NR 7 - LISTOPAD 2020

NEWSLETTER

IT-TECH

W NUMERZE:

- Cyberbezpieczeństwo w umowach wdrożeniowych systemów IT
- Oprogramowanie jako produkt podwójnego zastosowania (dual-use item)
- Czas pracy a branża IT
- Zagadnienia prawne i praktyczne stosowania kwalifikowanego podpisu elektronicznego
- Zakup komputerów przez zamawiających – pomogą zaktualizowane rekomendacje UZP
- Wyrok WSA: Nie ma obowiązku prowadzenia ewidencji IP BOX na bieżąco

Traple
Konarski
Podrecki
& Wspólnicy

TKP

Cyberbezpieczeństwo w umowach wdrożeniowych systemów IT

r.pr. Joanna Jastrząb, Aleksander Elmerych

Wdrożenia systemów informatycznych to niezwykle złożone procesy, trwające często miesiącami, a nawet latami. W zależności od rodzaju wdrożenia oprócz samego dostarczenia systemu często obejmuje ono również świadczenie szeregu dodatkowych usług po ukończeniu wdrożenia, takich jak utrzymanie czy rozwój oprogramowania. Z tych powodów umowy na rozwiązania IT zwykle są rozbudowane i wyczerpująco opisują funkcjonalności i cechy, które powinien mieć wdrażany system informatyczny, jak również szczegółowo określają wymagania techniczne, które powinien spełniać. Mimo bardzo dokładnego uregulowania tych aspektów często pomijana jest kwestia, która ma coraz większe znaczenie dla prawidłowego i niezakłóconego funkcjonowania oprogramowania – jego odpowiednie zabezpieczenie, uniemożliwiające wyciek danych oraz zapobiegające dostępowi nieuprawnionych osób trzecich.

Specyfika cyberbezpieczeństwa we wdrożeniach IT

Warto na wstępie podkreślić, że cyberbezpieczeństwo nie jest problemem występującym jedynie na gruncie przepisów dotyczących ochrony danych osobowych i może obejmować nie tylko bezpieczeństwo informacji, lecz także systemy i usługi świadczone za ich pomocą. Brak odpowiedniego zabezpieczenia systemu informatycznego może nieść ze sobą wiele innych poważnych konsekwencji, takich jak udostępnienie na zewnątrz informacji stanowiących tajemnicę przedsiębiorstwa, zaszyfrowanie danych przechowywanych w systemie z żądaniem okupu za ich odszyfrowanie (bardzo popularne ostatnio ataki *ransomware*) lub zakłócenie ciągłości działania, co z kolei może wpływać na odpowiedzialność wobec kontrahentów. Problematyka cyberbezpieczeństwa na gruncie umów wdrożeniowych jest więc niezwykle doniosła i obejmuje wiele problemów, także natury prawnej. Przygotowując umowę wdrożeniową, warto mieć na uwadze również to, że incydenty związane z zagrożeniami cyberbezpieczeństwa mogą ujawnić się nawet dłuższy czas po wdrożeniu systemu, dlatego dobra umowa wdrożeniowa powinna te kwestie uwzględniać (np. w ramach gwarancji na system).

Standardy i normy w obszarze cyberbezpieczeństwa

Trzeba podkreślić, że zupełne pominięcie kwestii cyberbezpieczeństwa w umowie może utrudniać lub wręcz uniemożliwiać pociągnięcie wykonawcy do odpowiedzialności. Zdecydowana większość umów wdrożeniowych kwalifikowana jest przez sądy jako umowy o dzieło, a więc umowy, w których wykonawca zobowiązany jest do osiągnięcia określonego wcześniej rezultatu. W wypadku braku wyznaczenia w umowie szczegółowych wymagań co do cech zamawianego dzieła oraz kryteriów, według których rezultat ten ma być oceniany, należy stosować ogólną zasadę wynikającą z przepisów Kodeksu cywilnego[1] (dalej: „k.c.”), zgodnie z którą dłużnik zobowiązany jest do działania z należytą starannością (art. 355 k.c.).

Miernik należytej staranności ocenia się przede wszystkim poprzez zawodowy charakter działalności (art. 355 § 2 k.c.) oraz normy i standardy przyjęte w danej branży. Niemniej w zakresie odpowiedniego zabezpieczenia programu komputerowego, podobnie jak w zakresie właściwego wykonania systemu informatycznego, nie istnieją uniwersalne, powszechnie stosowane standardy, które pozwoliłyby jednoznacznie ustalić kryteria należytej staranności wykonawcy. Tym samym w praktyce, w wypadku braku odpowiednich postanowień umownych, wyprowadzenie z konstrukcji należytej staranności zobowiązania wykonawcy do zapewniania w systemie informatycznym konkretnych funkcjonalności czy rozwiązań w zakresie cyberbezpieczeństwa jest niezwykle trudne.

[1] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2020 r., poz. 1740).

Strony mogą jednak za pomocą odpowiednich postanowień umowy zmodyfikować czy skonkretyzować kryterium należytej staranności wynikające z art. 355 § 2 k.c., zwłaszcza poprzez:

- dokładne określenie, jakie środki i cele powinien uwzględnić wykonawca w toku realizacji umowy – tym samym, aby zapewnić sobie odpowiedni poziom bezpieczeństwa, zamawiający może wprost opisać w umowie swoje wymagania w zakresie cyberbezpieczeństwa, w tym również konieczne do zastosowania przez wykonawcę techniczne sposoby zapewnienia bezpieczeństwa informacji, uwzględniające wymogi i priorytety danej organizacji, a także ewentualne dodatkowe wymagania, które mogą wynikać z przepisów szczególnych (np. z ustawy o krajowym systemie cyberbezpieczeństwa) czy z wytycznych lub rekomendacji organów nadzoru w przypadku uczestników rynków regulowanych;
- odwołanie się do konkretnych norm i standardów z zakresu cyberbezpieczeństwa, takich jak np. normy ISO (np. PN-EN ISO/IEC 27001 czy PN-EN ISO/IEC 27002), standardy amerykańskiego National Institute of Standards and Technology (NIST, np. Technical Guide to Information Security Testing and Assessment – 800–115), wytyczne sektorowe (np. opublikowana przez Komisję Nadzoru Finansowego Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach) czy inne szczegółowe standardy oraz normy;
- zobowiązanie wykonawcy do przedstawienia odpowiednich certyfikatów z zakresu cyberbezpieczeństwa posiadanych przez jego personel (np. CISSP).

Pozwoli to na jasne ustalenie zakresu obowiązków wykonawcy oraz jego odpowiedzialności za zapewnienie bezpieczeństwa dostarczanego systemu.

Odpowiedzialność wykonawcy

Naruszenie obowiązków w zakresie odpowiedniego zabezpieczenia wdrażanego systemu może z kolei świadczyć o nienależytym wykonaniu umowy przez wykonawcę. Z perspektywy zamawiającego istotne jest to, żeby na gruncie umowy wykonawca ponosił odpowiedzialność nie tylko za konkretne szkody poniesione w związku z włamaniem do systemu czy wyciekiem informacji, lecz także za sam brak zapewnienia odpowiednich zabezpieczeń systemu, co może potencjalnie skutkować wystąpieniem incydentów bezpieczeństwa. Innymi słowy, wykonawca nie powinien odpowiadać tylko wtedy, gdy zaistnieje konkretny skutek, a umowa powinna przewidywać mechanizmy, które pozwolą do tego skutku nie dopuścić (por. wykonanie zastępcze, opisane niżej). Często bowiem ma miejsce sytuacja, w której istnieje luka bezpieczeństwa lub nawet doszło do naruszenia zabezpieczeń systemu, jednak sama szkoda jeszcze nie powstała. W takim wypadku, jeśli umowa tej kwestii nie zabezpiecza, zamawiający nie ma możliwości domagania się naprawienia szkody od wykonawcy, mimo że podatność bezpieczeństwa istnieje i grozi zamawiającemu bardzo poważnymi konsekwencjami, także na gruncie przepisów dot. ochrony danych osobowych. Z tych powodów kluczowe staje się np. ustalenie, że w ramach gwarancji na system wykonawca ma obowiązek usuwania wad i błędów systemu, które stanowią luki i podatności – niezależnie od tego, czy zaistniał skutek w postaci wycieku danych, czy dostępu osób nieuprawnionych.

Testy penetracyjne

Do ujawnienia podatności systemu najczęściej dochodzi w rezultacie próby przełamania zabezpieczeń przez osoby trzecie – cyberprzestępców, którzy wykorzystują te podatności dla własnych celów, lub tzw. whistleblowerów, którzy informują właściciela systemu o nieprawidłowościach. Niemniej z uwagi na duże ryzyko związane z wykorzystaniem przez osoby trzecie luk w zabezpieczeniach zamawiający sam może dążyć do jak najwcześniejszego ich wykrycia, np. przeprowadzając odpowiednie testy systemu – zarówno w ramach procedury odbiorowej systemu, jak i już po wdrożeniu, np. w okresie gwarancji (tak, aby sprawdzić zabezpieczenia systemu IT na środowisku produkcyjnym – zasymulować atak hakera). Samo zobowiązanie w umowie wykonawcy do uwzględnienia odpowiednich rozwiązań, standardów czy norm z zakresu cyberbezpieczeństwa nie gwarantuje bowiem jeszcze ich spełnienia i nie zabezpiecza zamawiającego.

W tym kontekście zamawiający może przeprowadzić testy penetracyjne systemu IT. Wskazane jest jednak, żeby zostały one przeprowadzone przez podmiot trzeci, niezależny od stron umowy i zawodowo zajmujący się działalnością w zakresie cyberbezpieczeństwa. Koszty zlecenia przeprowadzenia takich testów mogą być wysokie, dlatego też istotne jest

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

określenie na gruncie umowy strony zobowiązanej do ich pokrycia – jak również zobowiązanie wykonawcy do wdrożenia zaleceń po przeprowadzonych testach lub usunięcia wykrytych luk i podatności systemu. Należy mieć na uwadze, że przeprowadzenie testów penetracyjnych wiąże się zazwyczaj z koniecznością ingerencji w system informatyczny (np. będzie wymagało jego czasowego zwielokrotnienia), co może być sprzeczne z warunkami licencji udzielonej zamawiającemu. Przed zleceniem testów penetracyjnych zamawiający powinien się zatem upewnić, że postanowienia licencyjne nie zabraniają mu przeprowadzenia takich testów oraz że umowa uprawnia go do udostępnienia audytorowi systemu, w zakresie niezbędnym do wykonania testów penetracyjnych.

Warto również pamiętać, aby zawrzeć z audytorem odpowiednią umowę – jako projekt wyjściowy, do dostosowania do konkretnego stanu faktycznego, można wykorzystać wzór przygotowany na potrzeby wystąpienia mec. Agnieszki Wachowskiej pt. „Jak kupować usługi z zakresu cyberbezpieczeństwa i jakie umowy zawierać?" w ramach XIII Forum Bezpieczeństwa i Audytu IT Semafor. Wzór umowy jest dostępny do pobrania tutaj: link.

Wykonanie zastępcze w umowie IT

Wykrycie luk bezpieczeństwa lub podatności we wdrożonym systemie IT (zarówno na skutek incydentu, jak i w ramach audytu czy testów penetracyjnych) może powodować, że dalsze korzystanie z systemu obarczone jest dużym ryzykiem. Luki i podatności grożą często wyciekiem niezwykle istotnych z perspektywy zamawiającego danych – zarówno danych osobowych, jak i informacji stanowiących tajemnicę przedsiębiorstwa. Jeśli umowa przewiduje odpowiednie mechanizmy pozwalające wymagać od wykonawcy usunięcia tych luk i podatności, a mimo to wykonawca odmawia zrealizowania tych zobowiązań (np. kwestionując raport z testów lub swoją odpowiedzialność), zamawiający może rozważyć skorzystanie z wykonania zastępczego i zlecić usunięcie wykrytych luk i podatności bezpieczeństwa podmiotowi trzeciemu.

Możliwość taką, bez konieczności wcześniejszego uzyskiwania upoważnienia sądu, przewiduje sam Kodeks cywilny w art. 480 § 3 k.c., jednak wyłącznie w wypadkach nagłych. Warto w tym miejscu wskazać, że orzecznictwo sądów powszechnych dosyć niejednolicie podchodzi do interpretacji pojęcia „wypadków nagłych". W niektórych wyrokach sądy stosunkowo szeroko traktują to pojęcie, wskazując przykładowo, że niepospr zątanie przez wykonawcę hali produkcyjnej kosmetyków po ukończeniu prac naprawczych – co uniemożliwia prowadzenie na jej obszarze produkcji ze względu na wymogi czystości – uzasadnia zastosowanie wykonania zastępczego na podstawie art. 480 § 3 k.c.[3], natomiast w innych przyjmują np., że perspektywa wielomilionowych kar oraz utraty kredytu bankowego finansującego budowę nie spełnia przesłanek z art. 480 § 3 k.c.[4]

Z tego też powodu, aby uniknąć wszelkich wątpliwości i zapewnić sobie skuteczny instrument w postaci możliwości wykonania zastępczego w razie wystąpienia incydentów bezpieczeństwa w systemie informatycznym, zamawiający powinien rozważyć, czy takie uprawnienie szczegółowo uregulować na gruncie samej umowy, dookreślając procedurę i przesłanki skorzystania z zastępczego wykonania. Warto również pamiętać, że w praktyce wykonanie zastępcze nie będzie możliwe, jeżeli zamawiający nie dysponuje kodem źródłowym systemu lub gdy w umowie brakuje postanowień licencyjnych uprawniających zamawiającego do ingerencji w ten kod źródłowy. W takiej sytuacji podmiot trzeci, któremu zamawiający zamierza zlecić zastępcze wykonanie prac, nie będzie dysponował ani prawną podstawą do dokonania modyfikacji, ani faktyczną możliwością ich wprowadzenia.

Więcej o możliwości zastosowania wykonania zastępczego w umowach IT pisaliśmy również na naszym blogu.

Podsumowanie

Problematyka cyberbezpieczeństwa jest z perspektywy umów wdrożeniowych niezwykle istotna – dla możliwości kompleksowego i bezpiecznego wykorzystania wdrożonego systemu trzeba zagwarantować, że został on odpowiednio zabezpieczony przed nieuprawnionym dostępem osób trzecich i atakami cyberprzestępców. W przeciwnym wypadku korzystanie z systemu może doprowadzić do wycieków danych, które będą skutkować dla zamawiającego bardzo poważnymi szkodami, zarówno majątkowymi, jak i wizerunkowymi.

Z tego powodu wymagania bezpieczeństwa przy wdrożeniach powinno się traktować równie istotnie, co wymagania funkcjonalne systemu.

Jednocześnie warto pamiętać o wprowadzeniu do umowy wdrożeniowej postanowień, które wyznaczą zakres odpowiedzialności wykonawcy za bezpieczeństwo systemu oraz umożliwią zamawiającemu szybką reakcję na ewentualne incydenty. Pozwoli to na zabezpieczenie interesów zamawiającego oraz zapewni możliwość minimalizacji strat na wypadek ewentualnego wykorzystania luk bezpieczeństwa systemu przez nieuprawnione osoby trzecie.

[3] Zob. wyrok Sądu Okręgowego w Szczecinie z dnia 16 listopada 2018 r., sygn. VIII GC 425/16.
[4] Zob. wyrok Sądu Apelacyjnego w Białymstoku z dnia 8 października 2018 r., sygn. I AGa 110/18.

Oprogramowanie jako produkt podwójnego zastosowania (dual-use item)

r.pr. Magdalena Gąsowska-Paprota

Produkty podwójnego zastosowania, określane również angielskim terminem *dual-use*, to produkty mogące mieć zastosowanie zarówno cywilne, jak i wojskowe. Z tego powodu mają one znaczenie strategiczne dla bezpieczeństwa państwa. W przypadku obrotu takimi towarami z zagranicą podlegają one kontroli, która wiąże się z koniecznością m.in. uzyskania zezwolenia na ich wywóz za granicę, zgłaszania dokonywania ich importu lub z innymi obowiązkami, jak wewnętrzna ewidencja oraz coroczne obowiązki raportowe, które są zależne od konkretnego rodzaju produktu oraz kraju, z którym następuje obrót danym towarem *dual-use*.

Produkty *dual-use* są najczęściej kojarzone z bronią, w tym np. z technologiami nuklearnymi, tymczasem zgodnie z przepisami prawa m.in. oprogramowanie może stanowić produkt podwójnego zastosowania – i to takie, które nie ma z pozoru nic wspólnego z obronnością czy technologiami wojennymi.

Co ważne, podmiot chcący prowadzić import lub eksport oprogramowania stanowiącego produkt podwójnego zastosowania ma obowiązek sam dokonać oceny produktu pod kątem jego ewentualnego zaklasyfikowania jako produkt *dual-use*, a w przypadku pozytywnego wyniku takiej ewaluacji – wypełniać dalsze obowiązki z tym związane, pod groźbą sankcji m.in. karnych.

Przepisy dotyczące zasad eksportu i importu produktów podwójnego zastosowania zawiera unijne Rozporządzenie Rady (WE) nr 428/2009 z dnia 5 maja 2009 r. ustanawiające wspólnotowy system kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania (wersja przekształcona)[1]. W Rozporządzeniu ustanowiono obszerną klasyfikację produktów podwójnego zastosowania, która jest zresztą zbieżna m.in. z amerykańską klasyfikacją tych produktów, i to do niej w pierwszej kolejności należy sięgnąć, chcąc dokonać oceny, czy dany produkt będzie miał charakter *dual-use*. Dodatkowe krajowe regulacje w tym zakresie ustanawia ponadto polska Ustawa z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa[2].

Główną cechą danego oprogramowania, która może spowodować jego klasyfikację jako produktu podwójnego zastosowania, może być fakt realizowania przez oprogramowanie funkcji kryptograficznej, czyli szyfrującej, dla ochrony informacji, nawet jako pobocznej w stosunku do głównego zastosowania oprogramowania.

Producenci oprogramowania realizującego funkcje szyfrujące eksportujący je za granicę lub podmioty importujące takie oprogramowanie do Polski powinni mieć na uwadze, czy ich produkt posługuje się protokołem szyfrującym o symetrycznej długości klucza przekraczającej 56 bitów lub równoważnej (przy czym znaczna część powszechnie stosowanych protokołów przekracza tę długość klucza). Jeżeli tak, to oprogramowanie może być objęte kontrolą obrotu jako produkt *dual-use*, chyba że podlega określonym w Rozporządzeniu wyłączeniom, w szczególności wynikającym z tzw. uwagi kryptograficznej. Dotyczy ona produktów software'owych, które można

[1] Dz. U. UE. L. z 2009 r. Nr 134, str. 1, z późn. zm.; dalej: „Rozporządzenie".
[2] T.j. Dz. U. z 2020 r., poz. 509.

ogólnie określić jako oprogramowanie zamknięte dostępne w masowej sprzedaży i proste w obsłudze – muszą one bowiem spełniać łącznie szereg kryteriów, takich jak: szeroki krąg nabywców, powszechna dostępność w punktach sprzedaży detalicznej, możliwość samodzielnej instalacji, brak możliwości modyfikowania funkcji kryptograficznej. Ocena spełnienia ww. cech musi być dokonywana dla każdego konkretnego przypadku i nie istnieje powszechnie dostępny wykaz, z którego można by się dowiedzieć, jakie produkty zostały zaklasyfikowane jako *dual-use items*, a jakie nie.

Jeżeli zaś nawet okaże się, że dane oprogramowanie podlega klasyfikacji produktów podwójnego zastosowania i nie może być z niej wyłączone na powyższych zasadach, nie jest to jeszcze jednoznaczne z koniecznością uzyskania pozwolenia na eksport. Wszystko zależy od kraju przeznaczenia takiego produktu – jeżeli jest to bowiem kraj członkowski UE lub kraj z grupy objętej tzw. zezwoleniem generalnym wynikającym z Rozporządzenia (m.in. USA, Kanada, Szwajcaria, Japonia, od początku 2021 r. również Wielka Brytania), uzyskanie zezwolenia na eksport nie będzie potrzebne. Niezależnie od tego konieczne może być jednak spełnienie szeregu innych obowiązków, takich jak: pozyskiwanie oświadczenia użytkownika końcowego oprogramowania o treści wymaganej przepisami, prowadzenie wewnętrznej ewidencji obrotu produktem podwójnego zastosowania czy przekazywanie corocznej informacji o tym obrocie organowi kontroli. W Polsce organem kontroli obrotu produktami podwójnego zastosowania jest obecnie Ministerstwo Rozwoju, Pracy i Technologii, natomiast organem monitorowania tego obrotu – ABW.

W razie wątpliwości co do zaistnienia lub zakresu obowiązków związanych z możliwością dokonania obrotu oprogramowaniem jako produktem *dual-use* warto zasięgnąć specjalistycznej porady w tym zakresie, aby nie narażać na odpowiedzialność wynikającą z przepisów siebie ani swojej organizacji.

Czas pracy a branża IT

r.pr. Joanna Jastrząb, r.pr. Wojciech Bigaj, adw. Paweł Krzykowski

Specyfika branży IT a czas pracy

Praca w branży IT kojarzy się często z elastycznym podejściem, zarówno jeśli chodzi o miejsce, jak i czas jej wykonywania. Niemniej jednak, w pewnych sytuacjach, w interesie pracodawcy będzie pozostawać uregulowanie zwłaszcza czasu pracy w sposób ściśle określony, z racji np. na specyfikę jego działalności. Przykładowo, następujące sytuacje mogą wymagać pracy w określonych godzinach:

- całodobowe usługi z zakresu obsługi incydentów cyberbezpieczeństwa w ramach *security operations center* (SOC);
- współpraca z podmiotami z innej strefy czasowej;
- usługi serwisowe systemów świadczone w modelu 24/7;
- prace w ramach wdrożeń systemów lub usług serwisowych, które sporadycznie wymagają pozostawania w gotowości poza godzinami pracy.

Jeśli pracodawca z branży IT podejmuje stałą współpracę z osobą prowadzącą jednoosobową działalność gospodarczą, powyższe kwestie może w prosty i konkretny sposób uregulować w łączącej strony umowie, zgodnie z zasadą swobody umów (3531 k.c.). Analogicznie podejść należy do osób współpracujących na podstawie umowy zlecenia. W przypadku osób zatrudnionych na podstawie umowy o pracę, pracodawca nie dysponuje taką swobodą – musi wziąć pod uwagę przepisy prawa pracy i odpowiednio wdrożyć wskazane kwestie w wewnętrznych regulacjach. Poniżej przedstawiamy podstawowe zasady w tym zakresie.

Organizacja czasu pracy

Do pracowników z branży IT mogą mieć zastosowanie takie same systemy czasu pracy jak w innych branżach, tj. podstawowy system czasu pracy, system równoważnego czasu pracy i zadaniowy system czasu pracy (w przypadkach uzasadnionych rodzajem pracy lub jej organizacją albo miejscem wykonywania pracy). Zadaniowy system czasu pracy oznacza dla pracodawcy mniej obowiązków w zakresie ewidencjonowania czasu pracy, ale nie całkowite zwolnienie z prowadzenia takiej ewidencji – nie ewidencjonuje się bowiem wyłącznie godzin pracy w danym dniu.

Warto również dodać, że pracownicy branży IT mogą zostać objęci pracą zmianową, przez którą należy rozumieć wykonywanie pracy według ustalonego rozkładu czasu pracy przewidującego zmianę pory wykonywania pracy przez poszczególnych pracowników po upływie określonej liczby godzin, dni lub tygodni. Praca zmianowa okaże się nieodzowna zwłaszcza, kiedy konieczne jest zapewnienie całodobowego supportu systemu.

Niemniej jednak, eksperci w zakresie czasu pracy podkreślają jednakże, że nie jest możliwe wykonywanie pracy zmianowej w ramach zadaniowego systemu czasu pracy, ponieważ ten system zakłada duży stopień samodzielności pracownika w zakresie organizacji czasu pracy. Pracę zmianową pracodawca może wprowadzić w układzie zbiorowym pracy, regulaminie pracy lub obwieszczeniu.

Nadgodziny i dodatki

Praca ponad obowiązujące pracownika normy czasu pracy lub przedłużony dobowy wymiar czasy pracy (w systemie równoważnym) będzie stanowić nadgodziny (w Kodeksie pracy zwanymi godzinami nadliczbowymi). Z perspektywy branży IT, będą one dopuszczalne w razie konieczności usunięcia awarii bądź w przypadku szczególnych potrzeb pracodawcy (art. 151 § 1 k.p). Te potrzeby rozumiane są jednak szeroko i mogą objąć np. sytuacje, kiedy praca w godzinach nadliczbowych jest konieczna aby dotrzymać terminów uzgodnionych z kontrahentami, np. w zakresie wdrożenia systemu.

Kodeks pracy w art. 151(1) przewiduje rekompensatę za nadgodziny w postaci dodatku w wysokości 100% wynagrodzenia (praca w nocy, w dni wolne lub niedziele i święta) lub 50% wynagrodzenia (pozostałe sytuacje) za każdą godzinę takiej pracy. Alternatywnie, zamiast dodatku, pracodawca może udzielić pracownikowi czasu wolnego w wymiarze godzin nadliczbowych. Wbrew przyjętemu przekonaniu, czas wolny udzielany jest nie tylko na wniosek pracownika –

inicjatywa może wyjść również ze strony pracodawcy. Wiązać się to będzie jednak ze zwiększonym wymiarem czasu wolnego – musi on być o połowę wyższy niż liczba przepracowanych godzin nadliczbowych. Natomiast to zawsze pracodawca decyduje o sposobie rekompensaty pracy w godzinach nadliczbowych a nie pracownicy.

Warto przy tym pamiętać, że powyższe nie obowiązuje w przypadku pracowników zarządzających w imieniu pracodawcy zakładem pracy lub kierowników wyodrębnionych komórek organizacyjnych – co do zasady muszą oni wykonywać pracę poza ustalonymi godzinami bez prawa do dodatku czy czasu wolnego (art. 151(4) k.p.). Aby nie powstały wątpliwości których ze stanowisk pracy dotyczy ten obowiązek u konkretnego pracodawcy, warto dookreślić to w wewnętrznych regulacjach.

Zasady pełnienia dyżurów

W niektórych przypadkach pracodawca będzie oczekiwać nie tyle ciągłego świadczenia pracy poza przyjętymi godzinami, ile pozostawania w gotowości do jej świadczenia – na wypadek zaistnienia potrzeby wykonania określonych zadań. W takich sytuacjach, może zobowiązać pracownika do pełnienia dyżuru.

Warto przy tym pamiętać, że pracownik nie może odmówić pozostawania na dyżurze, jeśli w jego ramach ma wykonywać zadania wynikające ze stosunku pracy, czyli z zajmowanego stanowiska. Taka praca nie może jednak naruszać prawa pracownika do odpoczynku, czyli prawa do co najmniej:

- 11 godzin nieprzerwanego odpoczynku w każdej dobie pracowniczej;
- 35 godzin nieprzerwanego odpoczynku w każdym tygodniu rozliczeniowym.

Regulacja Kodeksu pracy (art. 151(5) k.p.) określa ponadto, że za czas dyżuru, z wyjątkiem dyżuru pełnionego w domu, pracownikowi przysługuje czas wolny od pracy w wymiarze odpowiadającym długości dyżuru, a w razie braku możliwości udzielenia czasu wolnego wynagrodzenie wynikające z jego osobistego zaszeregowania, określonego stawką godzinową lub miesięczną. Powyższe oznacza więc, że za dyżury domowe, czyli w miejscu niewyznaczonym przez pracodawcę, kompensata czasem wolnym lub wynagrodzeniem nie przysługuje, chyba że pracownik w czasie dyżuru był zmuszony pracę wykonywać i wtedy – jeżeli pracował wcześniej w danej dobie pracowniczej – będzie to zazwyczaj praca w nadgodzinach.

Podsumowanie

Przytoczone powyżej w zarysie regulacje Kodeksu pracy określają pewne ramy, które powinny zostać dookreślone w wewnętrznych regulacjach przyjętych przez danego pracodawcę, takich jak polityki czy regulaminy. Mogą one okazać się przydatne zwłaszcza w kwestiach operacyjnych (np. w przypadku dyżurów, mogą określać sposoby komunikacji, czas przystąpienia do realizacji zgłoszonych w ramach dyżuru zadań) lub w sytuacji gdy pracodawca będzie chciał korzystniej uregulować niektóre z kwestii, niż zakłada Kodeks pracy (np. przyznać wynagrodzenie także za dyżur w domu). W każdym z tych przypadków, warto jednak zadbać aby przyjęte regulacje były spójne i zgodne z przepisami prawa pracy.

Zagadnienia prawne i praktyczne stosowania kwalifikowanego podpisu elektronicznego

r.pr. Magdalena Gąsowska-Paprota

Kontynuując pojawiający się w naszym newsletterze oraz na blogu TKP wątek digitalizacji w obrocie gospodarczym – wiążącej się ze zjawiskiem *paperless*, którego jednym z istotnych elementów jest wykorzystanie kwalifikowanego podpisu elektronicznego – prezentujemy kolejne zagadnienia prawne i praktyczne, istotne z punktu widzenia stosowania kwalifikowanego podpisu elektronicznego oraz innych związanych z nim usług zaufania.

Archiwizacja dokumentów podpisanych w formie elektronicznej

Archiwizowanie dokumentów (np. umów), które zostały podpisane w formie elektronicznej, tj. poprzez opatrzenie pliku zawierającego dokument kwalifikowanym podpisem elektronicznym – najczęściej poprzez zastosowanie formatu PAdES lub XAdES – musi się odbywać również w formie elektronicznej, poprzez cyfrowe zapisanie pliku. Tylko w tej formie bowiem plik opatrzony kwalifikowanym podpisem elektronicznym zachowuje cechy oryginalności, a kwalifikowany podpis elektroniczny może zostać zweryfikowany.

W praktyce wciąż się zdarza, że w związku z brakiem posiadania przez jedną ze stron umowy kwalifikowanego certyfikatu podpisu elektronicznego konieczne jest złożenie przez taką osobę podpisu własnoręcznego na umowie, podczas gdy druga strona podpisuje ją w formie elektronicznej. Taka procedura – tj. wymienienie się przez strony dokumentami podpisanymi przez jedną stronę kwalifikowanym podpisem elektronicznym, a przez drugą podpisem własnoręcznym – jest możliwa i będzie prowadzić do prawidłowego i ważnego zawarcia umowy (pod warunkiem, że treść wzajemnie przekazywanych dokumentów jest identyczna). W archiwizowaniu tak zawartej umowy istotne jest natomiast, by przechowywane były przez stronę umowy oba jej egzemplarze, na potrzeby odtworzenia zgodnych oświadczeń woli stron – zarówno egzemplarz papierowy podpisany własnoręcznie, jak i egzemplarz cyfrowy podpisany kwalifikowanym podpisem elektronicznym.

W archiwizacji dokumentów opatrzonych kwalifikowanym podpisem elektronicznym ważne jest zadbanie o możliwość wykazania prawidłowości podpisu pomimo upływu czasu, o czym poniżej.

Moc prawną daty pewnej w rozumieniu Kodeksu cywilnego ma natomiast kwalifikowany elektroniczny znacznik czasu[1], który stanowi odrębny rodzaj usługi zaufania[2] i który można dodatkowo nanieść na dokument wraz z kwalifikowanym podpisem elektronicznym. Kwalifikowany elektroniczny znacznik czasu warto wykorzystywać nie tylko wtedy, gdy dla danej czynności prawnej wymagana jest forma z datą pewną, lecz jako standard przy składaniu kwalifikowanego podpisu elektronicznego. Ułatwia to np. walidację kwalifikowanego podpisu elektronicznego również w czasie, gdy kwalifikowany certyfikat już wygasł (pomimo że dla ważności kwalifikowanego podpisu elektronicznego istotne jest, aby certyfikat był ważny w momencie złożenia podpisu – nie ma zaś znaczenia późniejsza utrata ważności certyfikatu – to po jego wygaśnięciu walidowanie kwalifikowanego podpisu elektronicznego jest w praktyce utrudnione).

Walidacja kwalifikowanego podpisu elektronicznego

Przed praktycznymi problemami z walidacją kwalifikowanego podpisu elektronicznego dokonywaną po wygaśnięciu ważności certyfikatu można się również ustrzec poprzez skorzystanie z usługi kwalifikowanej walidacji, wykonanej w czasie ważności certyfikatu. Kwalifikowana walidacja kwalifikowanego podpisu elektronicznego polega na weryfikacji i potwierdzeniu prawidłowości podpisu przez dostawcę usług zaufania – korzystającemu z usługi przekazywany jest raport z walidacji, który powinno się zarchiwizować wraz z podpisanym dokumentem. Powyższe daje najlepszą gwarancję „trwałości" kwalifikowanego podpisu elektronicznego, rozumianej jako możliwość wykazania prawidłowości pomimo upływu czasu, również na potrzeby dowodowe w postępowaniu przed sądami czy organami administracji. Jednocześnie w praktyce obrotu – w szczególności w przypadkach gdy przechowywanie dokumentów podpisanych kwalifikowanym podpisem elektronicznym przez dłuższy czas nie jest istotne – możliwe jest posłużenie się jedynie „zwykłą" walidacją kwalifikowanego podpisu elektronicznego, co polega na skorzystaniu z powszechnie dostępnego i bezpłatnego oprogramowania do tego przeznaczonego (podczas gdy kwalifikowana walidacja jest usługą płatną).

[1] Zgodnie z art. 81 § 2 pkt 3 Ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2020 r. poz. 1740).
[2] Zob. art. 41, 42 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. U. UE. L. z 2014 r. Nr 257, str. 73).

Wyroki WSA: Nie ma obowiązku prowadzenia ewidencji IP BOX na bieżąco

r.pr. Joanna Jastrząb, Dominika Duda

Zainteresowanych tematyką IP Box i innych warunków do skorzystania z tej stawki podatku dochodowego zapraszamy na nasz blog – artykuł dostępny jest pod tym linkiem.

Przepisy regulujące preferencyjną 5-proc. stawkę podatku dochodowego, nazywaną potocznie „IP Box", obowiązują już prawie 2 lata, ale dopiero teraz rozstrzyga się jedna z kluczowych kwestii dotyczących warunków jej zastosowania. Chodzi o obowiązek prowadzenia odrębnej ewidencji zdarzeń gospodarczych, w ramach tzw. obowiązku dokumentacyjnego, obejmującej wszystkie operacje finansowe związane z dochodami z działalności podlegającej IP Box[1].

Przepisy i stanowisko Dyrektora KIS

Regulacje prawne dotyczące IP Box są niejasne i z racji swojej ogólności wywołały pewne kontrowersje. Również opublikowane przez Ministerstwo Finansów objaśnienia podatkowe dotyczące tej ulgi nie rozwiały powstałych wątpliwości[2]. Jedną z nich jest obowiązek prowadzenia odrębnej ewidencji zdarzeń gospodarczych – nie było bowiem jasne, czy należy prowadzić ją na bieżąco, czy też podatnik może sporządzić ją dopiero po zakończeniu danego roku podatkowego, przy okazji składania zeznania podatkowego za ten rok.

Na powyższe pytanie odpowiedział Dyrektor Krajowej Informacji Skarbowej (dalej: „Dyrektor KIS") w wydawanych indywidualnych interpretacjach podatkowych. W odpowiedzi na pytania wnioskodawców – podatników – stwierdził jednoznacznie, że ewidencję należy prowadzić na bieżąco. Stanowisko to powtarzał jednolicie, uzasadniając je np. w następujący sposób: „Fakt sporządzenia (przedstawienia czy posiadania) w przyszłości odrębnej ewidencji dopiero na potrzeby skorzystania z IP Box nie wypełnia przesłanki z art. 30cb ust. 1 i 2 ustawy o podatku dochodowym od osób fizycznych. Stworzenie w przyszłości odrębnej ewidencji tylko po to, aby wypełnić obowiązek wynikający z powołanego przepisu, nawet w sytuacji, kiedy na jej podstawie możliwe będzie prawidłowe określenie podstawy opodatkowania stawką 5%, uniemożliwia zastosowanie preferencyjnej stawki opodatkowania uzyskiwanych dochodów"[3].

Wyroki wojewódzkich sądów administracyjnych

Z uwagi na taką wykładnię przepisów prezentowaną przez Dyrektora KIS wielu podatników nie zdecydowało się na rozliczenie ulgi IP Box za 2019 r. i zapłaciło podatek dochodowy z uwzględnieniem wyższych stawek. Niektórzy z nich nie zgodzili się jednak z tym stanowiskiem i odwołali się do sądów administracyjnych. Warto odnotować, że w dwóch znanych nam wyrokach sądy przyznały rację podatnikom i zakwestionowały stanowisko Dyrektora KIS.

Wojewódzki Sąd Administracyjny w Gorzowie Wielkopolskim w wyroku z lipca br.[4] uznał, że dla celów zastosowania IP Box wystarczające będzie sporządzenie odrębnej ewidencji na potrzeby rocznego rozliczenia i nie jest obowiązkiem przedsiębiorcy prowadzenie jej na bieżąco. Sąd zasadniczo wyraził dezaprobatę dla przyjętej przez Dyrektora KIS restrykcyjnej interpretacji i stwierdził, że przytoczone wyżej stanowisko dotyczące wykładni przepisów „jest zbyt daleko

[1] Art. 24e ust. 1 pkt 1 Ustawy z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych (dalej: „Ustawa CIT") i art. 30cb ust. 1 pkt 1 Ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (dalej: „Ustawa PIT").
[2] Zob. https://www.gov.pl/web/finanse/objasnienia-podatkowe-dot-preferencyjnego-opodatkowania-dochodow-wytwarzanych-przez-prawa-wlasnosci-intelektualnej-ip-box (dostęp: 3.11.2020).
[3] Indywidualna interpretacja podatkowa z dnia 7 stycznia 2020 r. wydana przez Dyrektora Krajowej Informacji Skarbowej, sygn. 0113-KDIPT2-3.4011.589.2019.2.SJ.
[4] Zob. wyrok WSA z dnia 30 lipca 2020 r. o sygn. akt I SA/Go 115/20 w Gorzowie Wielkopolskim.

idące, a przez to nieprawidłowe". Zwrócił przy tym uwagę, że „ewidencja ma być prowadzona w sposób należyty tak, aby móc w rocznym zeznaniu podatkowym wykazać łączną sumę przychodów, kosztów podatkowych, dochodów, strat, dochodów podlegających opodatkowaniu stawką 5% oraz dochodu, który nie będzie podlegał preferencyjnemu opodatkowaniu". Skutek taki można osiągnąć również wtedy, gdy ewidencja nie będzie prowadzona na bieżąco.

Taką samą interpretację przepisów przyjął Wojewódzki Sąd Administracyjny we Wrocławiu w wyroku z sierpnia br.[5]. Sąd uznał, że prowadzenie ewidencji samo w sobie jest konieczne dla zastosowania IP Box, ale „skoro ewidencja umożliwi sporządzenie w terminie deklaracji podatkowej, nie można jej uznać za prowadzoną nieprawidłowo lub niespełniającą przesłanek ustawowych tylko z tego względu, że nie jest prowadzona na bieżąco".

Wyjątek od reguły?

Oba sądy zajęły jasne stanowisko, że z uwagi na roczne rozliczenie IP Box brak prowadzenia ewidencji na bieżąco nie powinien stanowić przeszkody. Warto w tym kontekście wspomnieć o szczególnych regulacjach, których sądy nie analizowały, a które mogą prowadzić do uznania, że konieczne jest prowadzenie ewidencji systematycznie. Chodzi tutaj o szczególną regulację tarczy antykryzysowej[6], która przewiduje, że w wypadku gdy miało miejsce wytworzenie, rozwinięcie lub ulepszenie kwalifikowanego prawa własności intelektualnej, które ma pomóc w przeciwdziałaniu rozprzestrzenianiu się wirusa SARS-CoV-2, z ulgi IP Box można skorzystać nie tylko na koniec danego roku podatkowego, lecz także już w momencie wpłacenia zaliczek na podatek dochodowy – a więc w trakcie roku podatkowego. W tym kontekście uprawnione wydaje się stwierdzenie, że ewidencja powinna być prowadzona regularnie i na bieżąco – wraz ze stosowaniem stawki 5% podatku dochodowego do zaliczek.

Podsumowanie

Przedstawione wyroki nie są jeszcze prawomocne. Wydaje się jednak, że można się spodziewać utrzymania takiej wykładni przepisów przez inne sądy administracyjne. Decydujące znaczenie ma tutaj fakt, że ustawodawca nie zdecydował się uregulować sposobu prowadzenia ewidencji ani częstotliwości wprowadzania w niej wpisów. Skoro więc regulacje podatkowe nie wskazują, że podatnicy powinni prowadzić ewidencję na bieżąco, to nie ma podstaw, aby Dyrektor KIS formułował takie wnioski, niejako uzupełniając obowiązujące przepisy.

Warto zresztą podkreślić, że podobne podejście było prezentowane przez Dyrektora KIS na gruncie innej podatkowej preferencji – 50% kosztów uzyskania przychodu w przypadku dochodów osiąganych na podstawie umowy o pracę. Chociaż przepisy prawa nie wskazywały sposobu dokumentowania wytworzonych utworów ani nie wyznaczały, jak należy określić honorarium autorskie, Dyrektor KIS prezentował w tym zakresie szerokie rozważania, odmawiając prawidłowości niektórym ze sposobów przedstawianych przez płatników lub podatników. Mimo kilkunastu wyroków sądów na korzyść wnioskodawców wątpliwości w tym zakresie rozstrzygnął dopiero Minister Finansów w ogólnej interpretacji podatkowej, o której pisaliśmy w poprzednim wydaniu newslettera (link). Pozostaje mieć nadzieję, że w przypadku IP Box stan niepewności nie potrwa długo, a Dyrektor KIS uwzględni stanowisko sądów administracyjnych w wydawanych interpretacjach indywidualnych.

[5] Zob. wyrok WSA z dnia 26 sierpnia 2020 r. o sygn. akt I SA/Wr 170/20 we Wrocławiu.
[6] Art. 4 oraz art. 6 Ustawy z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw (Dz. U. poz. 568, z późn. zm.).

Zakup komputerów przez zamawiających – pomogą zaktualizowane rekomendacje UZP

r.pr. Tomasz Krzyżanowski

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 zesta-wów komputerowych. Rekomendacje* (2012 r.; dalej: „*Rekomendacje ds. komputerów*") oraz *Udzielanie zamówień publicznych na systemy informatyczne*[1]. Rekomendacje (2009 r.; dalej: „*Rekomendacje ds. systemów*"). O konsultacjach pisaliśmy także w poprzednim wydaniu newslettera (dostępnym tutaj).

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).

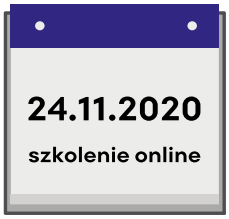
Dokument rekomendacji ma charakter tzw. dobrych praktyk a nie prawa obowiązującego i ma na celu przede wszystkim pomóc instytucjom zamawiającym w jak najlepszym przygotowaniu i przeprowadzeniu postępowań o udzielenie zamówienia publicznego, w tym w jak najlepszym opisaniu przedmiotu zamówienia.

Zakup urządzeń komputerowych wymaga precyzyjnego opisania przedmiotu zamówienia, tak aby z jednej strony uszanować zasadę uczciwej konkurencji, a jednocześnie uwzględnić uzasadnione potrzeby zamawiającego nabycia produktu o określonych parametrach. UZP stworzył nową wersję rekomendacji, które mają pomóc zamawiającym przygotować postępowanie o udzielenie zamówienia w tym zakresie. **W dniu 15 października 2020 r. opublikował nową zaktualizowaną wersję *„Rekomendacji ds. komputerów"*.** Materiał znajduje się na stronie UZP[2]. Nie jest to jednak jeszcze ostateczna treść, gdyż ta zostanie wypracowana w czasie dalszych konsultacji UZP z organizacjami branżowymi, biorąc pod uwagę uwagi zgłoszone w okresie w którym dokument podlegał konsultacjom publicznym.

[1] I tom rekomendacji dotyczących systemów informatycznych jest opublikowany na stronie UZP https://www.uzp.gov.pl/baza-wiedzy/dobre-praktyki/rekomendacje-dotyczace-zamowien-publicznych-na-systemy-informatyczne

[2] https://www.uzp.gov.pl/strona-glowna/slider-aktualnosci/konsultacje-rekomendacje-dotyczace-dostawy-zestawow-komputerowych/konsultacje-rekomendacje-dotyczace-dostawy-zestawow-komputerowych

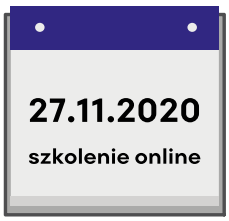
NADCHODZĄCE WYDARZENIA



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

r. pr. Agnieszka Wachowska

Więcej informacji >>



"Nowe Prawo komunikacji elektronicznej – jak przygotować się do nadchodzących zmian?"

Prelekcja pt. "Bezpieczeństwo danych, sieci i usług w prawie telekomunikacyjnym" - adw. Xawery Konarski
Prelekcja pt. "Zmiany w zakresie umów abonenckich, wynikające z Tarczy 3.0" r.pr. Agnieszka Wachowska

Więcej informacji >>

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

r. pr. Agnieszka Wachowska

Więcej informacji >>

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

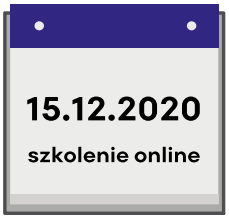
adw. Xawery Konarski, r. pr. Agnieszka Wachowska

Więcej informacji >>

"Praktyczna strona wdrażania rozwiązań chmurowych w sektorze energetycznym i przemyśle"

Prelekcja pt. "Praktyczna strona zagrożeń związanych z wejściem do chmury" - 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

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

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

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

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

Joanna Dworak
Radca prawny, Senior Associate
joanna.dworak@traple.pl

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

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

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

Małgorzata Kotwica
Associate
malgorzata.kotwica@traple.pl

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

Aleksander Elmerych
Junior Associate
aleksander.elmerych@traple.pl

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

Redaktor newslettera:
r.pr. Joanna Jastrząb