok TS UE może zmierzać do zmiany stanowiska w sprawie wyczerpania praw do utworów i przyjęcia bardziej restrykcyjnego

[3] Zob. uzasadnienie wniosku w sprawie dyrektywy Parlamentu Europejskiego i Rady z dnia 10 grudnia 1997 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym [COM(97) 628 wersja ostateczna, zwanego dalej „wnioskiem w sprawie dyrektywy"], leżącej u podstaw dyrektywy 2001/29

podejścia. Będzie on szczególnie istotny dla producentów bądź odsprzedawców złożonych programów komputerowych, składających się z osadzonych elementów graficznych, muzycznych czy słownych, w tym gier komputerowych.

Warto bowiem podkreślić, że TSUE wypowiedział się już w sprawie Nintendo (C-355/12) na temat złożonych programów komputerowych, a konkretnie gier komputerowych, stwierdzając, że są one chronione na gruncie dyrektywy 2001/29 jako całość[4]. Odczytując powyższe w świetle orzeczenia w sprawie Tom Kabinet można postawić wniosek, że obrót takimi „używanymi" programami będzie możliwy tylko w przypadku fizycznych egzemplarzy gier, a nie ich cyfrowych nośników. Do tej pory w tej kwestii nie wypowiedział się jednak kategorycznie ani TSUE ani polskie orzecznictwo, chociaż – jeszcze przed wyrokiem w sprawie Tom Kabinet - sąd we Francji uznał, że sprzedaż gier w wersji cyfrowej prowadzi do wyczerpania prawa do cyfrowego egzemplarza tej gry.

Wydaje się jednak, że bezpośrednie zastosowanie wyroku w sprawie Tom Kabinet do oprogramowania złożonego z wielu elementów, w tym graficznych, muzycznych czy słownych byłoby nieuprawnione z co najmniej kilku powodów:

- O ile sprzedaż fizycznego egzemplarza książki różni się od sprzedaży w formie elektronicznej, o tyle w przypadku złożonego oprogramowania mamy do czynienia z sytuacją analogiczną jak przy sprzedaży programu komputerowego – sprzedaż pudełkowa i elektroniczna są z punktu widzenia ekonomicznego do siebie zbliżone, a fizyczna kopia produktu, po jego zainstalowaniu, nie jest zawsze potrzebna – czasami płyta musi znajdować się w napędzie podczas korzystania, ale nie zawsze.
- Niezależnie od powyższego, płyta nadal zużywa się w znacznie mniejszym stopniu, bowiem nie korzystamy z niej fizycznie podczas korzystania z produktu tj. nie musimy jej dotykać czy przewracać kartek jak w książce.
- Trudno uznać, że program komputerowy ma funkcję pomocniczą wobec pozostałych części składowych oprogramowania, takich jak interfejs graficzny czy muzyka – tak jak uznano w przypadku e-booka. Sposób interakcji z programem i jego przejrzystość są często istotnym dla użytkownika elementem, jednak za każdym
- O ile e-book, nawet opatrzony znakiem wodnym, można łatwiej skopiować np. wykonując fotografie wszystkich stron, o tyle wykonanie kopii plików gry komputerowej czy innego oprogramowania zazwyczaj jest fabrycznie niemożliwe, a zrobienie zdjęć gry wideo czy oprogramowania nie umożliwia korzystania z nich. Nawet jednak jeśli kopia zostanie wykonana, jej odsprzedaż nie będzie legalna, zgodnie z wyrokiem w sprawie Ranks.

W końcu, zaprezentowany problem nie może zostać rozstrzygnięty poprzez zastosowanie różnych przepisów do części składowych takich złożonych produktów. Wyczerpanie prawa bowiem, a w konsekwencji odsprzedaż, może dotyczyć tylko całości utworu, w innym wypadku dojdziemy do stworzenia trudnego do zaakceptowania od strony praktycznej reżimu prawnego ochrony takich utworów, bez możliwości jego praktycznego stosowania.

Podsumowanie

Wyrok w sprawie Tom Kabinet z całą pewnością będzie miał kluczowe znaczenie w perspektywie obrotu wtórnego egzemplarzami e-booków, bowiem jednoznacznie opowiada się za stanowiskiem, zgodnie z którym, w przypadku książek elektronicznych, nie mamy do czynienie z instytucją wyczerpania prawa.

Powstaje jednak pytanie, jakie znaczenie wyrok ten będzie miał dla wtórnego obrotu złożonym oprogramowaniem. Być może jesteśmy świadkami zmiany – lub co najmniej - korekty linii orzeczniczej Trybunału, bowiem już wyrok w sprawie Ranks stanowił pewien krok w kierunku zwiększania ochrony twórców, a Tom Kabinet znacznie mocniej opowiada się po ich stronie. Pozostaje wobec tego śledzić kolejne orzeczenia TS UE, aby zidentyfikować czy ta tendencja będzie się utrzymywać. Jeżeli kolejne wyroki w stosunku do złożonego oprogramowania będą opierać się na wyroku Tom Kabinet, a nie UsedSoft, może dojść do znacznego zmniejszenia możliwości obrotu cyfrowymi egzemplarzami produktów na rynku wtórnym. Taka sytuacja byłaby korzystna dla twórców, a uciążliwa dla konsumentów, którzy oprogramowanie na rynku wtórnym mogą kupić taniej.

[4] „W zakresie, w jakim gra wideo, w tym wypadku jej elementy graficzne i dźwiękowe, przyczyniają się do oryginalności utworu, są one, wraz z całością danego dzieła, chronione prawem autorskim w ramach reżimu ustanowionego przez dyrektywę 2001/29."
[5] Zob. http://copyrightblog.kluweriplaw.com/2019/12/12/does-the-doctrine-of-exhaustion-apply-to-videogames-purchased-digitally-french-court-says-oui/?doing_wp_cron=1594117782.2534539699554443359375 oraz https://newtech.law/pl/zmierzch-rynku-wtornego-e-bookow-i-gier-wideo/

Zakup komputerów i systemów IT przez zamawiających – pomogą nowe rekomendacje UZP

Pod koniec 2019 r. Urząd Zamówień Publicznych (dalej: „UZP") zainicjował konsultacje z organizacjami branżowymi w zakresie aktualizacji bądź stworzenia na nowo dokumentów: Udzielanie zamówień publicznych na dostawę zestawów komputerowych. Rekomendacje (2012 r.; dalej: „Rekomendacje ds. komputerów") oraz Udzielanie zamówień publicznych na systemy informatyczne. Rekomendacje (2009 r.; dalej: „Rekomendacje ds. systemów").

UZP zaprosił do udziału w pracach przedstawicieli następujących organizacji: Polska Izba Informatyki i Telekomunikacji, Izba Gospodarki Elektronicznej, Związek Cyfrowa Polska, Polskie Towarzystwo Informatyczne oraz Polski Związek Ośrodków Przetwarzania Danych. Są to zatem organizacje branżowe, które aktywnie działają na rynku, reprezentując interes przedsiębiorców z branży ICT, w tym wspierając dobre praktyki na tym polu. Zaproszone organizacje oddelegowały swoich przedstawicieli do współpracy z UZP oraz zaangażowały znacznie większą liczbę ekspertów do prac w grupach roboczych utworzonych w tym celu wewnątrz organizacji. Wśród osób biorących udział w pracach są profesjonalni prawnicy oraz – co szczególnie ważne – specjaliści z branży ICT. Stworzono dwie odrębne grupy robocze: Zespół ds. zestawów komputerowych oraz Zespół ds. systemów informatycznych. W prace obu zespołów z ramienia Polskiej Izby Informatyki i Telekomunikacji zaangażowani są prawnicy z naszej kancelarii: mec. Agnieszka Wachowska, (Partner) oraz mec. Tomasz Krzyżanowski (Senior Associate).

Zespoły pracujące nad dokumentami wytycznych przyjęły dwie odmienne koncepcje dotyczące dokumentów rekomendacji. Obecnie tworzone rekomendacje ds. komputerów stanowić będą aktualizację wcześniej wydanego przez UZP dokumentu z 2012 r., uwzględniając postęp techniczny, jaki się dokonał w ostatniej dekadzie. Zostaną one również poszerzone o nowy zakres tematyczny.

Natomiast rekomendacje ds. Systemów z uwagi na specyfikę zmian na rynku informatycznym w odniesieniu do systemów informatycznych jakie dokonały się od 2009 r. tworzone są w zasadzie na nowo.

Oba dokumenty rekomendacji mają odnosić się do stanu prawnego, jaki będzie obowiązywał od 1 stycznia 2021 r., tj. będą się odwoływały do Ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (dalej: „Nowe PZP").

Warto odnotować, że w pracach obu zespołów ze strony UZP bierze aktywnie udział sam Prezes UZP, Hubert Nowak.

Oba dokumenty rekomendacji nie są ani nie będą aktami prawa. Prace nad nowymi rekomendacjami stanowią odpowiedź na potrzeby rynku, w szczególności publicznych zamawiających, którzy przy zakupach systemów informatycznych oraz sprzętu IT często borykają się z problemem odpowiedniego zorganizowania procesu zakupowego. Pomocne w tym mają być właśnie sugestie Prezesa UZP, który ma formalny autorytet w sferze zamówień publicznych i ustawowe uprawnienie ku tej działalności[1].

Dokumenty rekomendacji mają zatem na celu przede wszystkim pomóc instytucjom zamawiającym w jak najlepszym przygotowaniu i przeprowadzeniu postępowań o udzielenie zamówienia publicznego, w tym w jak najlepszym opisaniu przedmiotu zamówienia, a także ustaleniu odpowiednich warunków udziału w postępowaniu i kryteriów oceny ofert w sposób zapewniający równe traktowanie wykonawców oraz uczciwą konkurencję, przy uszanowaniu efektywności udzielania zamówień publicznych z uwzględnieniem uzasadnionych potrzeb zamawiającego. Warto przy tym odnotować, że beneficjentami dobrych praktyk forsowanych przez Prezesa UZP są także wykonawcy. Mniejsza liczba błędów zamawiających przy sporządzaniu dokumentacji postępowania powinna przekładać się na lepsze zrozumienie przedmiotu zamówienia przez wykonawców, a co za tym idzie także lepszą ocenę ryzyk projektu i odpowiednie skalkulowanie ceny.

[1] Prezes Urzędu Zamówień Publicznych jest centralnym organem administracji rządowej właściwym w sprawach zamówień publicznych, a do jego obowiązków należy m.in. przygotowywanie i upowszechnianie dokumentów stosowanych przy udzielaniu zamówień i dążenie do zapewnienia jednolitego stosowania przepisów o zamówieniach.

Poniżej przedstawimy zwięzły opis podsumowujący prace obu zespołów do tej pory.

I. Zespół ds. zestawów komputerowych

UZP wskazał, że zależy mu przede wszystkim na wsparciu w zakresie kwestii technicznych, które są istotną częścią rekomendacji i które w ostatnich 10 latach w znacznej części się zdezaktualizowały. Część wstępną i otoczenie prawne aktualizuje UZP. Z tego względu Zespół ds. zestawów komputerowych skupił się na aktualizacji dokumentu, począwszy od pkt. 3, tj. „Zasady konstruowania SIWZ w sposób nieograniczający konkurencji", zwracając szczególną uwagę na kwestie techniczne. Przyjęto przy tym model unikania nadmiernej kazuistyki. Rekomendacje mają mieć charakter na tyle ogólny, aby mogły być uniwersalnym poradnikiem w różnych postępowaniach na dostawę urządzeń komputerowych.

Kierunki zmian lub rozwiązania, jakie zaproponowano:

1. Rezygnacja z określenia „zestaw komputerowy" na rzecz pojęcia „urządzenia komputerowego" jako szerszego, obejmującego większe spektrum urządzeń, które pojawiły się na rynku w ostatniej dekadzie.

2. Wprowadzenie definicji poszczególnych grup urządzeń, np. definicje dla komputera stacjonarnego, komputera typu „All in One", komputera przenośnego, komputera przenośnego wzmocnionego, tabletu.

3. Konkretne zmiany, aktualizujące lub wprowadzające zupełnie nową treść:

- do tabeli nr 1 – Elementy opisu przedmiotu zamówienia na dostawę urządzeń komputerowych;
- do tabeli nr 2 – Wymagania dotyczące stosowanych testów wydajnościowych urządzeń;
- do tabeli nr 3 – Zapisy niedopuszczalne w opisie przedmiotu zamówienia na dostawę urządzeń komputerowych;
- do tabeli nr 5 – Przykładowy opis wymagań dla urządzenia komputerowego;
- wprowadzenie listy rekomendowanych certyfikatów;
- wprowadzenie listy rekomendowanych zabezpieczeń sprzętu komputerowego, zarówno mechanicznych (uchwyty, kłódki, zamki), jak i oprogramowania realizującego zabezpieczenie danych oraz ochronę danych, w tym danych osobowych, szyfrowanie danych;
- wprowadzenie odrębnych dodatkowych tabel z parametrami dla urządzeń drukujących, monitorów, smartfonów, tabletów.

4. Ponadto przedstawiono w odrębnym dokumencie propozycje opisania w Rekomendacjach ds. komputerów wymagań opisu przedmiotu zamówienia w zakresie próbek urządzeń oraz zwrócono się o przedstawienie w Rekomendacjach ds. komputerów przez UZP interpretacji Nowego PZP (art. 101 ust. 4) w zakresie tego, czy przy opisaniu przedmiotu zamówienia przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych istnieje wymóg analogiczny jak w art. 99 ust. 6, tj. obowiązek określenia przez zamawiającego kryteriów stosowanych w celu oceny równoważności, gdyż nie jest to wprost określone w ustawie.

Warto wskazać, że w czasie prac zespołu szczególne zainteresowanie i komentarze wywołał temat testów wydajnościowych, w tym korzyści i wad, jakie mają testy aplikacyjne i testy syntetyczne. Testy syntetyczne służą do pomiarów pojedynczych komponentów systemu, dają informacje o pomiarze jakiejś składowej niezależnie od pozostałych aspektów, np. karty graficznej. Wadą takich testów jest to, że nie dają informacji o szybkości całego komputera. Testy aplikacyjne wykorzystują typowe aplikacje biurowe czy multimedialne i mierzą czas wykonywania różnych zadań, np. przetwarzania dokumentów, wskazując na ogólną wydajność urządzenia. Ostateczna decyzja o kształcie rekomendacji w tym zakresie należy do UZP, jednakże z dotychczasowego przebiegu prac zdaje się wynikać, że rekomendowane będę testy aplikacyjne, a testy syntetyczne będą dopuszczalne w przypadku uzasadnienia potrzeby ich zastosowania przez zamawiających specyfiką danego postępowania.

Należy się spodziewać, że jeszcze w czasie wakacji UZP zamieści na swojej stronie internetowej zaktualizowany dokument rekomendacji wypracowany przez Zespół ds. komputerów w celu gruntownych konsultacji publicznych. Dodatkowo uzgodniono, że w następnej kolejności Zespół ds. zestawów komputerowych podejmie pracę nad ustaleniem dalszych suplementów, w tym dotyczących warunków udziału w postępowaniu oraz kryteriów selekcji i kryteriów oceny ofert.

II. Zespół ds. systemów informatycznych

Zgodnie z założeniami prac zespołu roboczego, nowe rekomendacje dotyczące zamawiania systemów informatycznych mają powstawać w częściach i być przygotowane w kilku oddzielnych publikacjach, stanowiących w całości kompleksowy przewodnik po zamawianiu systemów IT w reżimie Nowego PZP:

- Część 1. – Przygotowanie postępowania i OPZ (w tym zasady oceny ofert).
- Część 2. – Warunki udziału w postępowaniu, kryteria selekcji i kryteria oceny ofert.
- Część 3. – Umowa i realizacja zamówienia.

W czerwcu 2020 r. UZP opublikował pierwszy ważny dokument wypracowany przez Zespół ds. systemów. Materiał dotyczy czynności przygotowawczych przed wszczęciem postępowania[2]. Stanowi on wstęp do planowanych nowych wytycznych w zakresie zamawiania systemów IT oraz zawiera praktyczne wskazówki odnośnie działań, jakie zamawiający powinien rozważyć na etapie planowania i przygotowywania postępowania dotyczącego systemu informatycznego, jak również wpływu decyzji inicjujących proces zakupowy na dalsze losy postępowania. Szersze omówienie tego dokumentu znajduje się w niniejszym newsletterze w tekście „Rekomendacje UZP na systemy informatyczne".

Obecnie prace zespołu roboczego ds. systemów informatycznych skoncentrowane są na II tomie, czyli wytycznych dotyczących formułowania opisu przedmiotu zamówienia dla systemów informatycznych. Począwszy od tomu II, Prezes UZP zamierza poddawać konsultacjom publicznym powstające materiały, licząc na konstruktywne uwagi do nich.

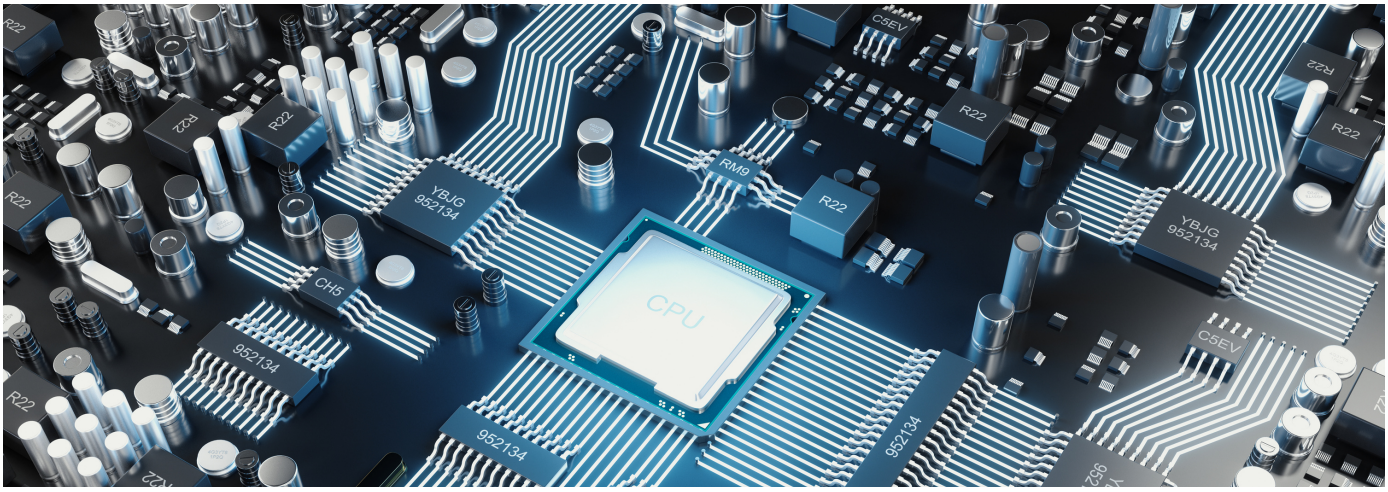
III. Podsumowanie

UZP oraz eksperci biorący udział w pracach obu zespołów wiążą z rekomendacjami duże nadzieje. Oba dokumenty, zanim się zdezaktualizowały, były kompleksowo wykorzystywane przez zamawiających przy tworzeniu dokumentacji przetargowych. Co więcej, również instytucje kontrolujące postępowania – w tym współfinansowane ze środków UE – często opierały się na treści rekomendacji, rozstrzygając, czy zamawiający naruszyli ustawę Prawo zamówień publicznych, w konsekwencji decydując lub nie o nałożeniu korekty finansowej. Celem prac obu zespołów jest stworzenie rekomendacji, które będą zawierać praktyczne wskazówki i jednocześnie przystawać do naszych czasów, stając się na nowo „przewodnikiem" dla zamawiających w zakresie zamówień z branży ICT.

Prace nad rekomendacjami stanowią spore wyzwanie. Materia, której poświęcone są rekomendacje nie jest prosta, oraz budzi pewne kontrowersje w środowisku specjalistów zajmujących się kwestiami IT oraz stosowaniem Nowego PZP w postępowaniach dot. IT, co wymaga wypracowania satysfakcjonującego wszystkich kompromisu i znalezienia rozwiązania, które będzie mogło być również rekomendowane przez UZP. Do tego eksperci zaangażowani w tworzenie rekomendacji pracują w ramach powołanych grup eksperckich pro bono i muszą znaleźć czas na tworzenie dobrych jakościowo wytycznych obok codziennych obowiązków zawodowych. Warto jednak podkreślić, że w pracy obu grup roboczych widać duże zaangażowanie i wspólny cel w postaci stworzenia dobrych merytorycznie i jednocześnie praktycznych dokumentów, które wywrą realny i pozytywny wpływ na rynek zamówień publicznych w zakresie ICT.

UZP planuje stopniowo udostępniać efekty prac obu zespołów. Wychodzi przy tym ze słusznego założenia, że należy dzielić się z wykonawcami i zamawiającymi efektami prac w miarę ich powstawania. Wypracowane materiały – jako autonomiczne dokumenty – będą poddawane konsultacjom publicznym. Zachęcamy zatem do śledzenia strony UZP oraz newslettera PZP kancelarii Traple Konarski Podrecki i Wspólnicy (będziemy informować o postępach prac) i włączania się w proces, który pozwoli na sukcesywne wypracowywanie dokumentów stanowiących istotną, praktyczną pomoc w przygotowaniu postępowań o udzielenie zamówienia publicznego.

[2] Zob. https://www.uzp.gov.pl/strona-glowna/slider-aktualnosci/zamowienia-publiczne-na-systemy-informatyczne-pierwszy-tom-rekomendacji/zamowienia-publiczne-na-systemy-informatyczne-pierwszy-tom-rekomendacji (dostęp: 6.08.2020).



Rekomendacje UZP na systemy informatyczne

Urząd Zamówień Publicznych (UZP) opublikował I tom rekomendacji dotyczących zamówień publicznych na systemy informatyczne. Opublikowany na stronach UZP dokument zawierający wytyczne dla zamawiających - "co warto zrobić i przemyśleć przed wszczęciem postępowania na system informatyczny", stanowi pierwszy z cyklu zapowiedzianych rekomendacji UZP dot. branży IT, będących wynikiem prac grup roboczych wspierających UZP przy nowych rekomendacjach dotyczących zamówień publicznych na systemy i sprzęt IT, w których z ramienia Polska Izba Informatyki i Telekomunikacji uczestniczą przedstawiciele naszej Kancelarii: mec. Agnieszka Wachowska, partner w kancelarii Traple Konarski Podrecki i Wspólnicy oraz mec. Tomasz Krzyżanowski. Szersze omówienie tego tematu znajduje się w niniejszym newsletterze w tekście „Zakup komputerów i systemów IT przez zamawiających – pomogą nowe rekomendacje UZP".

Dokument zawiera praktyczne wskazówki dla zamawiających, dotyczące kwestii, które powinni rozważyć na etapie planowania i przygotowywania postępowania dotyczącego systemu informatycznego, jak również wpływu decyzji inicjujących proces zakupowy na dalsze losy postępowania[1]. **Rekomendacje przygotowane zostały na podstawie przepisów tzw. Nowego PZP[2], które wejdzie w życie z dniem 1 stycznia 2021 r.**

Poprzednie rekomendacje UZP na systemy informatyczne pochodzą z 2009 r.[3]. Czyni je to w pewnym stopniu nieaktualnymi i niepraktycznymi, w trakcie dekady nastąpiły bowiem istotne zmiany prawne, o dynamicznym postępie technologicznym nie wspominając.

I tom rekomendacji Prezesa UZP składa się z dwóch części:

- **części 1**, obejmującej listę zagadnień, które powinien rozważyć zamawiający, przygotowując postępowanie;
- **części 2**, zawierającej informację o źródłach i narzędziach do pozyskiwania wiedzy koniecznej dla przygotowania postępowania.

Omówienie okoliczności, które zamawiający powinien wziąć pod uwagę, planując zakup systemów informatycznych, zostało przedstawione w rekomendacjach poprzez propozycję pytań (checklistę). Wśród pytań, na które powinien odpowiedzieć zamawiający, znalazły się następujące:

- Czy zamawiający dysponuje odpowiednim personelem, aby samodzielnie zidentyfikować swoje potrzeby i opisać przedmiot zamówienia?
- Czy zamawiający dysponuje odpowiednim personelem, aby samodzielnie zrealizować przedmiot zamówienia (wdrożenie systemu), czy potrzebuje wsparcia ze strony doradcy?
- Czy zamawiający dokonał inwentaryzacji posiadanych zasobów i potrzeb?
- Czy zamawiający konsultował potrzebę zamówienia z innymi zamawiającymi, realizującymi podobne zamówienia lub z którymi działa wspólnie?
- Czy zamawiający sprawdził możliwość uzyskania dofinansowania na planowany zakup sytemu informatycznego?
- Czy zamawiający ma wszystkie informacje, aby prawidłowo oszacować wartość zamówienia?
- Czy zamawiający zweryfikował swoje potrzeby pod kątem inwestycji w rozwiązania on-premises lub zamówienia na systemy w modelu chmurowym SaaS, czy też dopuszcza oba te rozwiązania?
- W jakim trybie postępowania zamawiający zamierza zamówić system IT?

[1] Zob. https://www.uzp.gov.pl/strona-glowna/slider-aktualnosci/zamowienia-publiczne-na-systemy-informatyczne-pierwszy-tom-rekomendacji/zamowienia-publiczne-na-systemy-informatyczne-pierwszy-tom-rekomendacji (dostęp: 20.07.2020).
[2] Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. oraz z 2020 r. poz. 299).
[3] Zob. https://www.uzp.gov.pl/__data/assets/pdf_file/0025/27574/Rekomendacje_UZP20ws._zamowiec584_na_systemy_informatyczne.pdf (dostęp: 20.07.2020).

Na podstawie tak postawionych pytań dla zamawiającego zostały sformułowane następujące rekomendacje dla zamawiających:

- Zweryfikuj zasoby kadrowe.
- Rozpoznaj swoje potrzeby i oczekiwania.
- Sprawdź zasoby informatyczne (sprzęt, oprogramowanie, systemy, licencje).
- Zweryfikuj, czy inni zamawiający nie mają podobnych potrzeb – aby przeprowadzić zamówienie wspólnie z nimi.
- Sprawdź, czy możesz ubiegać się o dofinansowanie.
- Starannie oszacuj wartość zamówienia.
- Ustal, czy zamawiasz oprogramowanie chmurowe bądź on-premises.
- Określ, w jakim trybie zamierzasz prowadzić postępowanie.

W odniesieniu do źródeł pozyskiwania wiedzy koniecznej do przygotowania postępowania zamawiający powinien rozpocząć od własnej organizacji zamawiającego, w szczególności wśród wykwalifikowanego personelu odpowiadającego za poszczególne obszary merytoryczne. Gdy w organizacji zamawiającego brakuje kwalifikacji odpowiednich dla projektu, konieczne jest pozyskanie wiedzy z rynku, np. poprzez zatrudnienie na podstawie umowy o pracę lub poprzez zakup usług doradczych.

Rekomendacje Prezesa UZP, chociaż opracowywane na podstawie Nowego PZP, mogą stanowić cenną wskazówkę dla zamawiających również przy przygotowywanych postępowaniach, do których zastosowanie mają aktualnie obowiązujące przepisy z zakresu zamówień publicznych.

I tom rekomendacji dostępny jest tutaj:
https://www.uzp.gov.pl/__data/assets/pdf_file/0020/43274/Czynnosci-przygotowawcze-zamowienie-publiczne-na-system-informatyczny.pdf.

Projekt zaleceń UNESCO w sprawie etyki AI

W ostatnich miesiącach Unia Europejska gruntownie zajęła się tematem sztucznej inteligencji (AI). Na naszym blogu można przeczytać o unijnym projekcie regulacji prawnych dotyczących odpowiedzialności za działanie AI. Niedawno opublikowany został również dokument pozwalający ocenić, czy dana AI jest godna zaufania. Świadomość nadchodzących zmian, np. w zakresie wynalazków stworzonych przez AI, sygnalizowana jest z kolei w dokumencie Intellectual property action plan, opracowanym przez Komisję Europejską.

Kwestią sztucznej inteligencji zajęło się także UNESCO: rozpoczęły się publiczne konsultacje online projektu zaleceń dotyczących etyki AI, przygotowanego przez Grupę Ekspercką Ad Hoc UNESCO (tekst dostępny pod linkiem: https://unesdoc.unesco.org/ark:/48223/pf0000373434).

Celem projektu zaleceń, jak wskazują jego autorzy, jest sformułowanie wartości etycznych, zasad i zaleceń politycznych w zakresie badań, projektowania, rozwoju, wdrażania i wykorzystywania sztucznej inteligencji, tak aby systemy AI działały dla dobra ludzkości, jednostek, społeczeństw i środowiska naturalnego. Dokument stanowi również bardzo interesującą diagnozę wielu problemów nie tylko o charakterze etycznym, ale również ekonomiczno-społecznym, związanych z upowszechnieniem AI. Jest to ciekawe i świeże spojrzenie, zwłaszcza mając na uwadze fakt, że wiele ze wskazanych w tym dokumencie problemów nie było dotąd szerzej podejmowanych.

Omawiany projekt, po konsultacjach międzyrządowych, ma zostać przedstawiony pod koniec 2021 r. Konferencji Generalnej, która może podjąć decyzję o jego przyjęciu. Ostateczna, przyjęta wersja rekomendacji nie będzie stanowić obowiązującego prawa, ale można założyć , że z pewnością przyczyni się do ustanowienia uznawanych na całym świecie standardów dotyczących AI.

W dokumencie wskazane są następujące obszary i ich cele, a także propozycje działań:

- Etyczne zarządzanie AI – zapewnienie zgodności badań, projektowania, rozwoju, wdrażania i wykorzystania AI z podstawowymi wartościami etycznymi, takimi jak prawa człowieka, różnorodność i integracja społeczna.
- Ocena wpływu AI – budowanie zdolności umożliwiających reagowanie w odpowiednim czasie na negatywne lub inne niezamierzone skutki wynikające z działania systemów AI.
- Budowanie potencjału w zakresie etyki AI – rozwój zdolności ludzkich i instytucjonalnych w celu umożliwienia oceny skutków etycznych, nadzoru i zarządzania AI.
- Rozwój i współpraca międzynarodowa przy stosowaniu AI– zapewnienie wspólnego i etycznego podejścia do stosowania AI w takich dziedzinach rozwoju, jak m.in.: opieka zdrowotna, rolnictwo / zaopatrzenie w żywność, edukacja, kultura, środowisko.
- Zarządzanie na rzecz etyki AI – promowanie uwzględniania kwestii etycznych w zarządzaniu systemami SI.

Wybrane istotne postulaty zostały przedstawione poniżej.

Równość szans, niedyskryminacja, prawa człowieka

W projekcie zaleceń zwrócono uwagę na problem podziałów społecznych, które pogłębiają się wraz z rozwojem cyfryzacji i upowszechnieniem AI. W tym kontekście, wskazano, że konieczne jest zapewnienie poszanowania drugiego człowieka – jego kultury, płci, wyznania, języka, pochodzenia czy orientacji seksualnej. W tym celu **już na etapie tworzenia AI**, a później w toku całego cyklu życia produktu konieczne jest zapewnienie udziału kobiet i mężczyzn, ludzi z różnych kultur i o różnym wyznaniu, a także osób z niepełnosprawnością. Wszystkie osoby biorące udział w pracach nad AI **powinny być ponadto odpowiednio wyedukowane w zakresie problemów i wzorców etycznych**, zgodnie z przyjętymi normami moralnymi i kulturowymi w poszczególnych rejonach świata.

Powyższe jest tym bardziej istotne, że obecnie jednym z dostrzegalnych problemów, jakie są związane z AI, jest „uprzedzenie" systemów, wynikające często z doboru członków grupy, która zajmowała się ich tworzeniem. Pewne stereotypy uwzględnione (nawet nieintencjonalnie) w projekcie systemu są później rozwijane i pogłębiane przez algorytmy. Jeżeli zatem już na etapie tworzenia algorytmów leżących u podstaw AI nie zostanie zapewniony zespół nie tylko interdyscyplinarny, ale także multikulturowy, złożony z ludzi różnej płci, rasy i wyznania, to następcze usuwanie tych uprzedzeń systemu będzie bardzo trudne lub niemożliwe.

Aspekt równego udziału w pracach nad AI wiąże się ściśle ze zdiagnozowanym problemem edukacji. Autorzy rekomendacji wskazują, że **konieczne jest zapewnienie przez państwa członkowskie** kształcenia ukierunkowanego na rozwój umiejętności informatycznych, podnoszenie świadomości zmian technologicznych i uczenie ludzi, w toku całej ich edukacji – niezależnie od wybranego kierunku – o tym, jak technologia AI wpływa na nasze życie i jak należy z nią współpracować. **Nacisk powinien zostać położony** na rozwijanie umiejętności potrzebnych do pracy z oraz nad AI: matematykę, czytanie, pisanie, programowanie.

Rynek pracy

Problem związany z edukacją, o którym mowa powyżej, to tylko jeden z przejawów nadchodzących zmian społecznych. W tym zakresie trudnym zadaniem może się okazać kwestia przeciwdziałania wykluczeniu obecnych pracowników, których AI może zastąpić bądź też którzy nie mają wystarczających umiejętności do obsługi systemów informatycznych. W rekomendacjach wskazano, że **państwa oraz pracodawcy, a także organizacje społeczne i zawodowe** powinny zapewnić **odpowiednie mechanizmy bezpieczeństwa dla takich osób – przede wszystkim odpowiednie szkolenia pozwalające zdobyć kompetencje w dobie zmian technologicznych**, a tam, gdzie to konieczne, **pozwalające tym osobom się przekwalifikować i podjąć pracę w innym zawodzie**.

Zarządzanie i regulacje prawne

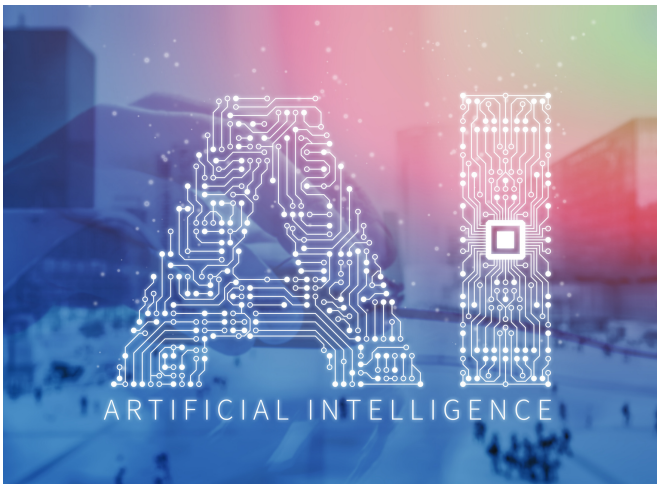
Kluczowy postulat to również **zapewnienie transparentności AI**, czyli – umożliwienie jasnego określenia, jak działa konkretna AI, aby móc post factum stwierdzić, dlaczego system podjął takie, a nie inne decyzje i skąd czerpał dane wykorzystane w procesie decyzyjnym. W dokumencie wskazano na pewne sektory, w których potrzeba transparentności jest większa, jak chociażby obszar prawny i sądowniczy, zwłaszcza że w wielu krajach trwają prace nad wprowadzeniem systemu sądownictwa opartego na AI, przede wszystkim w zakresie drobnych spraw rozpatrywanych w pierwszej instancji.

Jedną z propozycji jest również **stworzenie przez państwa systemu certyfikacji AI**. Proponowane jest wprowadzenie różnych klas certyfikacji w zależności od wrażliwości dziedziny zastosowania i oczekiwanego wpływu na życie ludzkie, środowisko, względy etyczne, takie jak m.in. równość, różnorodność i wartości kulturowe. Propozycja w tym zakresie jest więc różnorodna i nie ogranicza się jedynie do wybranych aspektów, jak np. cyberbezpieczeństwa systemów (por. artykuł „Europejskie programy certyfikacji cyberbezpieczeństwa – chmura i produkty ICT").

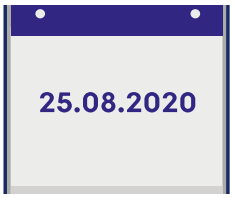
W rekomendacjach podjęto również temat **odpowiedzialności za działanie AI**. Twórcy zaleceń jednoznacznie opowiadają się przeciwko pociąganiu do odpowiedzialności samej AI oraz przeciwko przyznaniu jej osobowości prawnej. Poszczególne **państwa powinny zapewnić możliwość stałego monitoringu i oceny skutków działania AI**, a także jednoznacznego wskazania podmiotu odpowiedzialnego za skutki tych działań. W tym zakresie dokument nie przedstawia konkretnych propozycji dotyczących ustanowienia podmiotów odpowiedzialnych, jak np. zrobiono to w projekcie unijnych przepisów regulujących odpowiedzialność deliktową AI, omówionym na naszym blogu.

Podsumowanie

Opublikowany projekt zaleceń UNESCO, z racji swojej ogólności, nie przedstawia szczegółowych ani konkretnych rozwiązań dla zidentyfikowanych problemów. Nie we wszystkich przypadkach zresztą byłoby to możliwe – niektóre obszary wymagają dalszych analiz w celu zaprojektowania i przyjęcia optymalnych propozycji. Istotne jest przy tym to, że projekt stanowi przegląd i podsumowanie kwestii i wyzwań etycznych, które powinny zostać wzięte pod uwagę przy tworzeniu i przyjmowaniu przepisów w zakresie AI. Tym samym po przyjęciu ostatecznej wersji projektu może stać się ważnym punktem odniesienia dla ustawodawców poszczególnych państw członkowskich.



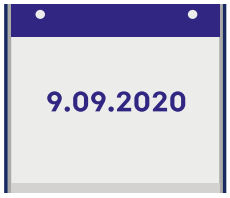
NADCHODZĄCE WYDARZENIA



"Prawne aspekty cyberbiezpieczeństwa"

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

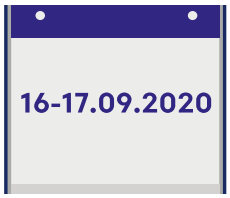
Więcej informacji >>



"Umowy na korzystanie z oprogramowania w chmurze obliczeniowej - wyzwania, ryzyka i praktyczne aspekty zawierania i negocjowania umów na cloud computing"

adw. Xawery Konarski, r. pr. Agnieszka Wachowska

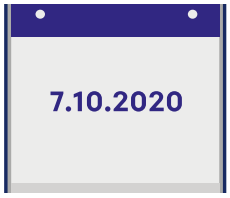
Więcej informacji >>



"XIII Forum Bezpieczeństwa i Audytu IT SEMAFOR"

„Jak kupować usługi z zakresu cyberbezpieczeństwa i jakie umowy zawierać?”
r. pr. Agnieszka Wachowska, r. pr. Joanna Jastrząb

Więcej informacji >>



"Wdrożenie IT - jak przygotować dobrą umowę oraz dobrze przygotować się do wdrożenia"

r. pr. Agnieszka Wachowska

Więcej informacji >>

ZESPÓŁ IT-TELCO

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

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

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

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

Joanna Stecyk
Radca prawny, Senior Associate
joanna.stecyk@traple.pl

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

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

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

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

Aleksander Elmerych
Junior Associate
aleksander.elmerych@traple.pl

Michał Kalinowski
Legal Trainee
michal.kalinowski@traple.pl

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