NR 6 - GRUDZIEŃ 2021

NEWSLETTER

IT-TECH

W NUMERZE M.IN.:

- Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa
- Ukształtowanie kar umownych w umowie IT – zasada odpowiedzialności
- Co dzieje się z wdrożeniem Europejskiego Kodeksu Łączności Elektronicznej i Prawem Komunikacji Elektronicznej?
- Sztucznie inteligentne wyroby medyczne. Biała księga TÜV SÜD, czyli nowe wytyczne dla branży medtech

Traple
Konarski
Podrecki
& Wspólnicy

TKP

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa

Agnieszka Wachowska, Aleksander Elmerych

Po wielu tygodniach zapowiedzi opublikowany został rządowy projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (dalej: „ustawa KSC")[1]. Częściowo pokrywa się on z projektem nowelizacji ustawy z września ubiegłego roku[2], jednak zawiera również szereg nowych, niepublikowanych wcześniej rozwiązań. Mimo wyznaczenia bardzo krótkiego terminu do projektu ustawy zgłoszonych zostało wiele uwag, pochodzących m.in. od organizacji zrzeszających przedsiębiorców, takich jak Polska Izba Informatyki i Telekomunikacji (PIIT), Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji (KIGEiT) czy Związek Pracodawców Branży Internetowej IAB Polska. Zgodnie z informacjami przekazanymi przez przedstawicieli rządu projekt został skierowany do Komitetu Rady Ministrów do spraw Bezpieczeństwa Narodowego i spraw Obronnych (KRMBNSO).

Tło prac nad nowelizacją ustawy KSC

Inicjatywa związana ze zmianą ustawy KSC pojawiła się już we wrześniu 2020 r., a część rozwiązań zaproponowanych w nowym projekcie ustawy pokrywa się z propozycją ubiegłorocznej nowelizacji. Procedowanie ubiegłorocznego projektu, mimo wielu dyskusji i szeregu przeprowadzonych konsultacji, zostało wstrzymane na etapie prac w Komitecie do Spraw Europejskich. W międzyczasie doszło do opublikowania projektu dyrektywy NIS 2 (szerzej pisaliśmy o nim tutaj), a w debacie publicznej cyberbezpieczeństwo stało się bardzo popularnym tematem, głównie za sprawą ataków cybernetycznych, które miały prowadzić do ujawnienia informacji istotnych z perspektywy funkcjonowania państwa. W świetle powyższych okoliczności zadecydowano o wznowieniu prac nad nowelizacją ustawy KSC i opublikowano propozycję ustawy, która łączy rozwiązania znane z ubiegłorocznego projektu oraz całkowicie nowe przepisy.

Zmiany w zakresie podmiotów podlegających przepisom ustawy KSC

Największą grupę podmiotów podlegających przepisom ustawy KSC stanowią operatorzy usług kluczowych (dalej: „OUK") oraz dostawcy usług cyfrowych (dalej: „DUC"). Zgodnie z założeniami projektu grupy podmiotów mogących stanowić OUK oraz DUC nie będą objęte znaczącymi zmianami. Istotną proponowaną zmianą jest natomiast włączenie do krajowego systemu cyberbezpieczeństwa przedsiębiorców telekomunikacyjnych, którzy byli z niego dotychczas całkowicie wyłączeni. Warto nadmienić, że przedsiębiorcy telekomunikacyjni mają podlegać przepisom ustawy KSC jedynie w ograniczonym zakresie (który został sformułowany w bardzo ogólny i nieprecyzyjny sposób) i tylko w sytuacji, gdy będą jednocześnie należeć do jednej z grup objętych szczególnymi obowiązkami na gruncie przepisów ustawy KSC (m.in. będą stanowić DUC lub OUK). Do krajowego systemu cyberbezpieczeństwa włączono również podmioty takie jak uczelnie wyższe, Urząd Komisji Nadzoru Finansowego czy podmioty świadczące usługi SOC na rzecz OUK.

[1] Zob. projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw z dnia 12 października 2021 r., dostępny pod adresem: https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-zamowien-publicznych.html (dostęp: 30.11.2021).

[2] Zob. projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych z dnia 7 września 2020 r., dostępny pod adresem: https://legislacja.rcl.gov.pl/docs//2/12337950/12716602/12716603/dokument463185.pdf (dostęp: 30.11.2021).

Realizacja obowiązków operatorów usług kluczowych w ramach SOC

Projekt nowelizacji nie wprowadza żadnych rewolucyjnych zmian dotyczących obowiązków podmiotów objętych krajowym systemem cyberbezpieczeństwa. Wprowadzone zmiany dotyczą głównie OUK i związane są ze sposobem realizacji obowiązków tych podmiotów m.in. w ramach zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, prowadzenia dokumentacji cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej czy obsługi i zgłaszania incydentów oraz współpracy w tym zakresie z właściwym CSIRT. Na gruncie obecnie obowiązujących przepisów obowiązki te powinny być wypełniane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub przez podmiot trzeci świadczący usługi z zakresu cyberbezpieczeństwa na podstawie umowy zawartej z takim podmiotem. Nowe przepisy stanowią natomiast, że obowiązki te powinny być wykonywane przez SOC (Security Operations Center – zespół pełniący funkcję operacyjnego centrum bezpieczeństwa), przy czym nadal SOC może zostać powołany w ramach wewnętrznej struktury organizacyjnej OUK albo funkcję SOC może pełnić podmiot zewnętrzny, działający na podstawie umowy lub powołany dla danego OUK przez podmiot nadzorujący.

Nowym rozwiązaniem jest natomiast wprowadzenie wymogu wyboru prawa polskiego jako właściwego dla umowy o prowadzenie SOC czy obowiązku udostępniania przez SOC świadczący usługi na rzecz OUK określonych informacji na swojej stronie internetowej (np. dotyczących wykorzystywanych kluczy publicznych czy stosowanych sposobów szyfrowania komunikacji). Wszystkie podmioty świadczące usługi SOC na rzecz OUK (niezależnie od tego, czy zostały powołane w ramach struktury OUK, czy też stanowią podmioty trzecie) będą również podlegały wpisowi do wykazu SOC prowadzonego przez ministra właściwego do spraw informatyzacji.

Nowe kompetencje ministra właściwego do spraw informatyzacji

Proponowane nowelizacją ustawy KSC zmiany, które budzą największe kontrowersje na rynku, związane są z nowymi kompetencjami przyznanymi ministrowi właściwemu do spraw informatyzacji. W pierwszej kolejności wskazać należy na możliwość przeprowadzenia **postępowania w sprawie uznania** za dostawcę wysokiego ryzyka, które może zakończyć się wydaniem decyzji administracyjnej uznającej dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka w przypadku stwierdzenia, że dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego czy życia lub zdrowia ludzi. Konsekwencją wydania takiej decyzji jest uniemożliwienie podmiotom szczególnie narażonym na cyberzagrożenia (m.in. wszystkim podmiotom objętym krajowym systemem cyberbezpieczeństwa, w tym DUC i OUK oraz przedsiębiorcom telekomunikacyjnym) korzystania z produktów, usług lub procesów objętych taką decyzją oraz zobowiązanie do wycofania ich z użytkowania w ciągu 7 lat, jeśli są obecnie wykorzystywane. Może się to wiązać ze znacznym zmniejszeniem dochodów dostawców, w stosunku do których została wydana decyzja o uznaniu za dostawcę wysokiego ryzyka.

Kolejnym rozwiązaniem, budzącym równie duże kontrowersje, jest kompetencja do wydania polecenia zabezpieczającego w przypadku wystąpienia incydentu krytycznego. Zgodnie z przedstawioną w projekcie propozycją polecenie zabezpieczające ma przybrać postać decyzji administracyjnej i będzie mogło dotyczyć m.in. podmiotów objętych krajowym system cyberbezpieczeństwa (m.in. OUK i DUC), przedsiębiorców telekomunikacyjnych czy przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w ustawie o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców. Polecenie zabezpieczające będzie mogło zawierać nakazy lub zakazy skierowane do jego adresatów, obejmujące przykładowo:

- zakaz korzystania z określonego sprzętu lub oprogramowania;
- nakaz wprowadzenia ograniczenia ruchu sieciowego z adresów IP lub adresów URL wchodzącego do infrastruktury danego podmiotu;
- nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania.

Przepisy dotyczące polecenia zabezpieczającego są krytykowane m.in. za to, że treść polecenia zabezpieczającego ma obejmować jedynie wskazanie „rodzaju podmiotów", do których polecenie to jest skierowane. Określone podmioty mogą zatem nie mieć nawet świadomości, że zostały zobowiązane do danego zachowania w drodze decyzji administracyjnej – natomiast za niezastosowanie się do treści tej decyzji będzie

groziła administracyjna kara pieniężna w wysokości do 3% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Sposób uregulowania obu omówionych powyżej instytucji budzi również szereg wątpliwości co do proponowanych rozwiązań procedury administracyjnej (m.in. w zakresie nadania im rygoru natychmiastowej wykonalności czy pozbawienia możliwości złożenia wniosku o ponowne rozpatrzenie sprawy).

Krajowy system certyfikacji cyberbezpieczeństwa

Propozycja nowelizacji ustawy KSC zakłada również utworzenie krajowego systemu certyfikacji cyberbezpieczeństwa, w ramach którego zostanie opracowany krajowy program certyfikacji cyberbezpieczeństwa. Zgodnie z założeniami dedykowane programy certyfikacji cyberbezpieczeństwa będą mogły zostać opracowane także dla poszczególnych produktów, usług lub procesów ICT, z uwzględnieniem ich specyfiki. W ramach krajowego programu certyfikacji cyberbezpieczeństwa mają zostać wyróżnione trzy poziomy uzasadnienia zaufania (podstawowy, istotny i wysoki) dla produktów, usług i procesów ICT, zróżnicowane pod względem ich odporności na zagrożenia cybernetyczne. Dostawcy będą mogli ubiegać się o certyfikację swoich produktów, usług i procesów ICT, która będzie potwierdzała spełnienie przez nie wymagań dla poszczególnych poziomów uzasadnienia zaufania, opisanych szerzej w krajowym programie certyfikacji cyberbezpieczeństwa. Oceny zgodności z poszczególnymi poziomami uzasadnienia zaufania będą dokonywały jednostki oceniające zgodność nadzorowane przez Polskie Centrum Akredytacji.

Operator strategicznej sieci bezpieczeństwa zapewni obsługę urzędów państwowych

Na podstawie przepisów proponowanych nowelizacją ustawy KSC utworzona ma zostać strategiczna sieć cyberbezpieczeństwa, której głównym zadaniem będzie zapewnienie realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w zakresie telekomunikacji. Zgodnie z założeniami strategiczna sieć cyberbezpieczeństwa ma być wykorzystywana przez jej operatora do świadczenia usług na rzecz najważniejszych urzędów państwowych (m.in. na rzecz Kancelarii Prezydenta, Kancelarii Sejmu i Senatu czy Biura Bezpieczeństwa Narodowego). Z uwagi na warunki, które powinien spełnić operator strategicznej sieci cyberbezpieczeństwa, jako naturalny kandydat do objęcia tej funkcji wskazywana jest spółka Exatel SA. Przepisy projektu zapewniają operatorowi strategicznej sieci cyberbezpieczeństwa szereg narzędzi mających na celu usprawnienie pełnienia powierzonej funkcji, m.in. poprzez przyznanie prawa pierwokupu sieci telekomunikacyjnych będących własnością Skarbu Państwa oraz jednostek samorządu terytorialnego.

Spółka Polskie 5G i przetarg na częstotliwości 5G

Projekt nowelizacji ustawy KSC przewiduje także utworzenie przez operatora strategicznej sieci bezpieczeństwa nowej spółki kapitałowej o nazwie Polskie 5G, której celem ma być realizacja ogólnopolskiej hurtowej sieci 5G. Głównym zadaniem spółki Polskie 5G ma być zapewnienie pokrycia całego terytorium kraju zasięgiem hurtowej sieci 5G oraz hurtowe, odpłatne oferowanie usług telekomunikacyjnych świadczonych z jej użyciem. Akcjonariuszami lub udziałowcami spółki Polskie 5G mają być m.in. operatorzy telekomunikacyjni, którym w drodze przetargu organizowanego przez Prezesa UKE mają zostać przyznane częstotliwości sieci 5G (w zakresach 713–733 MHz oraz 768–788 MHz). Pozostałe częstotliwości sieci 5G (w zakresach 703–713 MHz oraz 758–768 MHz) będą stanowić częstotliwości rządowe i zostaną przyznane przez Prezesa UKE operatorowi strategicznej sieci bezpieczeństwa.

Podsumowanie

Projekt nowelizacji ustawy KSC budzi wiele emocji i kontrowersji, w szczególności ze względu na wprowadzoną procedurę dotyczącą uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka oraz na możliwość wydawania przez ministra właściwego do spraw informatyzacji poleceń zabezpieczających. Wydaje się, że z uwagi na swoją doniosłość projekt powinien podlegać szerszym konsultacjom publicznym. Obecnie nie jest jeszcze znany kształt ostatecznego projektu po zakończonych konsultacjach, który miałby podlegać dalszej ścieżce legislacyjnej. Należy się jednocześnie spodziewać, że ze względu na rosnącą rolę cyberbezpieczeństwa prace nad tym projektem mogą być prowadzone w sposób dynamiczny. Jednocześnie warto nadmienić, że projekt nowelizacji ustawy KSC jest jedynie początkiem działań legislacyjnych ustawodawcy w zakresie cyberbezpieczeństwa – zgodnie z zapowiedziami sekretarza stanu i pełnomocnika ds. cyberbezpieczeństwa w KPRM Janusza Cieszyńskiego zaraz po nowelizacji ustawy KSC zostaną rozpoczęte prace nad ustawą o partnerstwie w cyberbezpieczeństwie. Szczegółowy zakres tej ustawy jest jednak nieznany w momencie publikacji artykułu.

Rekomendacje Ministerstwa Klimatu i Środowiska w zakresie cyberbezpieczeństwa dla sektora energii

Jakub Chlebowski

15 października 2021 r. Ministerstwo Klimatu i Środowiska przedstawiło rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa w sektorze energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów. Rekomendacje, opracowane na podstawie art. 42 ust. 1 pkt 5 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2020 r., poz. 1369), powstały w drodze konsultacji z CSIRT NASK, CSIRT GOV, CSIRT MON oraz z operatorami usług kluczowych sektora energii.

Czego dotyczą rekomendacje?

Rekomendacje wydane przez Ministerstwo Klimatu i Środowiska są zbiorem dobrych praktyk, które powinny zostać wdrożone przez przedsiębiorstwa z branży energetycznej, zwłaszcza przez podmioty mające status operatorów usług kluczowych, aby możliwe było stworzenie kompleksowych reguł dotyczących wielu obszarów organizacji w celu ochrony ich zasobów informatycznych.

Rekomendacje dotyczą m.in. następujących obszarów:

- tworzenie procedur zarządzania ryzykiem;
- korzystanie z usług dostawców;
- podnoszenie świadomości personelu;
- przeprowadzanie audytów bezpieczeństwa;
- zapewnienie ciągłości działania, w szczególności ciągłości działania usług kluczowych;
- bezpieczeństwo fizyczne;
- bezpieczeństwo sieci i systemów informatycznych;
- zasady zgłaszania i obsługi incydentów.

Każda ze sfer opisanych w dokumencie Ministerstwa zawiera rekomendacje uwzględniające specyfikę sektora energii.

Warto mieć na uwadze, że rekomendacje Ministerstwa często nie dają jednoznacznych i jednolitych odpowiedzi na to, jaki sposób zapewnienia odpowiedniego poziomu cyberbezpieczeństwa przez sektor energii jest właściwy. Wiele z tych wytycznych określa przede wszystkim cel, jaki powinien zostać osiągnięty dzięki ich implementacji, lub stanowi założenia, którymi powinny się kierować podmioty z branży energii przy ustalaniu indywidualnych standardów cyberbezpieczeństwa. Podmioty z sektora energii przy określaniu adekwatnych zasad cyberbezpieczeństwa powinny brać pod uwagę indywidualne uwarunkowania, m.in. wykorzystywane systemy, kategorie przetwarzanych informacji, aktualnie występujące zagrożenia czy znaczenie prowadzonej działalności dla bezpieczeństwa narodowego.

W celu wsparcia procesu szacowania ryzyka wystąpienia incydentu cyberbezpieczeństwa w systemach informacyjnych wykorzystywanych do świadczenia usługi kluczowej Ministerstwo jako część rekomendacji opracowało wzór formularza pozwalającego na określenie poziomu dojrzałości organizacji operatora usługi kluczowej w zakresie cyberbezpieczeństwa. Dzięki przeprowadzeniu takiej oceny operator usługi kluczowej może określić minimalną listę wymagań cyberbezpieczeństwa, które powinien spełniać, na poziomie podstawowym, średnim i rozszerzonym.

Znaczenie rekomendacji dla dostawców IT

Najważniejsze z perspektywy dostawców IT świadczących usługi dla podmiotów z sektora energii są wytyczne dotyczące korzystania przez podmioty z sektora energii z usług osób trzecich, w szczególności rekomendacje skupiające się na zagadnieniach, które powinny zostać uwzględnione w umowach z dostawcami IT i przy pomocy których powinny być mitygowane ryzyka cyberbezpieczeństwa. Dodatkowo Ministerstwo zwraca uwagę na konieczność tworzenia przez podmioty z branży energii wewnętrznych regulacji, które pozwolą na lepszy nadzór nad realizacją zadań przez dostawców IT.

Mając na względzie treść rekomendacji, dostawcy IT powinni być przygotowani na to, że podmioty z sektora energii mogą wymagać od nich kontraktowego ukształtowania zasad współpracy w taki sposób, aby spełniać wymogi znajdujące się w rekomendacjach. Może to być m.in. umowne zobowiązanie

się dostawcy IT do realizacji konkretnych obowiązków (np. bieżącej aktualizacji oprogramowania, implementacji „łatek bezpieczeństwa" w dostarczanych systemach, rozporządzania prawami autorskimi w określonych zakresie, czy to poprzez udzielenie licencji, czy poprzez przenoszenie autorskich praw majątkowych do rozwiązań) oraz zabezpieczenie realizacji tych obowiązków poprzez ustanowienie systemu kar umownych.

Z perspektywy dostawcy IT ważna jest także jego świadomość na temat tego, że rekomendacje skierowane do sektora energii powinny być pośrednio stosowane również przez dostawców IT, jeśli świadczą oni usługi na rzecz podmiotów z sektora energii. Wytyczne z każdego obszaru przedstawionego w dokumencie Ministerstwa, m.in. z zakresu zgłaszania incydentów bezpieczeństwa, procedur zarządzania ryzykiem, bezpieczeństwa sieci czy nawet bezpieczeństwa fizycznego obiektów, będą musiały być przestrzegane przez dostawcę IT, jeśli będzie to konieczne do spełnienia wymagań stawianych przez podmiot z sektora energii. Dostawca IT, aby mógł świadczyć usługi podmiotom z sektora energii, będzie musiał dostosować się do stosowanych przez swojego klienta procedur i mechanizmów cyberbezpieczeństwa, aby zapewnić jego odpowiedni poziom.

Rekomendacje Ministerstwa a usługi chmurowe

Ministerstwo w przedstawionych rekomendacjach zwraca uwagę na kwestię korzystania z rozwiązań chmurowych dostarczanych przez podmioty zewnętrzne jako szczególną formę usług, w stosunku do której powinny być spełnione dodatkowe wymagania. Możliwość realizacji tych wymagań powinna być nie tylko zapewniona na poziomie organizacyjnym, lecz także – zgodnie z rekomendacjami – zabezpieczona poprzez odpowiednie zapisy kontraktowe, które będą uwzględniały aspekty bezpieczeństwa i dostępności usług chmurowych.

Zgodnie z treścią rekomendacji przy wyborze usług chmurowych podmioty z branży energii powinny podejmować szczególne środki bezpieczeństwa. Z tego względu zalecane jest stosowanie dodatkowych sposobów zabezpieczania danych przetwarzanych w chmurze, w szczególności ich szyfrowanie czy korzystanie z uwierzytelniania wieloetapowego, a także opracowanie planów ciągłości działania uwzględniających potencjalną możliwość utraty kontroli nad przetwarzanymi informacjami u danego dostawcy.

Dodatkowo Ministerstwo rekomenduje, aby zarówno przed rozpoczęciem korzystania z usług chmurowych przez podmioty z sektora energii, jak i w trakcie wykorzystywania tych usług przeprowadzane było szacowanie ryzyka korzystania z takich rozwiązań. Dlatego też dostawca usług chmurowych powinien być organizacyjnie przygotowany na przeprowadzanie takich procedur przez klientów oraz aktywnie ich wspierać przy dokonywaniu analizy ryzyka.

Ukształtowanie kar umownych w umowie IT – zasada odpowiedzialności

Piotr Nepelski

Odpowiedzialność wykonawcy

Zasada winy wynika z przepisów Kodeksu cywilnego[1]. Stosownie do art. 471 Kodeksu cywilnego dłużnik (np. wykonawca) jest zobowiązany do naprawienia szkody wynikłej z niewykonania lub nienależytego wykonania zobowiązania, chyba że niewykonanie lub nienależyte wykonanie jest następstwem okoliczności, za które dłużnik nie ponosi odpowiedzialności.

Powyższą regułę możemy określić jako podstawową zasadę odpowiedzialności. Stosownie jednak do art. 473 § 1 Kodeksu cywilnego dopuszczalne jest rozszerzenie odpowiedzialności. Przepis pozwala na to, aby dłużnik (np. wykonawca) poprzez umowę przyjął na siebie odpowiedzialność za niewykonanie lub nienależyte wykonanie zobowiązania z powodu oznaczonych okoliczności, za które na mocy ustawy (w tym art. 471 Kodeksu cywilnego) odpowiedzialności nie ponosi.

W razie chęci rozszerzenia odpowiedzialności wykonawcy powinno zostać to wyraźnie zastrzeżone w umowie. Czasami zamawiający sądzą, że wystarczające jest posłużenie się określeniem „opóźnienie"[2] przy konstruowaniu postanowienia o karze za niedotrzymanie terminu realizacji umowy. To jednak za mało, by skutecznie rozszerzyć odpowiedzialność wykonawcy.

W orzecznictwie podnosi się, że jeśli strony zastrzegą karę za opóźnienie, ale bez wyraźnej klauzuli zmiany zasad odpowiedzialności wynikających z przepisów Kodeksu cywilnego, to takie opóźnienie należy rozumieć jako postać kwalifikowaną opóźnienia, czyli zwłokę.

Trafnie w tym zakresie wypowiedział się Sąd Apelacyjny w Białymstoku w wyroku z dnia 8 czerwca 2016 r., sygn. I ACa 116/16, który uznał, że odpowiedzialność dłużnika w zakresie kary umownej, bez względu na przyczynę niewykonania zobowiązania, powinna być w umowie wyraźnie określona. Nie ma bowiem podstaw do dorozumienia rozszerzonej odpowiedzialności dłużnika.

O potrzebie wyraźnego wskazania odejścia od kodeksowej zasady odpowiedzialności wypowiedział się w podobnym tonie także Sąd Najwyższy[3]. Jeżeli więc zamawiający chce rozszerzyć odpowiedzialność wykonawcy, to powinien w umowie jednoznacznie wskazać, w jakich okolicznościach wykonawca ma tę odpowiedzialność ponosić.

Reżim PZP

Zasada ta zachowuje aktualność również w reżimie prawa zamówień publicznych, w którym prawodawca podjął próbę ograniczenia nadmiernego przerzucania odpowiedzialności na wykonawcę. Stosownie do art. 433 Prawa zamówień publicznych[4] projektowane postanowienia umowy nie mogą przewidywać odpowiedzialności wykonawcy za opóźnienie, chyba że jest to uzasadnione okolicznościami lub zakresem zamówienia.

W reżimie prawa zamówień publicznych jest więc dopuszczalne rozszerzenie odpowiedzialności wykonawcy, ale powinno to następować w wyjątkowych sytuacjach. Może to być np. wdrożenie systemu IT, który ma krytyczne znaczenie dla prowadzonej przez zamawiającego działalności, w stopniu, w jakim naruszenie umowy przez wykonawcę może naruszyć fundamenty działania zamawiającego.

[1] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2020 r., poz. 1740).
[2] „Opóźnienie" obejmuje każdy przypadek niewykonania zobowiązania w terminie, w odróżnieniu od „zwłoki", która odnosi się do sytuacji niewykonania zobowiązania z przyczyn zawinionych przez dłużnika.
[3] Por. m.in. wyrok Sądu Najwyższego z dnia 8 lipca 2004 r., sygn. IV CK 583/03, oraz wyrok Sądu Najwyższego z dnia 27 września 2013 r., sygn. I CSK 748/12.
[4] Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2021 r., poz. 1129).

Regulacja doboru personelu w umowach na „body leasing" w IT

Marcin Ręgorowicz

Ze względu na brak odrębnej regulacji ustawowej w umowach na tzw. body leasing podstawowe znaczenie ma redakcja samego kontraktu. Dyskusje dotyczące zagadnień prawnych przy tego rodzaju umowach często są skupione na kwestiach związanych z przenoszeniem majątkowych praw autorskich. Jednakże dla zapewnienia prawidłowej i efektywnej współpracy stron równie istotne są regulacje kwestii biznesowych, przede wszystkim związanych ze specyfiką świadczenia tego rodzaju usług, tj. świadczeniem ich przez specjalistów o określonych kwalifikacjach.

Wstęp

Jak to już zostało opisane w poprzednim wydaniu newslettera, szeroko rozpowszechniony na rynku IT „body leasing" polega na czasowym pozyskaniu od podmiotów zewnętrznych specjalistów o określonych kompetencjach, którzy realizują bieżące zadania w organizacji zamawiającego. „Body leasing" wiąże się z tym, że strony podejmują współpracę, w ramach której, mówiąc w dużym uproszczeniu, dostawca wypożycza zamawiającemu specjalistów o określonych kwalifikacjach w celu realizacji przez nich zadań bezpośrednio w organizacji zamawiającego. W sensie prawnym powyższa współpraca ujmowana jest w formie umowy o świadczenie usług – dostawca zobowiązuje się do wykonywania na rzecz zamawiającego faktycznych świadczeń przez osoby fizyczne o określonych kompetencjach, działające w ścisłym powiązaniu z organizacją zamawiającego.

Z tego typu modelem współpracy wiąże się szereg specyficznych zagadnień prawnych, przede wszystkim w zakresie zabezpieczenia przeniesienia na odbiorcę usług praw do elementów wytwarzanych przez współpracujących z nim specjalistów (co zostało omówione w poprzednim wydaniu newslettera). Niemniej również prawidłowe uregulowanie zasad współpracy stron w toku wykonywania umowy może nastręczać pewnych trudności wobec braku regulacji ustawowej tego rodzaju umów. Z tego powodu przy sporządzaniu i negocjowaniu umów na „body leasing" należy pamiętać o uregulowaniu kilku kluczowych zagadnień – przede wszystkim zaś zasad doboru i powoływania specjalistów oraz weryfikowania przez zamawiającego ich kompetencji.

Określenie kompetencji specjalistów w umowach

W pierwszej kolejności wskazać należy, że najczęściej występującym na rynku modelem zawierania umów na „body leasing" jest umowa ramowa, na podstawie której zawierane są umowy szczegółowe, najczęściej w formie różnego rodzaju „zamówień" lub „zleceń". O ile umowa ramowa określa podstawowe zasady współpracy stron i zawiera większą część regulacji stosunku prawnego łączącego strony, o tyle treść umów szczegółowych sprowadza się najczęściej do określenia szczegółów o charakterze czysto biznesowym, tj.: profilu specjalisty, z którym nawiązywana jest współpraca, czasu, w jakim usługi będą wykonywane przez tę osobę, rodzaju tych usług czy stawki należnego dostawcy wynagrodzenia. Taka konstrukcja umów jest w większości przypadków optymalna, pozwala bowiem zawrzeć wszelkie niezbędne postanowienia regulujące współpracę stron w jednej umowie, pozostawiając do uregulowania w umowach szczegółowych wąski od strony ilościowej zakres.

Oczywiście niezależnie od przyjętego modelu umowy kluczowe jest jak najdokładniejsze określenie wymagań zamawiającego co do specjalistów, z którymi ma zostać podjęta współpraca. Istotne jest przede wszystkim możliwie precyzyjne określenie ich profilu kompetencyjnego oraz sposobu potwierdzania tych kompetencji. Przy przyjęciu modelu umowy ramowej konieczne jest zatem, aby umowa szczegółowa określała wprost wymagane kompetencje czy doświadczenie zawodowe danego specjalisty. Zbyt wysoki poziom ogólności będzie skutkował sporami między stronami i znacząco utrudni przede wszystkim wykonywanie uprawnień kontrolnych przez zamawiającego, o których będzie mowa niżej.

Procedura doboru specjalistów

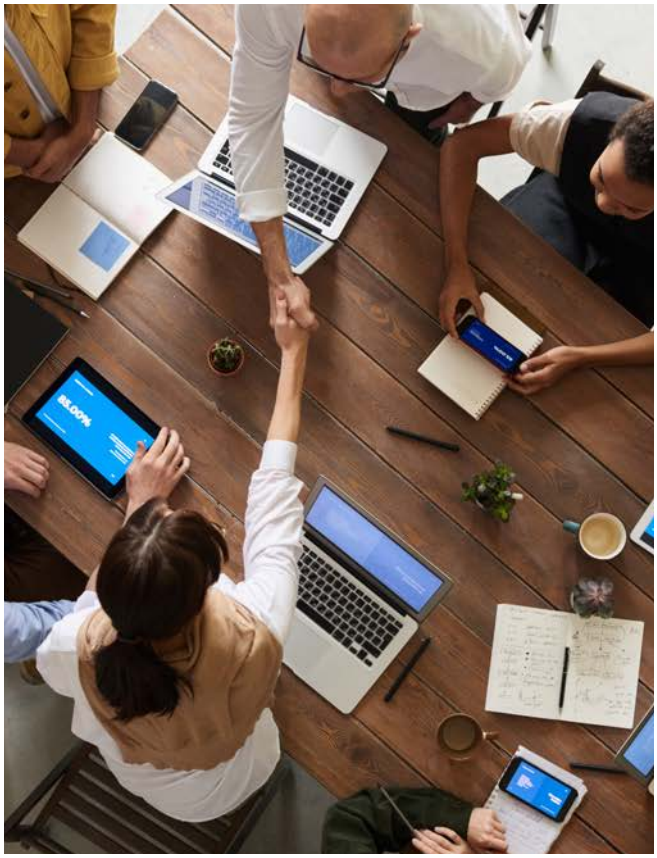
Z powyższym wiąże się konieczność prawidłowego uregulowania procedury doboru specjalistów. Kluczowe jest przede wszystkim ustalenie zasad ich wyboru. W praktyce najczęściej po złożeniu przez zamawiającego stosownego zapytania, w którym wskazano zapotrzebowanie na osoby o określonych kompetencjach, dostawca zobowiązany będzie do przedstawienia potencjalnych kandydatów do podjęcia współpracy.

W ramach tego etapu poza kwestiami bardziej prozaicznymi, jak wyraźne określenie przedstawicieli stron uprawnionych do składania zapotrzebowania na specjalistów czy akceptacji konkretnych kandydatów, istotne jest przede wszystkim uregulowanie sprecyzowanych terminów odpowiedzi na zapytania zamawiającego i przedstawienia kandydatów. Ponadto niezbędne jest określenie skutku złożenia przez zamawiającego powyższego zapytania – może to przyjąć formę konkretnego zobowiązania do przedstawienia w sprecyzowanym terminie określonej liczby kandydatów spełniających wymagania zamawiającego, a brak jego spełnienia stanowić będzie naruszenie postanowień umowy (jest to rozwiązanie korzystne dla zamawiającego). Alternatywnie dostawca może mieć jedynie możliwość (uprawnienie) złożenia odpowiedzi na zapytanie – bez skonkretyzowanego zobowiązania, a więc po prostu prawo do powstrzymania się, według własnego uznania, od przedstawienia kandydatów (co jest oczywiście korzystne dla dostawcy). Powyższą kwestię należy jednoznacznie uregulować, by w toku współpracy uniknąć wątpliwości interpretacyjnych wynikających z rozbieżnych oczekiwań stron co do skutku zgłoszenia przez zamawiającego zapotrzebowania na specjalistów.

Weryfikacja kompetencji specjalistów

W umowie na „body leasing" niezbędne jest uregulowanie zasad akceptacji (lub jej odmowy) przedstawionych kandydatów i żądania przedstawienia innych osób, a także zakresu uprawnień zamawiającego do weryfikacji kompetencji osób przedstawianych przez dostawcę. Oczywiście podstawowym od strony biznesowej elementem współpracy w ramach „body leasingu" jest zapewnienie wykonywania usług przez specjalistów o określonych, wymaganych przez zamawiającego kompetencjach. Jest to w zasadzie głównym celem zawierania tego rodzaju umowy, a tym samym podstawowym zobowiązaniem dostawcy. Niemniej dla dostawcy istotnym problemem, zwłaszcza od strony biznesowej, może być ciągła odmowa akceptacji przez zamawiającego przedstawianych kandydatów i konieczność wskazywania następnych – szczególnie gdy dostawca jest wprost zobowiązany do przedstawienia kandydatów odpowiadających preferencjom zamawiającego w konkretnym terminie.

Optymalnym rozwiązaniem tego problemu wydaje się przyznanie zamawiającemu uprawnienia do weryfikacji przedstawianych kandydatów pod kątem posiadania przez nich kompetencji i przyznanie prawa odmowy akceptacji danego specjalisty tylko w przypadku, gdy nie będzie ich miał – wbrew zapewnieniom dostawcy. W tym zakresie przydatne jest przede wszystkim wprowadzenie postanowień umownych zobowiązujących dostawcę do udokumentowania kompetencji i doświadczenia specjalistów oraz przyznanie zamawiającemu uprawnienia do ich weryfikacji, a także żądania udzielenia dalszych wyjaśnień. Ponadto zamawiającemu można przyznać uprawnienie żądania przeprowadzenia bezpośredniej rozmowy z danym specjalistą.



Uprawnienie do zmiany specjalistów

Oczywiście weryfikacja kompetencji danego specjalisty przed nawiązaniem współpracy nie zawsze jest wystarczająca – będzie ona dokonywana w znacznym stopniu już w toku faktycznej realizacji zadań przez specjalistę na rzecz zamawiającego. Istotne jest zatem uregulowanie kwestii prawa zamawiającego do żądania zmiany specjalistów, z którymi współpracuje, już po nawiązaniu współpracy. Celem tego rozwiązania jest zapewnienie zamawiającemu z jednej strony weryfikacji deklarowanych kompetencji specjalisty na etapie właściwego wykonywania umowy, a z drugiej – zabezpieczenia należytego wykonywania usług świadczonych na podstawie umowy.

W celu prawidłowego zabezpieczenia powyższej kwestii niezbędne jest przyznanie zamawiającemu prawa do żądania zmiany danego specjalisty w czasie obowiązywania umowy. Jednocześnie z powyższym uprawnieniem powinno być powiązane konkretne zobowiązanie dostawcy do przedstawienia nowych specjalistów o odpowiednich kompetencjach. Istotne jest, by termin wykonania powyższego zobowiązania był precyzyjnie określony. Oczywiście dla bezpieczeństwa zamawiającego ważne jest również przyznanie mu prawa do żądania natychmiastowego odwołania specjalisty – i zaprzestania faktycznego wykonywania przez niego zadań. Ma to służyć ochronie zamawiającego w przypadkach rażąco nieprawidłowych działań danego specjalisty.

Z kolei z punktu widzenia dostawcy konieczne jest określenie precyzyjnych przesłanek odwoływania i zmiany specjalistów – i ograniczenia ich przede wszystkim do przypadków, gdy ujawni się, że dane osoby mają kompetencje rzeczywiście niewystarczające w stosunku do umówionych wymagań zamawiającego lub wykonują swoje zadania w sposób nienależyty. Służyć to będzie ograniczeniu ryzyka nadużywania swoich uprawnień przez zamawiającego przez żądanie zmiany specjalistów z nieistotnych przyczyn.

Zastępstwo specjalistów

W umowach na „body leasing" rekomendowane jest także uregulowanie kwestii zastępstwa specjalistów w trakcie ich nieobecności – zarówno planowanych, jak i nieplanowanych. Przyczyny nieobecności specjalistów mogą być rozliczne (od planowanego krótkiego urlopu po nagłą i wielomiesięczną absencję spowodowaną chorobą), jednak skutki tej nieobecności mogą być dotkliwe przede wszystkim dla zamawiającego. W takiej sytuacji niezbędne jest zapewnienie ciągłości świadczenia usług i wyznaczenie zastępstwa, o ile w danej sytuacji będzie to uzasadnione biznesowo. Należy mieć bowiem na uwadze, że zamawiającego nie łączy ze specjalistą stosunek prawny, nie ma on zatem możliwości bezpośredniego wpływu na specjalistów, zwłaszcza w zakresie np. planowania urlopów. Dostawca może mieć jednak w stosunku do specjalistów obowiązki wynikające wprost z przepisów prawa (np. obowiązek udzielenia urlopu zgodnie z przepisami prawa pracy).

W umowie konieczne jest zatem przewidzenie powyższych okoliczności i określenie uprawnień zamawiającego w przypadku nieobecności specjalisty. Przede wszystkim niezbędne jest przyznanie zamawiającemu prawa do żądania przedstawienia przez dostawcę zastępstwa oraz określenia przejrzystych zasad w tym zakresie. Należy mieć przy tym na uwadze, że w odniesieniu do zastępstw rzeczywiste potrzeby stron (zwłaszcza zamawiającego) mogą być różne w poszczególnych przypadkach – nie zawsze w jego interesie będzie zmiana specjalisty, zwłaszcza gdy określone osoby mają szczególne kompetencje lub np. są bardzo zaangażowane w realizowany projekt. Zmiana takich osób rodziłaby dla zamawiającego istotne problemy.

Niemniej dostawca może nie zawsze mieć możliwość zapewnienia zastępstwa (zwłaszcza w krótkim terminie) specjalisty o określonych kompetencjach. Przede wszystkim może się to wiązać z nieakceptowalnymi dla dostawcy kosztami utrzymywania rozbudowanego zespołu specjalistów z różnych dziedzin. Z powyższych względów rekomendowane jest zawarcie w umowie ogólnego zobowiązania dostawcy do zapewnienia zastępstwa dla specjalistów na żądanie zamawiającego, ale szczegółowe zasady wykonywania tego zobowiązania powinna cechować daleko idąca elastyczność. Warto jednak określić pewne ogólne, ale precyzyjne ramy zobowiązania dostawcy – przede wszystkim końcowy termin dostarczenia zastępstwa.

Podsumowanie

Możliwość pozyskania specjalistów o niezbędnych zamawiającemu kompetencjach jest zasadniczo podstawową racją gospodarczą umowy na „body leasing". Z tego powodu kluczowe jest precyzyjne unormowanie relacji stron w zakresie doboru specjalistów i weryfikacji ich kompetencji zarówno przed podjęciem współpracy, jak i w toku obowiązywania umowy. Zawierane umowy powinny zawierać szczegółowe postanowienia w tym zakresie, zwłaszcza regulujące uprawnienie zamawiającego do odmowy podjęcia współpracy z danym specjalistą lub żądania jego zmiany w czasie obowiązywania umowy.

Co się dzieje z wdrożeniem Europejskiego kodeksu łączności elektronicznej i Prawem komunikacji elektronicznej?

Karolina Grochecka-Goljan

Państwa członkowskie Unii Europejskiej były obowiązane wdrożyć unijną dyrektywę Europejski kodeks łączności elektronicznej z dnia 11 grudnia 2018 r.[1] do 21 grudnia 2020 r. W wielu jurysdykcjach, w tym w Polsce, proces wdrożenia dyrektywy wciąż trwa.

Polski ustawodawca zdecydował się na kompleksowe podejście do wdrożenia, a ustawa Prawo komunikacji elektronicznej ma w całości zastąpić ustawę Prawo telekomunikacyjne[2].

Jaki jest zatem status wdrożenia unijnej dyrektywy Europejski kodeks łączności elektronicznej w Polsce?

Status wdrożenia Europejskiego kodeksu łączności elektronicznej

Jak opisywaliśmy w newsletterze IT-Tech nr 1 ze stycznia 2021 r., z dniem 21 grudnia 2020 r. weszła w życie nowelizacja ustawy Prawo telekomunikacyjne, która stanowiła pierwszy etap wdrożenia w polskim prawie przepisów Europejskiego kodeksu łączności elektronicznej.

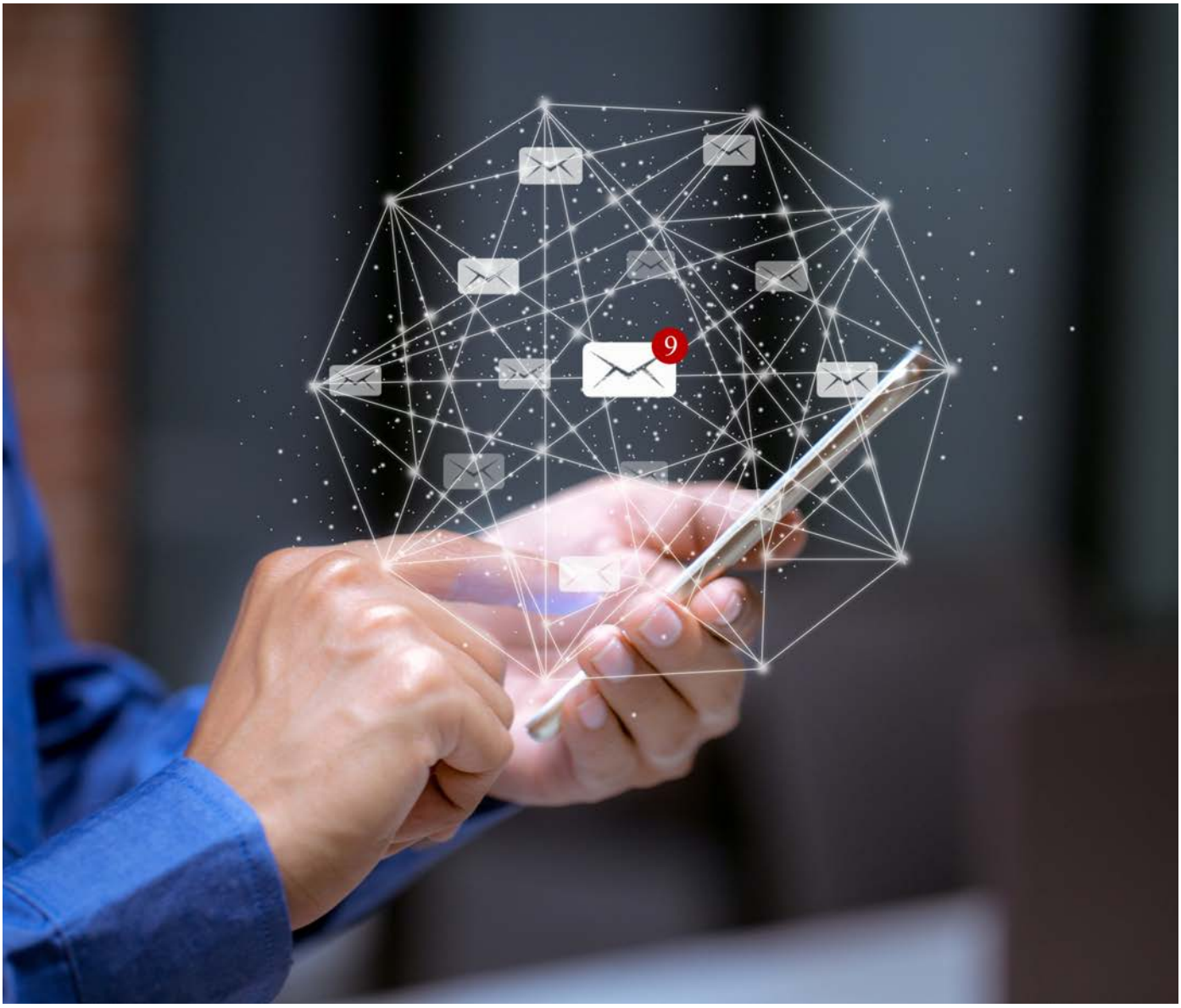
Pomimo funkcjonujących już projektów ustawy Prawo komunikacji elektronicznej, które były poddane konsultacjom publicznym, we wrześniu 2021 r. Departament Telekomunikacji KPRM opublikował nowe projekty ustawy Prawo komunikacji elektronicznej i ustawy wprowadzającej PKE[3].

Wrześniowy projekt zawiera modyfikacje przepisów w stosunku do uprzednio publikowanego projektu ustawy. Zmianie uległy w szczególności przepisy dotyczące wykonywania działalności gospodarczej – rozszerzono zakres danych, które przedsiębiorca ma obowiązek przedkładać Prezesowi UKE. Zmienione zostały również projektowane przepisy dotyczące zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego – wprowadzono możliwość nałożenia na przedsiębiorcę telekomunikacyjnego obowiązku ograniczenia zakresu lub obszaru wykorzystania zasobów częstotliwości radiowych w przypadku stanu nadzwyczajnego na wniosek użytkownika rządowego, a także rozszerzono dostęp do danych abonentów w zakresie obowiązku zapewnienia warunków do uzyskiwania informacji przez uprawnione podmioty.

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona) (Dz. U. UE L z 2018 r., Nr 321, str. 36, z późn. zm.).
[2] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2021 r., poz. 576).
[3] Projekt z 3 września 2021 r., dostępny tutaj: https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-prawo-komunikacji-elektronicznej.html (dostęp: 1.12.2021).

Dodano również przepisy w zakresie praw użytkowników końcowych, mające działać na korzyść i w celu ochrony abonentów – za takie należy uznać w szczególności uznanie za nieważną umowy zawartej poza lokalem przedsiębiorstwa podczas nieumówionej wizyty przedsiębiorcy w miejscu zamieszkania lub zwykłego pobytu konsumenta. Rozszerzono też katalog naruszeń podlegających karze pieniężnej, np. na: naruszenie zakazu zawierania umów o świadczenie usług komunikacji elektronicznej poza lokalem przedsiębiorstwa podczas nieumówionej wizyty (art. 278 ust. 4), naruszenie zakazu uporczywego naruszania obowiązków dotyczących zawierania umowy o świadczenie usług komunikacji elektronicznej, w szczególności wprowadzania abonenta w błąd na etapie zawierania umowy (art. 278 ust. 8), naruszenie zakazu uporczywego naruszania obowiązków związanych z umożliwieniem rozwiązania umowy w formie dokumentowej (art. 290 ust. 1–4), uniemożliwianie albo utrudnianie abonentowi rozwiązania umowy w formie dokumentowej (art. 290 ust. 5).

Pomimo prawie rocznego opóźnienia we wdrożeniu Europejskiego kodeksu łączności elektronicznej do polskiego porządku prawnego zakończenia prac nad Prawem komunikacji elektronicznej nie widać na horyzoncie. Niewątpliwie jest to mocno wyczekiwana regulacja, w szczególności z uwagi na objęcie jej zakresem usług komunikacji elektronicznej, co jest pojęciem szerszym od usług telekomunikacyjnych dotychczas regulowanych w Prawie telekomunikacyjnym. Wiąże się to z kolei np. z możliwością nałożenia na dostawców usług nieobjętych dotychczasowymi regulacjami nowych obowiązków, które w pewnych aspektach mogą być nawet zrównane z obowiązkami przedsiębiorców telekomunikacyjnych. Projekt znajduje się na liście nowelizacji, której się bacznie przyglądamy.



Sztucznie inteligentne wyroby medyczne. Biała księga TÜV SÜD, czyli nowe wytyczne dla branży medtech

Kamila Dymek

Czym jest biała księga i dlaczego warto poświęcić jej uwagę?

Zastosowanie sztucznej inteligencji (AI) w wyrobach medycznych staje się coraz bardziej powszechne i stanowi ogromny potencjał dla sektora zdrowia. Mimo to wciąż brakuje odpowiednich uregulowań prawnych, a obowiązujące w UE przepisy dotyczące wyrobów medycznych nie odzwierciedlają transformacji cyfrowej ani złożoności algorytmów AI. Przepaść pomiędzy zaawansowaną technologią a przepisami prawa powoduje, że wprowadzenie na rynek urządzenia medycznego z AI to ogromne wyzwanie. Stawka jest szczególnie wysoka, bo takie urządzenia mogą ratować życie i zdrowie człowieka, ale także im zagrażać. Dlatego jednostka notyfikowana TÜV SÜD opublikowała białą księgę[1], w której dzieli się kluczowymi aspektami wykorzystania AI w branży medtech. Publikacja ta ma pomóc producentom i programistom w zastosowaniu właściwego podejścia do oceny bezpieczeństwa tworzonych produktów.

Korzyści z zastosowań sztucznej inteligencji w branży medtech

Sztuczna inteligencja, szczególnie uczenie maszynowe (ML), odgrywa coraz większą rolę w analizie, diagnozowaniu oraz monitorowaniu leczenia pacjenta. Wyposażone w AI urządzenia medyczne i oprogramowanie jako urządzenia medyczne (SaMD) dzięki ciągłemu przetwarzaniu ogromnych ilości danych szybko dostosowują się do zmieniających się warunków i optymalizują swoje działanie w czasie rzeczywistym. „Te właściwości mogą prowadzić do poprawy wyników leczenia pacjentów, co z kolei skutkuje obniżeniem kosztów i znacznym wzrostem ogólnej jakości opieki zdrowotnej na całym świecie" – pisze dr Abtin Rad w białej księdze. Jako przykład ilustrujący te korzyści podać można kanadyjską firmę specjalizującą się w opartym na AI monitorowaniu rozprzestrzeniania się chorób zakaźnych. Ostrzegała ona swoich klientów przed ryzykiem epidemii w Chinach w grudniu 2019 r., prawie dwa miesiące przed tym, jak WHO podała informację o szczególnym przypadku choroby grypopodobnej w Wuhanie[2]. Dostęp do globalnych danych dotyczących biletów lotniczych umożliwił z kolei AI prawidłowe prognozowanie rozprzestrzeniania się wirusa w kilka dni po jego pojawieniu się.

Wyzwania i zagrożenia dla branży

Ta sama cecha, która świadczy o tak wielkim potencjale AI, tj. zdolność dostosowywania się do zmieniających się warunków i nowych informacji, stanowi zarazem największe wyzwanie dla producentów wyrobów medycznych. Powoduje bowiem, że ocena ryzyka związanego z danym wyrobem jest bardzo trudna, a jej wyniki mogą być zmienne w czasie. Co więcej, na ocenę możliwości AI kluczowy wpływ ma ilość i jakość danych, na które oddziaływać mogą m.in. uprzedzenia w ich doborze i gromadzeniu oraz błędy w ich etykietowaniu. Zaufanie mogą zaś wzbudzić tylko te prognozy AI, które będą przejrzyste i wytłumaczalne. Tymczasem modele AI bardzo często działają jak czarna skrzynka, tzn. zrozumienie sposobu podejmowania przez nie decyzji może być bardzo trudne lub wręcz niemożliwe, w odróżnieniu od tradycyjnego statycznego kodu programu, który może być oceniany linia po linii.

[1] *Artificial Intelligence in Medical Devices. Verifying and validating AI-based medical devices*, https://www.tuvsud.com/en/-/media/global/pdf-files/whitepaper-report-e-books/tuvsud-ai-in-medical-devices-whitepaper.pdf (dostęp: 2.12.2021).

[2] L. Beigel, *Koronawirus: Dlaczego algorytm jako pierwszy dowiedział się o epidemii*, https://www.rnd.de/digital/coronavirus-warum-ein-algorithmus-zuerst-von-der-epidemie-wusste-JE32CSE745EW7CBU5ESLVE36ZE.html (dostęp: 2.12.2021).

Prawo znów nie nadąża za technologią

Opisana powyżej specyfika powoduje, że obowiązujące obecnie przepisy nie są dostosowane do wykorzystywania tych innowacyjnych technologii. Przykładowo rozporządzenie unijne w sprawie wyrobów medycznych[3] określa wymagania dotyczące oprogramowania bardzo ogólnikowo. Zgodnie z rozporządzeniem oprogramowanie musi być m.in. zaprojektowane tak, aby „zapewnić powtarzalność wyników, niezawodność i działanie zgodne z ich przewidzianym używaniem" oraz aby było zgodne z aktualnym stanem wiedzy. Zatem norma ISO 14971, stosowana z powodzeniem przy ocenie ryzyka wyrobów medycznych opartych na tradycyjnych technologiach, w odniesieniu do AI traci na przydatności. W kwietniu 2021 r. Komisja Europejska przedstawiła projekt unijnego rozporządzenia w sprawie sztucznej inteligencji[4]. Zaproponowała w nim ogólne wymogi dla systemów AI wysokiego ryzyka, do których zaliczać się mają także produkty będące elementem wyrobu medycznego lub stanowiące wyrób medyczny[5]. Dalszy rozwój sztucznej inteligencji w medycynie jest jednak uzależniony od istnienia norm zaprojektowanych specjalnie do oceny tego typu technologii.

Checklista

W białej księdze omówiono podstawowe kryteria oceny wyrobów medycznych wykorzystujących technologie AI opracowane z udziałem TÜV SÜD przez Stowarzyszenie Jednostek Notyfikowanych ds. Wyrobów Medycznych w Niemczech (IG-NB) w formie listy kontrolnej (checklisty). Identyfikuje ona ok. 150 kryteriów oceny technologii medycznych z podziałem na następujące 6 sekcji:

- „Cel" to grupa kryteriów służących stwierdzeniu, czy technologie medyczne wykorzystujące AI oferują wyraźne korzyści w stosunku do porównywalnych technologii niewykorzystujących AI. Ponadto kryteria te określają ramy, które producenci i twórcy oprogramowania powinni stosować do oceny ryzyka związanego z zastosowaniem tych technologii.

- „Wymagania dotyczące oprogramowania" dotyczą funkcjonalności i wydajności algorytmów i obejmują kryteria takie jak: możliwość zastosowania zgodnie z przeznaczeniem, oczekiwane zakresy wartości wyników, powtarzalność i odtwarzalność wyników oraz zachowanie algorytmu w sytuacji, gdy dane wejściowe nie spełniają określonych wymagań. Kryteria te odnoszą się też do interfejsu użytkownika.

- „Zarządzanie danymi" to zestaw kryteriów związanych z gromadzeniem danych do trenowania, walidacji i testowania danych wykorzystywanych do oceny algorytmów AI. Kryteria te obejmują m.in. metody anonimizacji oraz czynniki w doborze danych mogące być źródłem uprzedzeń.

- „Opracowanie modelu", czyli kryteria służące do oceny integralności i efektywności procesu opracowywania modelu AI, a także oceny jakości samego modelu, m.in. możliwość identyfikacji tych zbiorów danych, które usprawniają algorytm.

- „Rozwój produktu" to grupa kryteriów odnoszących się do rozwoju oprogramowania, w tym testowania i tworzenia dokumentacji oraz oceny działania w różnych językach programowania i środowiskach albo na różnych platformach sprzętowych. W ramach tej grupy przedstawione są także kryteria oceny, czy produkt rzeczywiście zapewnia oczekiwane korzyści medyczne.

- „Wprowadzenie produktu do obrotu" obejmuje kryteria mające zastosowanie podczas produkcji, dystrybucji i instalacji technologii medycznej wykorzystującej AI, również dotyczące bieżącego nadzoru i oceny technologii po jej wprowadzeniu na rynek.

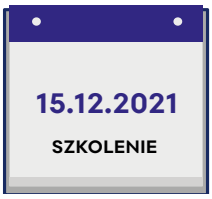
Wnioski

Do czasu opublikowania norm regulujących bezpieczeństwo „medycznej AI" powyższe kryteria mogą być wykorzystane do minimalizacji ryzyka w trakcie jej tworzenia. Mimo że wytyczne zawarte w białej księdze nie mają mocy aktu prawnego, stosowanie rekomendowanych w niej praktyk może przygotować producentów oprogramowania na nadchodzące zmiany prawne i uchronić przed konsekwencjami wprowadzenia na rynek produktów, które w przyszłości okażą się niebezpieczne dla ich użytkowników. Z tego względu spółki technologiczne opracowujące „medyczne AI" powinny rozważyć przyjęcie kompleksowego podejścia do oceny bezpieczeństwa, skoncentrowanego na procesach we wszystkich fazach cyklu życia produktu oraz wykraczającego poza datę wprowadzenia go na rynek. Należy zauważyć, że w sytuacjach, w których producent zleca kluczowe elementy któregokolwiek z tych procesów podmiotom zewnętrznym, powyższe zalecenia mają do nich zastosowanie, wobec czego mogą stanowić kryteria również przy doborze podwykonawców.

Biała księga opracowana przez TÜV SÜD dostępna jest w języku angielskim pod adresem.

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG.

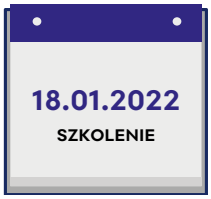
NADCHODZĄCE WYDARZENIA



UMOWY NA UTRZYMANIE, SERWIS I ROZWÓJ SYSTEMÓW IT – NAJLEPSZE PRAKTYKI I SPORNE KWESTIE

r. pr. Agnieszka Wachowska

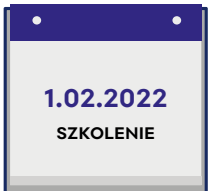
Więcej informacji >>



UMOWY Z PRACOWNIKAMI I WSPÓŁPRACOWNIKAMI W IT – PROBLEMY PRAWNE W PRAKTYCE Z UWZGLĘDNIENIEM ZAGADNIEŃ PRAWA AUTORSKIEGO I PREFERENCJI PODATKOWYCH

r. pr. Agnieszka Wachowska, r.pr. Marcin Ręgorowicz

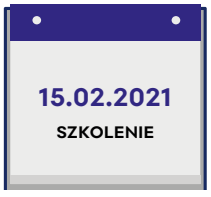
Więcej informacji >>



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 >>



PRAWNE ASPEKTY CYBERBEZPIECZEŃSTWA

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

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

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

Jakub Chlebowski
Radca prawny, Senior Associate
jakub.chlebowski@traple.pl

MarcinRęgorowicz
Radca prawny, Senior Associate
marcin.regorowicz@traple.pl

Dominika Stecka, LL.M. Eur.
Aplikantka radcowska, Associate
dominika.stecka@traple.pl

Małgorzata Kotwica
Associate
malgorzata.kotwica@traple.pl

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

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

Redaktorka newslettera:
adw. Karolina Grochecka-Goljan