NR 2 - MAJ 2022

NEWSLETTER

IT-TECH

W NUMERZE M.IN.:

- Nowy projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa – jakie wprowadza zmiany?
- Outsourcing IT w decyzji PUODO
- Dostawca narzędzi IT odpowie za wykorzystanie ich przez kartel
- Data Act – jak wpłynie na umowy chmurowe?
- Wytyczne Datatilsynet dotyczące przetwarzania danych osobowych w chmurze

Traple
Konarski
Podrecki
& Wspólnicy

TKP

Nowy projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa – jakie wprowadza zmiany?

Agnieszka Wachowska, Aleksander Elmerych

25 marca 2022 r. na stronie internetowej Rządowego Centrum Legislacji opublikowany został projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa z dnia 15 marca 2022 r.[1] (dalej również: „projekt nowelizacji"), zapowiadany od wielu tygodni przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa Janusza Cieszyńskiego. Prace nad nowym projektem miały nabrać tempa z początkiem roku, jednak zostały opóźnione – na opóźnienie najprawdopodobniej miała też wpływ rosyjska inwazja na Ukrainę i związane z tym zwiększone zaangażowanie w zapobieganie ewentualnym atakom cybernetycznych na polską infrastrukturę rządową. Poprzedni projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, z dnia 12 października 2021 r.[2], wywołał wiele emocji i kontrowersji, w szczególności ze względu na procedurę dotyczącą uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka oraz na możliwość wydawania przez ministra właściwego ds. informatyzacji poleceń zabezpieczających – do projektu ustawy zgłoszonych zostało wiele uwag, pochodzących m.in. od organizacji zrzeszających przedsiębiorców, lecz niestety w opublikowanych na RCL materiałach brak jest odniesienia się do tych uwag.

Przedsiębiorcy komunikacji elektronicznej włączeni do krajowego systemu cyberbezpieczeństwa

Najistotniejszą zmianą w stosunku do wcześniejszego (szóstego) projektu nowelizacji z dnia 12 października 2021 r. jest włączenie do krajowego systemu cyberbezpieczeństwa przedsiębiorców komunikacji elektronicznej, przy czym definicja „przedsiębiorcy komunikacji elektronicznej" na gruncie projektu nowelizacji pozostaje zbieżna z definicją pochodzącą z projektu ustawy – Prawo komunikacji elektronicznej z dnia 2 grudnia 2021 r.[3], który również nieustannie od dwóch lat jest nadal procedowany. Zgodnie za obecną wersją projektu nowelizacji UKSC za przedsiębiorcę komunikacji elektronicznej uznaje się nie tylko przedsiębiorcę telekomunikacyjnego (np. operatora telekomunikacyjnego), lecz także wszystkie inne podmioty świadczące publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów (a więc m.in. podmioty świadczące usługi poczty elektronicznej, usługi przekazywania wiadomości, a także dostarczający czaty grupowe, czy różnego rodzaju komunikatory). Zmiana ta stanowi istotne rozszerzenie zakresu podmiotów, do których należy stosować przepisy ustawy o krajowym systemie cyberbezpieczeństwa – zgodnie bowiem z projektem nowelizacji z dnia 12 października 2021 r. krajowym systemem cyberbezpieczeństwa mieli być objęci wyłącznie przedsiębiorcy telekomunikacyjni. Natomiast zgodnie z obecną wersją projektu nowelizacji UKSC **wszyscy przedsiębiorcy komunikacji elektronicznej będą podlegać przepisom ustawy o krajowym systemie cyberbezpieczeństwa, niezależnie od wielkości oraz niezależnie od tego, czy mogą zostać zakwalifikowani jako operatorzy usług kluczowych czy dostawcy usług cyfrowych**. Warto również odnotować, że w najnowszym projekcie nowelizacji zrezygnowano z pomysłu zakresowego stosowania ustawy o krajowym systemie cyberbezpieczeństwa do przedsiębiorców komunikacji elektronicznej – zgodnie z najnowszym projektem należy do nich stosować całą ustawę, chyba że wyraźne wyłączenie wynika z przepisów szczególnych.

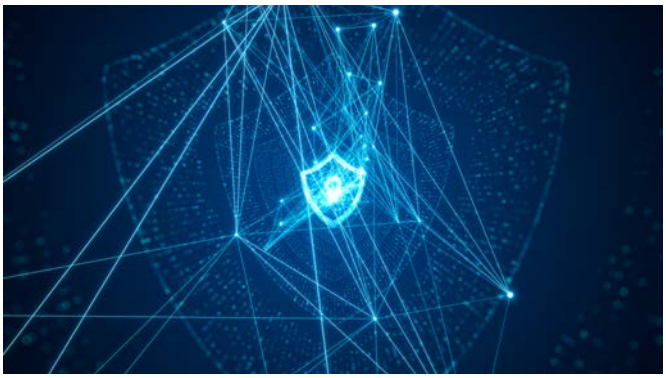
[1] Zob. projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw z dnia 15 marca 2022 r., dostępny pod adresem: https://legislacja.rcl.gov.pl/projekt/12337950 (dostęp: 29.03.2022).

[2] 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: 29.03.2022).

[3] Zob. projekt ustawy – Prawo komunikacji elektronicznej z dnia 2 grudnia 2021 r., dostępny pod adresem: https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-prawo-komunikacji-elektronicznej.html (dostęp: 29.03.2022).

Szczególne obowiązki przedsiębiorców komunikacji elektronicznej

W związku z włączeniem przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa projekt nowelizacji zakłada także wprowadzenie całkowicie nowego rozdziału 4a, który reguluje ich szczególne obowiązki w zakresie cyberbezpieczeństwa. Obowiązki te mają zostać nałożone na wszystkich przedsiębiorców komunikacji elektronicznej, a więc w szczególności na podmioty takie jak dostawcy poczty elektronicznej, czy podmioty dostarczające usługi przekazywania wiadomości, czaty grupowe, czy różnego rodzaju komunikatory.



Przedsiębiorcy komunikacji elektronicznej mają być zobowiązani m.in. do:

- uwzględniania możliwości wystąpienia sytuacji szczególnego zagrożenia (a więc m.in. sytuacji stanowiących bezpośrednie zagrożenie dla bezpieczeństwa sieci i usług komunikacji elektronicznej czy sytuacji wymagających współpracy przedsiębiorców komunikacji elektronicznej z organami administracji publicznej i innymi podmiotami w czasie obowiązywania stanów nadzwyczajnych czy w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny);
- przeprowadzania udokumentowanego, systematycznego szacowania ryzyka wystąpienia ww. sytuacji;
- publikowania na swoich stronach internetowych m.in. informacji o potencjalnych zagrożeniach związanych z korzystaniem przez użytkowników z usług komunikacji elektronicznej, o rekomendowanych środkach ostrożności i najbardziej popularnych sposobach zabezpieczania telekomunikacyjnych urządzeń końcowych przed oprogramowaniem złośliwym lub szpiegującym czy o przykładowych konsekwencjach braku lub nieodpowiedniego zabezpieczenia telekomunikacyjnych urządzeń końcowych;
- informowania na swojej stronie internetowej o incydencie telekomunikacyjnym i jego wpływie na dostępność świadczonych usług, jeżeli wpływ ten jest istotny;
- informowania użytkowników o przypadkach szczególnego i znacznego zagrożenia wystąpienia incydentu telekomunikacyjnego;
- podejmowania środków technicznych i organizacyjnych zapewniających poufność, integralność, dostępność i autentyczność przetwarzanych danych oraz adekwatny poziom cyberbezpieczeństwa, a także dokumentowania podjęcia takich środków.

Warto zwrócić uwagę na to, że minimalny poziom ww. środków technicznych i organizacyjnych, do których podjęcia zobowiązani mają być przedsiębiorcy komunikacji elektronicznej, będzie mógł zostać określony w rozporządzeniu wydanym przez ministra właściwego ds. informatyzacji. Wydaje się, że wydanie takiego rozporządzenia znacznie ułatwiłoby wypełnienie wspomnianych obowiązków, przede wszystkim przez mniejszych przedsiębiorców komunikacji elektronicznej. Warto również podkreślić, że Prezes Urzędu Komunikacji Elektronicznej (UKE) ma w tym zakresie uzyskać szczególne uprawnienia kontrolne. Prezes UKE będzie mógł w drodze decyzji administracyjnej nałożyć na przedsiębiorcę komunikacji elektronicznej m.in. obowiązek uzupełnienia i właściwego zastosowania środków technicznych i organizacyjnych na rzecz cyberbezpieczeństwa czy poddania się przez przedsiębiorcę komunikacji elektronicznej (na jego koszt) audytowi bezpieczeństwa.

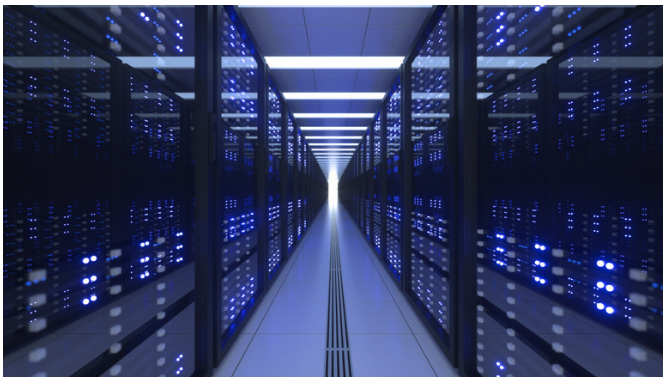
Wszyscy przedsiębiorcy komunikacji elektronicznej mają mieć również obowiązek:

- zapewnienia obsługi incydentów telekomunikacyjnych – całkowicie nowej kategorii incydentów, obejmującej wszelkie zdarzenia, które mają rzeczywisty, niekorzystny skutek dla bezpieczeństwa sieci i usług komunikacji elektronicznej;
- zgłaszania poważnych incydentów telekomunikacyjnych w ciągu 24 godzin do nowego, utworzonego specjalnie z myślą o sektorze telekomunikacyjnym CSIRT Telco (przy czym progi dla uznania incydentu telekomunikacyjnego za poważny incydent telekomunikacyjny zostaną określone w rozporządzeniu ministra właściwego ds. informatyzacji);
- współdziałania z właściwymi CSIRT w obsłudze poważnych incydentów telekomunikacyjnych.

Świadomość zakresu obowiązków przedsiębiorców komunikacji elektronicznej na gruncie projektowanej nowelizacji jest niezwykle istotna z uwagi na grożące tym przedsiębiorcom wysokie kary za niewypełnienie większości tych obowiązków (m.in. w zakresie obsługi i zgłaszania incydentów telekomunikacyjnych czy szacowania ryzyka i podejmowania odpowiednich środków technicznych i organizacyjnych na rzecz cyberbezpieczeństwa). Kary te mogą wynosić do 3% wartości przychodu danego podmiotu za poprzedni rok kalendarzowy (w szczególnych przypadkach, gdy dany podmiot w ostatnich trzech latach kalendarzowych przed wymierzeniem kary nie osiągnął przychodu lub osiągnął przychód w wysokości

nieprzekraczającej 500 000 zł, kara to może wynosić maksymalnie 15 000 zł).

Niezależnie od powyższego, należy pamiętać o tym, że w pewnych szczególnych sytuacjach przedsiębiorca komunikacji elektronicznej może zostać uznany za operatora usługi kluczowej (np. w przypadku podmiotów prowadzących punkt wymiany ruchu internetowego) lub też być jednocześnie dostawcą usług cyfrowych – w takiej sytuacji, oprócz obowiązków wynikających z rozdziału 4a, taki podmiot będzie musiał wypełnić wszystkie obowiązki przewidziane dla operatorów usług kluczowych lub dostawców usług cyfrowych, za których naruszenie również mogą zostać wymierzone kary pieniężne.



Ocena bezpieczeństwa systemów informacyjnych

Warto zwrócić uwagę na jeszcze jedno nowe rozwiązanie zaproponowane w projekcie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, którym jest przyznanie właściwym CSIRT **kompetencji do przeprowadzenia oceny bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorów usług kluczowych, dostawców usług cyfrowych i przedsiębiorców komunikacji elektronicznej**. Ocena taka polegać ma na przeprowadzeniu testów bezpieczeństwa systemu informacyjnego w celu identyfikacji jego podatności. Nie jest przy tym jasne, jakie „systemy informacyjne" mają być przedmiotem audytu ze strony CSIRT – definicja „systemu informacyjnego" z projektu nowelizacji ustawy odwołuje się bowiem do definicji „systemu teleinformatycznego" z Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[4], która ma bardzo szeroki zakres i może obejmować szereg różnych systemów informatycznych, w tym komercyjne systemy do obsługi przedsiębiorstw typu ERP czy CRM. Co jednak niezwykle istotne, poddanie się ocenie bezpieczeństwa systemów informacyjnych ma być w pełni dobrowolne – może się bowiem odbyć jedynie za zgodą podmiotu krajowego systemu cyberbezpieczeństwa.

Uznanie dostawcy za dostawcę wysokiego ryzyka i polecenia zabezpieczające

Ważne jest również to, że mimo bardzo silnego sprzeciwu i wielu uwag zgłaszanych przez przedsiębiorców na wcześniejszym etapie prac nad nowelizacją UKSC, w najnowszym, marcowym projekcie nowelizacji UKSC, utrzymane zostały kompetencje ministra właściwego ds. informatyzacji w zakresie uznania dostawcy za dostawcę wysokiego ryzyka oraz wydawania poleceń zabezpieczających w przypadku wystąpienia incydentu krytycznego (więcej pisaliśmy o nich na naszym blogu), choć w obecnej wersji nowelizacji zaproponowano pewne nieznaczne zmiany.

W pierwszej kolejności, jeżeli chodzi o decyzję w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, należy zwrócić uwagę na to, że:

- przed wydaniem takiej decyzji obligatoryjne jest przeprowadzenie analizy dotyczącej wpływu konkretnych produktów, usług lub procesów na bezpieczeństwo usług;
- ewentualna decyzja uznająca dostawcę za dostawcę wysokiego ryzyka nie jest wiążąca dla przedsiębiorców komunikacji elektronicznej (z wyjątkiem przedsiębiorców telekomunikacyjnych obowiązanych posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń oraz takich przedsiębiorców komunikacji elektronicznej, którzy są równocześnie operatorami usług kluczowych), co oznacza, że podmioty te nie są objęte zakazem użytkowania produktów i usług (m.in. sprzętu i oprogramowania) wyprodukowanych przez tego dostawcę, a także nie są zobowiązane do wycofania z użytku tych produktów i usług – kwestia ta może być szczególnie istotna dla operatorów telekomunikacyjnych, którzy wybudowali infrastrukturę telekomunikacyjną na podstawie urządzeń dostawcy, który następnie został uznany za dostawcę wysokiego ryzyka;
- wprowadzona została nowa administracyjna kara pieniężna w wysokości do 50 000 zł, która może zostać nałożona na podmiot, który nie przekazuje, na wniosek uprawnionych organów, informacji o wycofywanych typach produktów, usług i procesów w zakresie objętym decyzją o uznaniu za dostawcę wysokiego ryzyka, a także możliwość nałożenia indywidualnej kary pieniężnej na kierującego takim podmiotem w wysokości do 300% jego miesięcznego wynagrodzenia.

Niezależnie od powyższego projekt nowelizacji nadal nie przewiduje możliwości złożenia wniosku o ponowne rozpatrzenie sprawy w przypadku decyzji uznającej danego dostawcę za dostawcę wysokiego ryzyka, a decyzja ta wciąż ma podlegać natychmiastowemu wykonaniu.

[4] T.j. Dz. U. z 2021 r., poz. 2070, ze zm.

W zakresie instytucji polecenia zabezpieczającego, to poza koniecznością przeprowadzenia przed ich wydaniem bardziej pogłębionej analizy nie zdecydowano się na wprowadzenie znaczących zmian w stosunku do wersji projektu nowelizacji UKSC z października 2021 r. W związku z tym zastrzeżenia dotyczące nieokreśloności tej decyzji administracyjnej, jak również wątpliwości dotyczące proponowanych rozwiązań procedury administracyjnej (m.in. w zakresie nadania takiej decyzji rygoru natychmiastowej wykonalności czy pozbawienia możliwości złożenia wniosku o ponowne rozpatrzenie sprawy) pozostają nadal aktualne, mimo zgłoszenia szeregu uwag przez podmioty zainteresowane.

Inne nowości w projekcie nowelizacji

Poza opisanymi powyżej zagadnieniami projekt nowelizacji przewiduje również inne zmiany – dokonano m.in. podziału SOC (zespołów pełniących funkcję operacyjnego centrum bezpieczeństwa) na SOC wewnętrzne (utworzone w ramach struktury operatora usługi kluczowej) i SOC zewnętrzne (zewnętrzne podmioty świadczące usługi SOC na rzecz operatora usługi kluczowej) oraz usunięto rozdział dotyczący utworzenia Funduszu Cyberbezpieczeństwa czy przepisy odnoszące się do przyznawania świadczenia teleinformatycznego (w związku z uregulowaniem obu tych kwestii w osobnej ustawie[5]).

Dalsza ścieżka legislacyjna

Projekt nowelizacji uzyskał rekomendację Stałego Komitetu Rady Ministrów i ma zostać rozpatrzony przez Komitet Rady Ministrów do spraw Bezpieczeństwa Narodowego i spraw Obronnych, a następnie wrócić do Stałego Komitetu Rady Ministrów. Prace legislacyjne powinny teraz nabrać tempa i wydaje się, że równolegle z pracami nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa procedowany powinien być projekt ustawy – Prawo komunikacji elektronicznej – z uwagi na istniejące silne powiązania pomiędzy tymi aktami prawnymi. Mając jednocześnie na uwadze długą historię projektów nowelizacji tych przepisów, pewności co do tego kiedy uchwalone zostaną ich finalne wersje i czy będą one zbieżne z obecnie przedstawionymi propozycjami – nie ma.

[5] Zob. Ustawa z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. poz. 2333).

Jak przedsiębiorcy telekomunikacyjni powinni informować użytkowników o cyberzagrożeniach?

Agnieszka Wachowska, Jakub Chlebowski

10 marca 2022 r. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) opublikowała wytyczne dotyczące informowania przez przedsiębiorców telekomunikacyjnych użytkowników o cyberzagrożeniach[1]. Opublikowanie wytycznych jest konsekwencją obowiązywania w Unii Europejskiej od grudnia 2020 r. Europejskiego kodeksu łączności elektronicznej (EKŁE), który na podstawie art. 40 ust. 3 zobowiązuje przedsiębiorców telekomunikacyjnych do informowania o występujących cyberzagrożeniach. Przedstawione przez ENISA wytyczne zawierają rekomendacje dotyczące tworzenia polityk informowania użytkowników o cyberzagrożeniach, a także *case studies* procedur już stosowanych przez wybranych przedsiębiorców telekomunikacyjnych.

Dlaczego przedsiębiorcy telekomunikacyjni powinni informować o cyberzagrożeniach?

Zgodnie z art. 40 EKŁE państwa członkowskie przy transpozycji tej dyrektywy powinny nałożyć na przedsiębiorców telekomunikacyjnych obowiązek podejmowania właściwych i proporcjonalnych środków technicznych i organizacyjnych w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług, tak aby te środki zapewniały poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka, z uwzględnieniem aktualnego stanu wiedzy i technologii. O ile legislatorzy dają przedsiębiorcom telekomunikacyjnym dowolność w wyborze stosowanych środków (ograniczając się do wskazania, że wśród możliwych do zastosowania środków jest korzystanie z szyfrowania), o tyle dodatkowym instrumentem, który ma przeciwdziałać cyberzagrożeniom, jest określony w art. 40 ust. 3 EKŁE obowiązek informowania użytkowników o takich zagrożeniach.

Zgodnie z EKŁE informowanie użytkowników powinno mieć dwie postaci:

1. „W przypadku szczególnego i znacznego zagrożenia wystąpieniem incydentu związanego z bezpieczeństwem" przedsiębiorcy telekomunikacyjni powinni poinformować „użytkowników, na których takie zagrożenie może mieć wpływ, **o wszelkich możliwych środkach ochronnych lub naprawczych, które użytkownicy mogą podjąć**".
2. „W stosownych przypadkach podmioty powinny **informować swoich użytkowników również o samym zagrożeniu**", rezygnując z informowania o możliwych do podjęcia środkach ochronnych i naprawczych.

Jednocześnie motyw 96 EKŁE przedstawia więcej szczegółów związanych z informowaniem użytkowników o cyberzagrożeniach. W przypadku szczególnych i istotnych zagrożeń dla bezpieczeństwa informacja powinna dotyczyć **nie tylko samych zagrożeń**, lecz także **środków, które użytkownicy powinni podjąć w celu ochrony bezpieczeństwa łączności**, takich jak konieczność zastosowania szczególnego rodzaju oprogramowania lub technologii szyfrowania. Przekazywanie takich informacji użytkownikom powinno być **bezpłatne**. Dodatkowo motyw 96 EKŁE precyzuje, że informowanie o zagrożeniach jest tylko jednym z elementów przeciwdziałania cyberzagrożeniom, a podjęte działania informacyjne nie powinny jednocześnie zwalniać przedsiębiorców telekomunikacyjnych „z obowiązku podjęcia na własny koszt odpowiednich i natychmiastowych środków w celu zaradzenia wszelkim zagrożeniom bezpieczeństwa oraz przywrócenia normalnego poziomu bezpieczeństwa danej usługi".

Sposobem na zapewnienie skutecznej realizacji tych obowiązków przez telekomy jest – zgodnie z art. 41 ust. 1 EKŁE – umożliwienie właściwym organom krajowym wydawania przedsiębiorcom telekomunikacyjnym wiążących instrukcji „dotyczących środków wymaganych, aby zaradzić incydentowi związanemu z bezpieczeństwem lub aby zapobiec wystąpieniu takiego incydentu".

Zasady wynikające z EKŁE miały być transponowane do polskiego porządku prawnego poprzez ustawę Prawo komunikacji elektronicznej (PKE), jednakże mimo toczących się od

[1] Zob. https://www.enisa.europa.eu/news/enisa-news/cyber-threat-warnings-the-ins-and-outs-of-consumer-outreach (dostęp: 31.03.2022).

2020 r prac w tym zakresie oraz publikowania kolejnych wersji projektu – ustawa Prawo komunikacji elektronicznej do chwili obecnej nie trafiła nawet do sejmu.

Mając na uwadze obecne prace legislacyjne, wydaje się, że transpozycja przepisów EKŁE w tym zakresie może zostać wkrótce dokonana poprzez zmianę przepisów ustawy o krajowym systemie cyberbezpieczeństwa. Zmiany takie właśnie przewiduje najnowszy projekt nowelizacji UKSC z dnia 15 marca 2022 r.[2] (projekt nowelizacji UKSC). Na podstawie przedstawionego projektu nowelizacji (art. 20f ust. 1) na przedsiębiorcę komunikacji elektronicznej (w tym przedsiębiorcę telekomunikacyjnego)[3] nałożony zostanie obowiązek publikacji na stronie internetowej informacji o:

- potencjalnych zagrożeniach związanych z korzystaniem przez użytkowników z usług komunikacji elektronicznej,
- rekomendowanych środkach ostrożności i najbardziej popularnych sposobach zabezpieczania telekomunikacyjnych urządzeń użytkowników przed złośliwym lub szpiegującym oprogramowaniem,
- przykładowych konsekwencjach braku lub nieodpowiedniego zabezpieczenia telekomunikacyjnych ich urządzeń.

Dodatkowo w sytuacji szczególnego i znacznego zagrożenia wystąpienia incydentu telekomunikacyjnego[4] przedsiębiorca komunikacji elektronicznej ma obowiązek poinformowania użytkowników na takie zdarzenie narażonych. Obowiązek ten obejmuje informację o zagrożeniu, możliwych środkach, które użytkownicy mogą podjąć, oraz związanych z tym kosztach. Jeżeli wpływ incydentu telekomunikacyjnego na dostępność świadczonych usług jest istotny, przedsiębiorca komunikacji elektronicznej ma jednocześnie obowiązek poinformowania o takim incydencie na swojej stronie internetowej.

Realizacja obowiązków dotyczących informowania użytkowników o incydentach telekomunikacyjnych, w tym sposób przekazania takiej informacji, będzie również wzmocniona wynikającym z art. 20h ust. 5 projektu nowelizacji UKSC uprawnieniem Prezesa Urzędu Komunikacji Elektronicznej (Prezes UKE), który w drodze decyzji będzie mógł nałożyć na przedsiębiorcę komunikacji elektronicznej obowiązek podania do publicznej wiadomości informacji o wystąpieniu poważnego incydentu telekomunikacyjnego, gdyby wykorzystywane przez Prezesa UKE kanały komunikacji (strona Biuletynu Informacji Publicznej Urzędu Komunikacji Elektronicznej) były niewystarczające do ochrony interesu publicznego.

W zakresie obowiązków informowania o cyberzagrożeniach należy również zwrócić uwagę na przedstawioną propozycję ustawy Prawo komunikacji elektronicznej (PKE)[5], zgodnie z którą (art. 279 ust. 2 pkt. 5 PKE) – w przypadku przyjęcia PKE w kształcie obowiązującym na kwiecień 2022 r. – ustawodawca będzie zobowiązywać przedsiębiorców telekomunikacyjnych, aby zakres podejmowanych przez nich działań związanych z cyberzagrożeniami i sposób informowania o takich zagrożeniach precyzowali w umowach o świadczenie usług komunikacji elektronicznej z użytkownikami, a także informowali o tym użytkowników jeszcze na etapie udzielania informacji przedumownych.

Zasady informowania o cyberzagrożeniach

ENISA na podstawie praktyk obecnie stosowanych przez sektor telekomunikacji w opublikowanych wytycznych wskazała, że informowanie użytkowników o cyberzagrożeniach **powinno być oparte na dwóch stosowanych przez przedsiębiorcę strategiach, którymi są**:

1. **Strategia cyberbezpieczeństwa** – polegająca na zdefiniowaniu wysokopoziomowych planów telekomów na budowanie odporności na zagrożenia.
2. **Strategia komunikacji z użytkownikami** – polegająca na tworzeniu zasad komunikacji poprzez wybór odpowiedniego stylu komunikacji, użycie właściwych kanałów i planowanie efektów podejmowanych działań.

Połączenie obu tych strategii stosowanych przez przedsiębiorcę telekomunikacyjnego będzie pozwalało mu zdefiniować, w jaki sposób przeciwdziałać cyberzagrożeniom przez samych użytkowników.

[2] Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw z dnia 15 marca 2022 r., https://legislacja.rcl.gov.pl/projekt/12337950 (dostęp: 11.04.2022 r.)

[3] Zgodnie z projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw z dnia 15 marca 2022 r., przedsiębiorca komunikacji elektronicznej to przedsiębiorca telekomunikacyjny lub podmiot świadczący publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów.

[4] Zgodnie z definicją zawartą w projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw z dnia 15 marca 2022 r. za incydent telekomunikacyjny uznaje się każde zdarzenie, które ma rzeczywisty, niekorzystny skutek dla bezpieczeństwa sieci i usług komunikacji elektronicznej

[5] Projekt ustawy Prawo komunikacji elektronicznej z dnia 2 grudnia 2021 r., https://mc.bip.gov.pl/prawo-i-prace-legislacyjne/projekty-aktow-prawnych-mc/projekt-ustawy-prawo-komunikacji-elektronicznej.html (dostęp: 11.04.2022 r.)

W zależności od wyboru sposobu informowania o zagrożeniach cyberbezpieczeństwa ENISA wyróżnia dwie kategorie komunikacji z użytkownikami:

- Informacje przeznaczone do budowania ogólnej świadomości na temat potencjalnych ryzyk.
- Informacje dotyczące konkretnych cyberzagrożeń (np. phishing, kradzież danych, ataki DoS) z opisem działań mających na celu minimalizację wystąpienia tych ryzyk – z wytycznych wynika, że **tego typu komunikacja jest skuteczniejsza**, zwłaszcza gdy przekazywane użytkownikom informacje dotyczą bardziej konkretnych zagrożeń i są kierowane do użytkownika bezpośrednimi kanałami (lepiej e-mail lub SMS niż post na portalu społecznościowym lub komunikat prasowy).

Jeśli chodzi o informowanie o konkretnym cyberzagrożeniu, ENISA proponuje następującą procedurę obsługi takiego zagrożenia, która została podzielona na trzy etapy:

1. **Etap oceny zagrożenia** – na tym etapie przedsiębiorcy telekomunikacyjni powinni ***case-by-case*** **ocenić, czy komunikacja z użytkownikiem jest potrzebna**, w szczególności powinni oni zadać sobie pytanie, na ile poważne i prawdopodobne jest to zagrożenie, czego dotyczy i jaki wpływ może mieć na użytkowników (np. czy poinformowanie nie spowoduje zwiększenia ryzyka wystąpienia incydentu cyberbezpieczeństwa). ENISA jednocześnie wskazuje, że telekomy powinny mieć świadomość, iż decyzja o poinformowaniu użytkownika nie powinna być podejmowana zbyt pochopnie – zbyt częsta aktywność telekomów może doprowadzić do sytuacji, że użytkownicy zaczną ignorować otrzymywane wiadomości.
2. **Etap komunikacji** – na tym etapie przedsiębiorcy telekomunikacyjni powinni **wybrać odpowiednią formę komunikacji z użytkownikiem**, aby najlepiej odpowiedzieć na pojawiające się zagrożenie. ENISA rekomenduje, aby przedsiębiorcy telekomunikacyjni ocenili w szczególności, kogo będzie dotyczyć zagrożenie, jaki będzie najlepszy kanał komunikacji z zagrożoną grupą użytkowników oraz jakie środki powinien podjąć sam użytkownik, przy czym telekomy powinny pamiętać, że podstawową zasadą komunikacji z użytkownikiem jest **tworzenie prostych komunikatów zawierających tylko praktyczne informacje** z uwagi na ich największą skuteczność w dotarciu do grupy docelowej.
3. **Etap oceny skutków komunikacji** – na tym etapie przedsiębiorcy telekomunikacyjni powinni dokonać **estymacji, na ile skuteczne były publikowane przez nich komunikaty w przeciwdziałaniu cyberzagrożeniom**. ENISA rekomenduje, aby telekomy definiowały obiektywnie weryfikowalne parametry, które pozwolą na ocenę skuteczności stosowanej komunikacji (m.in. poprzez weryfikację, czy użytkownicy podjęli zalecane im działania).

Ryzyka związane z komunikacją z użytkownikami

ENISA jednocześnie wskazuje na wyzwania, jakie stoją przed przedsiębiorcami przy komunikacji z użytkownikami. Najważniejszymi z tych wyzwań są:

1. **Ryzyko „zmęczenia" użytkowników komunikatami** – zbyt częsta lub zbyt skomplikowana komunikacja, a także wymaganie od użytkowników podejmowania zbyt wielu działań mogą doprowadzić do sytuacji, że użytkownicy zaczną ignorować otrzymywane komunikaty, oraz spowodują, że cele, do jakich dążą przedsiębiorcy telekomunikacyjni poprzez publikowane informacje, nie zostaną osiągnięte.
2. **Ryzyko wykorzystania komunikacji do oszustw** – niewłaściwie sformułowane komunikaty mogą być wykorzystane do działań przestępczych (m.in. phishingu). Źle zaprojektowane informacje mogą doprowadzić do sytuacji, że użytkownik nie będzie w stanie odróżnić informacji telekomów o realnym zagrożeniu od komunikacji stanowiącej próbę oszustwa.
3. **Ryzyko bagatelizowania innych działań** – informowanie użytkowników powinno być tylko działaniem uzupełniającym w stosunku do innych czynności, które przedsiębiorcy telekomunikacyjni powinni podejmować, aby minimalizować ryzyko wystąpienia incydentu cyberbezpieczeństwa. W szczególności powinni podejmować działania techniczne i organizacyjne, które będą przeciwdziałać cyberzagrożeniom lub łagodzić ich skutki (np. poprzez automatyczne blokowanie wiadomości SMS stanowiących próbę oszustwa).

Podsumowanie

Przygotowane przez ENISA wytyczne stanowią zbiór dobrych praktyk, którymi przedsiębiorcy telekomunikacyjni powinni się kierować przy informowaniu użytkowników o zagrożeniach, aby skutecznie chronić użytkowników, a także – jeśli to konieczne – aktywnie włączać ich do systemu ochrony przed tymi zagrożeniami. Skuteczne osiągnięcie tego jest możliwe tylko poprzez umiejętne kształtowanie przekazu o cyberzagrożeniach. Jednocześnie przedsiębiorcy telekomunikacyjni powinni pamiętać, że podejmowanie działań w zakresie informowania użytkowników nie tylko służy ochronie świadczonych usług przed cyberzagrożeniami, ale jest również ustawowym obowiązkiem (zarówno zgodnie z art. 175e ust. 2 Prawa telekomunikacyjnego, jak i na podstawie EKŁE, a za nim art. 20f ust. 1 UKSC) którego niewypełnienie może prowadzić do sankcji w postaci kary pieniężnej w wysokości **3% przychodu osiągniętego w poprzednim roku kalendarzowym**.

Outsourcing IT w decyzji PUODO

Xawery Konarski

W dniu 19 stycznia 2022 r. Prezes Urzędu Ochrony Danych Osobowych (PUODO) nałożył **rekordową karę pieniężną w wysokości 4,9 mln złotych na administratora** (Fortum Marketing and Sales Polska S.A.), równocześnie wymierzając karę 250 tys. złotych podmiotowi przetwarzającemu (procesorowi) – PIKA S.A.

Podstawą do wszczęcia postępowania i nałożenia ww. kar było naruszenie ochrony danych, polegające na skopiowaniu danych klientów administratora przez nieuprawnione osoby. Do sytuacji tej doszło w trakcie wprowadzania, przez podmiot przetwarzający, zmian w systemie IT administratora. O incydencie administrator powiadomił zarówno organ, jak i – w wykonaniu wezwania PUODO – zainteresowane podmioty danych.

Podstawą ukarania administratora było – wynikłe z zaniedbań procesora – niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych, a także niedokonanie odpowiedniej weryfikacji podmiotu przetwarzającego. Szczególnie istotne są w związku z tym argumenty podniesione przez PUODO w związku z zarzutem braku należytego nadzoru przez administratora.

Po pierwsze organ podkreślił, że przed zawarciem umowy powierzenia przetwarzania danych administrator jest zobowiązany do przeprowadzenia weryfikacji podmiotu przetwarzającego. Z tego obowiązku nie zwalnia go okoliczność wcześniejszej – jak to miało miejsce w niniejszej sprawie – długotrwałej współpracy z podmiotem przetwarzającym. W tym kontekście bez znaczenia jest również, że uprzednio nie doszło do incydentów bezpieczeństwa, a podmiot przetwarzający jest jednym z liderów w dziedzinie świadczonych usług.

Po drugie organ zarzucił administratorowi, że pomimo posiadanych procedur oraz wiedzy nie prowadził – w trakcie trwania umowy – nadzoru nad tym, czy wdrożenie IT realizowane przez podmiot przetwarzający przebiega zgodnie z powszechnie obowiązującymi standardami oraz umową powierzenia przetwarzania danych osobowych.

Po trzecie PUODO wskazał, że administrator przed wszczęciem postępowania nie przeprowadzał w podmiocie przetwarzającym audytów, w tym inspekcji, w celu sprawdzenia, czy PIKA w sposób prawidłowy realizuje swoje obowiązki wynikające z RODO. Możliwość przeprowadzenia takich audytów, w tym inspekcji, wynika z art. 28 ust. 3 lit. h rozporządzenia 2016/679, stosownie do którego umowa powierzenia przetwarzania danych osobowych ma stanowić, że podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. Administrator powinien bowiem w czasie korzystania przez niego z usług podmiotu przetwarzającego dysponować wiedzą, czy i w jaki sposób podmiot, któremu powierzył przetwarzanie danych osobowych, spełnia wymogi określone w RODO. Nie ulega wątpliwości, że najskuteczniejszym sposobem zapewnienia sobie tej wiedzy przez administratora jest dokonywanie w podmiocie przetwarzającym stosownych audytów, w tym inspekcji. Takich środków bezpieczeństwa administrator jednak nie zastosował, co w konsekwencji przyczyniło się do wystąpienia naruszenia ochrony danych osobowych.

Decyzja wydana w analizowanej sprawie ma **bardzo istotne znaczenie dla rynku usług outsourcingu IT**. Nałożenie rekordowej kary pieniężnej uwypukliło ryzyka po stronie zamawiającego te usługi (administratora danych). Może on bowiem zostać ukarany za zaniechania podmiotu przetwarzającego. W tym kontekście szczególnie istotny jest obowiązek weryfikacji podmiotu przetwarzającego zarówno na etapie zawarcia umowy powierzenia danych, jak i jej realizacji. Mimo że nie wynika to bezpośrednio z przepisów, PUODO podkreśliło w tym względzie znaczenie audytów jako narzędzia do weryfikacji wypełnienia przez procesora wymogów RODO oraz umowy powierzenia.

Decyzja

Dostawca narzędzi IT odpowie za wykorzystanie ich przez kartel

dr Katarzyna Menszig-Wiese (specjalistka w zakresie prawa konkurencji), Agnieszka Wachowska

Zmowy między przedsiębiorcami, którzy zamiast rywalizować, wolą po cichu współpracować z konkurentami, pozostają bolączką polskiego rynku. Ukryty charakter tego typu praktyk utrudnia ich wykrywanie i efektywne zwalczanie. Prezes Urzędu Ochrony Konkurencji i Konsumentów (UOKiK) sięgnął więc po dotychczas niewykorzystywany w Polsce instrument i będzie próbował przypisać odpowiedzialność antymonopolową nie tylko bezpośrednim uczestnikom porozumienia, lecz także „pomocnikom" dostarczającym narzędzi wykorzystywanych do wdrożenia zmowy. Czy dostawcy rozwiązań IT mają się czego obawiać?

Porozumienie na rynku farmaceutycznym

Pod koniec lutego Prezes UOKiK poinformował o wszczęciu postępowania antymonopolowego dotyczącego sprzecznej z prawem konkurencji wymiany informacji między hurtowniami farmaceutycznymi. Miało do niej dochodzić przy wykorzystaniu oprogramowania zainstalowanego w aptekach. Za jego pośrednictwem konkurencyjne hurtownie miały pozyskiwać m.in. informacje o stosowanych przez nie cenach, rabatach i wysokości marży. Tego typu sprawy stanowią klasykę gatunku i częsty przedmiot oceny organu antymonopolowego. Wymiana informacji o znaczeniu biznesowym jest postrzegana bardzo krytycznie na gruncie prawa konkurencji. Pozwala bowiem na zastąpienie rywalizacji koordynacją, co negatywnie wpływa na interes konsumentów. W tej sprawie precedensowe jest to, że zarzuty postawione zostały nie tylko bezpośrednim uczestnikom zakazanego porozumienia, lecz także podmiotom, które miały dostarczyć im narzędzi do jego implementacji. Czy jednak dla takiego nowego trendu istnieje podstawa prawna?

Odpowiedzialność antymonopolowa pomocnika kartelu

Ustawa o ochronie konkurencji i konsumentów nie przewiduje kar dla „pomocników" kartelu. O ile w prawie karnym i prawie cywilnym regulacja kodeksowa dostarcza odpowiedniej podstawy dla przypisania odpowiedzialności również innym podmiotom niż bezpośredni sprawcy, o tyle w prawie administracyjnym (a do niego zalicza się prawo konkurencji) próżno szukać analogicznego przepisu. Jak więc Prezes UOKiK prawnie uzasadni postawienie zarzutów dostawcom oprogramowania wykorzystywanego rzekomo przez hurtownie farmaceutyczne do wymiany informacji? Będzie to wymagało od niego sporej dozy prawniczej ekwilibrystyki.

Kluczem będzie tu najpewniej prawo konkurencji Unii Europejskiej. Choć traktatowa regulacja antymonopolowa także nie przewiduje wyraźnej podstawy do pociągania do odpowiedzialności pomocników kartelu, to w 2015 r. Trybunał Sprawiedliwości Unii Europejskiej wyinterpretował ją z dotychczasowego orzecznictwa. W wyroku w sprawie AC-Treuhand II[1] wskazano mianowicie, że Komisja Europejska (jako unijny organ ochrony konkurencji) w odniesieniu do pomocników kartelu *„powinna udowodnić, że dane przedsiębiorstwo zamierzało przyczynić się swoim zachowaniem do wspólnych celów realizowanych przez ogół uczestników i że wiedziało ono o postępowaniu planowanym lub wprowadzanym w życie przez inne przedsiębiorstwa w dążeniu do tych samych celów lub że mogło to rozsądnie przewidzieć i było gotowe zaakceptować takie ryzyko"*. Prościej ujmując, **jeżeli przedsiębiorca *przyczynił się* do naruszenia prawa konkurencji, a *wiedział*, w czym uczestniczy, lub nawet tylko *mógł się tego domyślić*, to organ antymonopolowy może go ukarać. I to surowo**.

Czy dostawcy narzędzi IT powinni się obawiać nowego trendu?

Dostawcom narzędzi IT słusznie może się jeżyć włos na głowie. Przesłanka „przyczynienia się" może być wykładana bardzo szeroko.. Nie będzie też zaskoczeniem, jeżeli organ będzie przypisywał przedsiębiorcom niesłychaną wprost bystrość i zdolność przewidzenia, w jakim celu wykorzystane zostanie dostarczone przez nich narzędzie. Czy jednak powołanie się na unijne orzecznictwo zaradzi na brak wyraźnej podstawy do karania pomocników kartelu w polskich przepisach?

[1] Wyrok TSUE z dnia 22 października 2015 r., C-194/14 P.

W ocenie dr Katarzyny Menszig-Wiese, radczyni prawnej i Senior Associate w zespole prawa konkurencji naszej Kancelarii nie. A w każdym razie – nie zawsze. Choć możemy się spodziewać, że polski organ ochrony konkurencji spróbuje przeszczepić na nasz grunt unijny wzorzec, to przed Sądem Ochrony Konkurencji i Konsumentów będzie **można walczyć o zmianę decyzji uznającej dostawcę narzędzi IT współodpowiedzialnym za antykonkurencyjne porozumienie**. Na gruncie obecnie obowiązujących przepisów można zbudować silną argumentację przeciwko próbom rozciągania odpowiedzialności antymonopolowej na pomocników antykonkurencyjnych porozumień. W prawie UE potrzeba zapewnienia efektywności ochronie konkurencji mogła posłużyć za uzasadnienie dla nowej koncepcji odpowiedzialności antymonopolowej. Natomiast na gruncie polskiej ustawy większą wagę przypisywać trzeba będzie zasadzie określoności czynów zabronionych, czyli temu, że **dla przedsiębiorców musi być jasne, co jest zakazane pod groźbą kary. Obecnie żaden przepis nie zakazuje wyraźnie pomocnictwa w antykonkurencyjnym porozumieniu**.

Jednocześnie, zarysowany powyżej kierunek rozwoju praktyki egzekwowania prawa konkurencji powinien stanowić ważny sygnał dla przedsiębiorców z branży IT **do zachowania większej czujności, a także do wdrożenia mechanizmów minimalizowania ryzyka antymonopolowego**. Wydaje się bowiem już przesądzone, że Prezes UOKiK rozpocznie nową praktykę decyzyjną karania również pomocników kartelu. Tym samym, dostawcy IT powinni być czujni i przede wszystkim mieć rozeznanie i świadomość co do tego, jakie działania są niedozwolone z punktu widzenia prawa konkurencji i jakich funkcjonalności dotyczących wymieniany danych między konkurentami nie powinni ofertować swoim klientom. Może się jednak zdarzyć taka sytuacja, że dostarczone przez dany podmiot narzędzie IT zostanie bez jego wiedzy, lub nawet wbrew umowie, wykorzystane przez klientów dla antykonkurencyjnych celów. W takim przypadku nie można wykluczyć, że Prezes UOKiK przypisze odpowiedzialność antymonopolową także dostawcy narzędzia. Uzna bowiem, że przedsiębiorca mógł się domyślić, jak zostanie wykorzystany jego produkt. W razie stwierdzenia naruszenia zakazu porozumień Prezes UOKiK może nałożyć na przedsiębiorcę karę administracyjną w wysokości do 10% obrotu osiągniętego w roku obrotowym poprzedzającym rok nałożenia kary. Ustawa o ochronie konkurencji i konsumentów przewiduje nadto sankcje dla managerów do 2 mln zł.

Co powinny teraz zrobić firmy z branży IT?

Jak dostawca narzędzi IT może zabezpieczyć się przed odpowiedzialnością antymonopolową? Najważniejsza jest świadomość istnienia tego ryzyka.

Po pierwsze, już na etapie przedkontraktowym potrzebna jest weryfikacja, czy cele, do których osiągnięcia mają posłużyć dostarczane narzędzia, nie mają antykonkurencyjnego charakteru, np. czy oprogramowanie nie będzie umożliwiało użytkownikom wymiany informacji o cenach lub wpływania na możliwość kształtowania cen przez dystrybutorów. Tym samym już na etapie analizowania zapytania ofertowego oraz składania oferty dostawcy IT powinni być czujni, czy z takiego zapytania wprost lub pośrednio nie wynika, że oprogramowanie, która ma być przez nich dostarczane, może służyć niedozwolonym działaniom.

Po drugie, zasadne jest uwzględnienie ryzyka antymonopolowego po stronie dostawcy przy negocjowaniu treści umowy. Odpowiednio sformułowane postanowienia mogą zabezpieczyć dostawców IT przed przykrą niespodzianką. Przykładowo jeśli dostawca IT ma w ramach umowy wykonać analizę przedwdrożeniową, z której wyniknie, że oprogramowanie, które ma być przez niego wdrażane, może służyć niedozwolonej wymianie informacji – wykonawca taki powinien mieć możliwość odstąpienia od umowy bez obarczania go odpowiedzialnością za takie działanie.

Po trzecie, warto być przygotowanym na wypadek podjęcia przez Prezesa UOKiK czynności dochodzeniowych, takich jak kontrola lub przeszukanie w siedzibie przedsiębiorcy. W takiej sytuacji sprawdzi się posiadanie odpowiedniej polityki postępowania na wypadek wizyty przedstawicieli organu. Jeżeli natomiast Prezes UOKiK zażąda informacji i dokumentów w związku ze wszczętym postępowaniem, należy potraktować to bardzo poważnie i terminowo przygotować odpowiedź, najlepiej konsultując jej brzmienie z doradcą antymonopolowym.

Zarysowana na wstępie sprawa najpewniej jeszcze w tym roku zakończy się wydaniem decyzji administracyjnej. Precedensowy krok otworzy drogę do szerszego stosowania nowej koncepcji odpowiedzialności antymonopolowej wobec dostawców narzędzi IT.

Publikacja projektu Aktu w sprawie danych (Data Act) – rozporządzenia w sprawie zharmonizowanych zasad dotyczących sprawiedliwego dostępu do danych i korzystania z nich

MarcinRęgorowicz

23 lutego 2022 r. Komisja Europejska opublikowała projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania, zwanego jako Data Act (Akt w sprawie danych). Regulacja, która ma stanowić jeden z elementów realizacji szerszej, tzw. Europejskiej Strategii w zakresie danych, zawiera propozycję licznych rozwiązań legislacyjnych, których wejście w życie będzie miało istotny wpływ na funkcjonowanie europejskiej gospodarki.

Akt w sprawie danych

Głównym celem proponowanego rozporządzenia, jak i całej Europejskiej Strategii w zakresie danych przyjętej przez Komisję Europejską w lutym 2020 r. jest zapewnienie rozwoju europejskiej gospodarce opartej na danych przede wszystkim przez budowę jednolitego rynku danych, gwarantującego swobodny przepływ i korzystanie z danych w granicach UE i między sektorami z korzyścią dla obywateli.

W celu realizacji tego założenia w ramach Aktu w sprawie danych zaproponowano wiele regulacji, które mają służyć przede wszystkim wykorzystaniu potencjału rosnącej ilości danych, generowanych w ramach gospodarek Unii Europejskiej, zwłaszcza poprzez zwiększenie dostępności tych danych dla różnych grup podmiotów, minimalizację barier dla przepływu czy wykorzystania tych danych, a przez to – pobudzanie innowacyjności i wspieranie budowy gospodarki opartej na danych.

Równolegle celem projektowanych przepisów jest zapewnienie „sprawiedliwego podziału wartości danych między podmiotami gospodarki opartej o dane", zwiększenie dostępu do danych czy zwiększenie ochrony praw podstawowych osób fizycznych.

Kluczowe elementy proponowanej regulacji

Powyższe cele mają zostać osiągnięte dzięki wprowadzeniu szeregu przepisów, które będą miały daleko idące skutki w zasadzie dla wszystkich uczestników rynku.

Przede wszystkim w ramach proponowanego rozporządzenia wprowadzono siatkę pojęciową, zawierającą wiele fundamentalnych definicji, takich jak „**dane**" (wszelkie cyfrowe odwzorowania działań, faktów lub informacji oraz wszelkie kompilacje takich działań, faktów lub informacji, w tym w formie zapisu dźwiękowego, wizualnego lub audiowizualnego), „**posiadacz danych**", „**użytkownik**" czy „**interoperacyjność**".

Projekt rozporządzenia wprowadza również przepisy zwiększające dostęp do danych dla szerokiego kręgu podmiotów, w tym konkretne uprawnienia dla użytkowników urządzeń czy powiązanych usług generujących dane. Proponowane regulacje wprowadzają konkretne uprawnienia użytkowników do żądania wydania danych wygenerowanych przez produkty lub powiązane z nimi usługi czy prawo żądania przekazania tych danych osobom trzecim (np. na potrzeby świadczenia usług z pominięciem pierwotnego producenta produktu czy dostawcy usługi). Skuteczność powyższych uprawnień wzmocniona zostanie przez wprowadzenie wymogu projektowania produktów i świadczenia powiązanych z nimi usług w ten sposób, aby dane generowane w wyniku korzystania z nich były domyślnie łatwo, bezpiecznie oraz – w razie potrzeby i w stosownych przypadkach – bezpośrednio dostępne dla użytkownika oraz łatwo przenoszalne. Dodatkowo producenci produktów czy dostawcy powiązanych usług zostaną obciążeni obowiązkiem informacyjnym w stosunku do użytkowników, obejmującym informacje o samych danych oraz możliwości uzyskania dostępu do nich.

Na podstawie Aktu o danych dodatkowe uprawnienia do dostępu do danych generowanych i przetwarzanych w sektorze prywatnym mają uzyskać podmioty publiczne, w tym organy administracji krajowej czy europejskiej.

Ważnym elementem proponowanych regulacji są również przepisy dotyczące zapewnienia łatwości przenoszenia danych w celu ułatwienia zmiany dostawców usług przetwarzania danych w chmurze. Przede wszystkim dostawcy zostaną zobowiązani do usuwania wszelkich przeszkód technicznych, handlowych czy umownych, które mogłyby utrudniać ich klientom rozwiązywanie umów czy zawarcie nowych umów z innymi dostawcami, przenoszenia danych czy utrzymywanie równoważnych funkcjonalnie usług w środowiskach innych dostawców. W tym zakresie mają również zostać przez Komisję zaproponowane wzorcowe postanowienia umowne.

Oczywiście całość regulacji dopełniona jest systemem sankcji w modelu zbliżonym do rozwiązań znanych z regulacji w zakresie danych osobowych – zwłaszcza RODO oraz uprawnieniami do wnoszenia skarg do właściwych organów.

W związku ze zmianami proponowane są również zmiany w zakresie Dyrektywy 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych (w tym zmiany zakresu stosowania prawa *sui generis* do baz danych) w celu dostosowania tych przepisów do potrzeb wynikających z projektowanych przepisów Aktu w sprawie danych.

Co dalej?

Bez wątpienia proponowane przepisy Aktu w sprawie danych będą mieć znaczący wpływ na funkcjonowanie europejskiego rynku cyfrowego i wywrze bezpośrednie skutki w działalności podmiotów z wielu branż gospodarki, których działalność coraz częściej opiera się na generowaniu i przetwarzaniu danych: od przedsiębiorstw świadczących usługi przetwarzania danych w chmurze, przez podmioty wdrażające rozwiązania z zakresu tzw. internetu rzeczy (IoT), aż po producentów sprzętu AGD, który coraz częściej generuje znaczące ilości danych (nierzadko niezbędne do jego prawidłowego działania). Szeroki zakres nowych regulacji będzie wymagać od organizacji podjęcia istotnych działań w celu zapewnienia zgodności z nowymi przepisami. Z tego powodu mimo wczesnego etapu legislacyjnego proponowanego rozporządzenia (projekt będzie musiał przejść w dalszej kolejności standardową procedurę legislacyjną – w tym kolejne czytania i głosowania w Radzie Unii Europejskiej i Parlamencie Europejskim) oraz późniejszego *vacatio legis* (proponowany okres 12 miesięcy), uczestnicy rynku powinni jak najwcześniej zacząć proces dostosowania swojej działalności do nowych regulacji.

Data Act – jak wpłynie na umowy chmurowe?

Karolina Grochecka-Goljan

W dniu 23 lutego 2022 r. został opublikowany projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych) – tzw. Data Act[1].

Czy propozycje postanowień Data Act wpłyną na umowy chmurowe?

Plan wyjścia z chmury obliczeniowej (*exit plan*)

Jak wskazywaliśmy w newsletterze IT-Tech 1/2022, dobrze opracowany *exit plan* jest potężnym narzędziem w rękach zamawiającego chmurę obliczeniową. Pozwala uniknąć zjawiska *vendor lock-in* lub je zminimalizować, zadziałać szybko w sytuacji kryzysowej, a także ustalić zakres obowiązków wykonawcy na etapie, gdy stosunki między nim a zamawiającym są poprawne, a tym samym – kiedy jest to jeszcze możliwe.

Wskazywaliśmy również na poradniki i wytyczne dotyczące chmury, które zawierają wymagania odnośnie do opracowania planu wyjścia z chmury obliczeniowej. Zgodnie z poradnikami i wytycznymi podstawą zastosowania planu wyjścia powinny być odpowiednie klauzule umowne związane z rozwiązaniem umowy, które miałyby m.in.:

1. zapewniać użytkownikowi możliwość rozwiązania umowy i przeniesienia danych w razie potrzeby;
2. zobowiązywać dostawcę do współpracy podczas przenoszenia powierzonych mu danych, systemów lub aplikacji do innego dostawcy usług lub bezpośrednio do infrastruktury użytkownika.

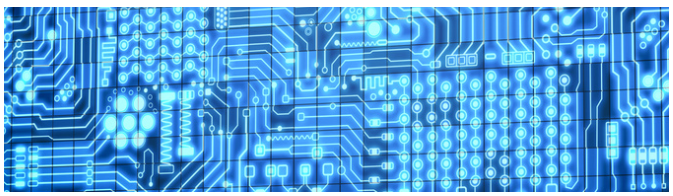
Przedmiotowe poradniki i wytyczne nie mają jednak charakteru prawa powszechnie obowiązującego. Oczywiście dostawcy, którzy chcą się liczyć na rynku usług chmurowych, powinni spełniać wymagania płynące z publikowanych poradników i wytycznych, jednakże za brak stosowania powyższych zasad nie mogą go spotkać żadne sankcje, a także użytkownicy chmury nie mają obecnie żadnych narzędzi do tego, aby domagać się wprowadzenia odpowiednich postanowień do umów chmurowych.

Czy proponowane przepisy Data Act zmienią sytuację zamawiających i wykonawców?

Obowiązek zapewnienia przejścia na inne usługi przetwarzania danych?

Projekt Data Act zawiera propozycje postanowień gwarantujących możliwość przejścia na inne usługi przetwarzania danych. Co istotne, jeśli zaproponowany projekt regulacji zostanie przyjęty, to z uwagi na jego charakter – tj. formę rozporządzenia – **będzie on, podobnie jak obecnie RODO, obowiązywać bezpośrednio, bez konieczności implementacji do krajowych porządków prawnych**.

Zgodnie z projektem art. 23 Data Act dostawcy usług przetwarzania danych mają obowiązek wprowadzić środki przewidziane w art. 24–26 Data Act (tj. postanowienia umowne dotyczące zmiany usług przetwarzania danych, stopniowego wycofywania opłat z tytułu zmiany dostawcy oraz związane z aspektami technicznymi zmiany dostawcy), aby zapewnić klientom korzystającym z ich usług możliwość przejścia na inną usługę przetwarzania danych, obejmującą ten sam rodzaj usług, świadczoną przez innego dostawcę usług.



[1] Tekst Data Act w różnych wersjach językowych jest dostępny tutaj: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0068 (dostęp: 21.04.2022).

Dostawcy usług przetwarzania danych[2] w szczególności usuwają przeszkody handlowe, techniczne, umowne i organizacyjne, które utrudniają klientom:

1. **wypowiedzenie umowy o świadczenie usługi** po upływie okresu wypowiedzenia wynoszącego maksymalnie 30 dni kalendarzowych;
2. **zawarcie nowych umów z innym dostawcą** usług przetwarzania danych, obejmujących ten sam rodzaj usług;
3. **przenoszenie ich danych, aplikacji i innych aktywów cyfrowych do innego dostawcy** usług przetwarzania danych;
4. **utrzymanie równoważności funkcjonalnej usługi w środowisku informatycznym innego dostawcy** lub innych dostawców usług przetwarzania danych, obejmujących ten sam rodzaj usług, zgodnie z art. 26.

Umowa a zmiana dostawcy usług przetwarzania danych

Data Act precyzuje, że **prawa klienta i obowiązki dostawcy usług** przetwarzania danych w odniesieniu **do zmiany dostawcy** takich usług muszą być **jasno określone w pisemnej umowie**.

W umowie powinny być określone co najmniej następujące elementy:

1. Klauzule umożliwiające klientowi, na jego wniosek, **przejście na usługę przetwarzania danych oferowaną przez innego dostawcę usług przetwarzania danych lub przeniesienie wszystkich danych, aplikacji i aktywów cyfrowych wygenerowanych bezpośrednio lub pośrednio przez klienta do systemu lokalnego**:

- w szczególności klauzule umożliwiające ustanowienie **obowiązkowego maksymalnego okresu przejściowego wynoszącego 30 dni kalendarzowych**, podczas którego dostawca usług przetwarzania danych:
    1. wspomaga i – jeżeli jest to technicznie wykonalne – kończy proces zmiany dostawcy;
    2. zapewnia pełną ciągłość świadczenia odpowiednich funkcji lub usług.

2.Wyczerpująca specyfikacja wszystkich kategorii danych i aplikacji, które można eksportować w trakcie procesu zmiany dostawcy, w tym co najmniej:

- wszystkich danych importowanych przez klienta w momencie zawarcia umowy o świadczenie usług oraz
- wszystkich danych i metadanych utworzonych przez klienta w wyniku korzystania z usługi w okresie jej świadczenia, w tym m.in. parametrów konfiguracji, ustawień zabezpieczeń, praw dostępu i rejestrów dostępu do usługi.

3. Minimalny okres, w którym można odzyskać dane, wynoszący co najmniej 30 dni kalendarzowych, rozpoczynający się po zakończeniu okresu przejściowego uzgodnionego między klientem a dostawcą usług, tj. maksymalnego okresu przejściowego wynoszącego 30 dni kalendarzowych.

Aspekty techniczne zmiany dostawcy

Propozycje przepisów Data Act ustanawiają również obowiązki w zakresie aspektów technicznych zmiany dostawcy.

Dostawcy usług przetwarzania danych, które to usługi dotyczą skalowalnych i elastycznych zasobów obliczeniowych ograniczonych do elementów infrastruktury, takich jak serwery, sieci i zasoby wirtualne niezbędne do obsługi infrastruktury, ale nie zapewniają dostępu do usług operacyjnych, oprogramowania ani aplikacji, które są przechowywane, przetwarzane w inny sposób lub wdrażane na tych elementach infrastruktury, muszą zapewnić klientowi po przejściu na usługę obejmującą ten sam rodzaj usługi, oferowaną przez innego dostawcę usług przetwarzania danych, równoważność funkcjonalną w korzystaniu z nowej usługi.

[2] Zgodnie z art. 2 Data Act „»usługa przetwarzania danych« oznacza usługę cyfrową inną niż usługa online w zakresie treści zdefiniowana w art. 2 pkt 5 rozporządzenia (UE) 2017/1128, świadczoną klientowi, która umożliwia administrowanie na żądanie skalowalnym i elastycznym zbiorem scentralizowanych, rozproszonych lub wysoce rozproszonych zasobów obliczeniowych do wspólnego wykorzystywania oraz szeroki dostęp zdalny do tego zbioru”.

W przypadku usług innych niż usługi dotyczące skalowalnych i elastycznych zasobów obliczeniowych ograniczonych do elementów infrastruktury dostawcy muszą:

1. **publicznie i bezpłatnie udostępnić otwarte interfejsy**;
2. **zapewnić zgodność** z otwartymi specyfikacjami interoperacyjności lub europejskimi normami interoperacyjności określonymi zgodnie z art. 29 ust. 5 Data Act.

Jeżeli takie standardy nie istnieją, dostawca, na wniosek klienta, eksportuje wszystkie wygenerowane lub współwygenerowane dane (w tym formaty i struktury danych) do ustrukturyzowanego, powszechnego i nadającego się do odczytu maszynowego formatu.

W art. 28 Data Act wskazano też wymagania, które muszą zostać spełnione przez operatorów przestrzeni danych w celu ułatwienia interoperacyjności danych oraz mechanizmów i usług udostępniania danych.

Podsumowanie

Zaproponowana regulacja jest dobrym krokiem w kierunku „twardego" uregulowania pozycji zamawiającego w kontekście przejścia na usługi innego dostawy. Charakter regulacji w formie rozporządzenia powoduje, że niezależnie od woli dostawców będą oni musieli spełnić wymagania określone obecnie w projekcie Data Act. Pozwoli to na uniknięcie vendor lock-in i umożliwi przeniesienie danych, aplikacji i innych aktywów cyfrowych zamawiających do innego dostawcy usług przetwarzania danych.

Pamiętać należy przy tym, że analizowana treść Data Act jest jednak projektem rozporządzenia – będziemy obserwować, w jaki sposób zostaną ostatecznie ukształtowane przepisy dotyczące obowiązku zapewnienia przejścia na inne usługi przetwarzania danych.

Wytyczne Datatilsynet dotyczące przetwarzania danych osobowych w chmurze

Mateusz Kupiec

Chmura obliczeniowa to nazwa zbiorcza rozwiązań pozwalających korzystającym z nich podmiotom na dostęp za pośrednictwem sieci do wspólnej puli możliwych do konfiguracji zasobów przetwarzania (np. sieci, serwerów, aplikacji i usług[1]. W chmurze organizacje przechowują wiele informacji, w tym dane osobowe. Najwięksi dostawcy usług chmurowych przetwarzają powierzone im informacje w centrach danych znajdujących się poza Europejskim Obszarem Gospodarczym, najczęściej w USA. Po wyroku w sprawie Schrems II i opublikowaniu przez EROD zaleceń 01/2020 dotyczących środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych zagadnienie transferu danych do państw trzecich stało się szczególnie skomplikowane.

Duński organ nadzorczy z zakresu ochrony danych osobowych (Datatilsynet), dostrzegając problemy, z jakimi muszą się zmierzyć podmioty korzystające z różnego rodzaju usług chmurowych, postanowił opublikować wytyczne dotyczące przetwarzania danych w chmurze.

Wytyczne Datatilsynet

W wytycznych Datatilsynet wiele miejsca poświęcono na analizę zagadnienia transferu danych do państw trzecich (w szczególności do USA) w związku z korzystaniem przez administratorów z narzędzi oferowanych przez dostawców usług chmurowych. Jednakże zakres przedmiotowy wytycznych jest znacznie szerszy, ponieważ organ omawia w nich typologię usług chmurowych, a także zagadnienie audytu dostawcy usług chmurowych oraz jego podwykonawców.

Ogólne zalecenie Datatilsynet, jakie wynika z wytycznych organu, sprowadza się do konieczności zapoznania się przez administratora z modelem działania konkretnego dostawcy usług chmurowych oraz dokonania analizy sytuacji prawnej w państwie trzecim, w którym się on znajduje.

Transfery danych w związku z przechowywaniem danych w chmurze

Omawiając zagadnienie transferów danych do państw trzecich, Datatilsynet przedstawia m.in. następujące wnioski:

- Administratorzy przed rozpoczęciem transferu powinni się upewnić, że dostawca usług chmurowych spoza EOG, z którego rozwiązań korzystają, może ich poinformować o wcześniej otrzymanych wnioskach służb o dostęp do powierzonych mu danych.
- Administrator musi wykazać, że kategorie danych osobowych, które zamierza powierzyć dostawcy usług chmurowych spoza EOG, nie były wcześniej objęte żadnymi wnioskami otrzymanymi przez konkretnego dostawcę.
- W przypadku prawa amerykańskiego nie jest wykluczone, że istnieją dane osobowe, które są wyłączone z zakresu przedmiotowego „informacji obcego wywiadu" (*foreign intelligence information*), o których mowa w sekcji 702 ustawy o nadzorze wywiadu zagranicznego (Foreign Intelligence Surveillance Act, dalej: „FISA"). Jednakże to administrator musi wykazać, że przekazywane przez niego dane nie podlegają pod FISA. Same oświadczenia dostawcy są niewystarczające do prawidłowego spełnienia tego obowiązku.
- Należy dokonać wyczerpującej oceny przepisów obowiązujących w państwach trzecich, w których znajdują się dostawcy usług chmurowych i ich (potencjalni) podwykonawcy. Administratorzy, dokonując takiej oceny, przed podjęciem decyzji o transferze danych powinni zatem przyjąć „najgorszy możliwy scenariusz" jako podstawę swojej analizy, tj. uznać, że wszystkie kraje trzecie, do których mają być przekazywane dane osobowe, mają „problematyczne" ustawodawstwo. Dopiero wtedy powinni zbadać, jakie dodatkowe środki techniczne muszą zostać wdrożone, aby zapewnić poziom ochrony danych zasadniczo równoważny z gwarancjami unijnymi.

[1] P. Mell, T. Grance, *The NIST Definition of Cloud Computing, NIST Special Publication 800-145*, 2011, s. 2, https://csrc.nist.gov/publications/detail/sp/800-145/final (dostęp 10.03.2022).

- Środki umowne i organizacyjne na ogół nie przeszkodzą amerykańskim służbom w uzyskaniu dostępu do danych osobowych będących przedmiotem transferu. Konieczne będzie zatem wdrożenie dodatkowych środków technicznych.
- Szyfrowanie nie będzie skutecznym środkiem technicznym, który zagwarantuje bezpieczeństwo danych będących przedmiotem transferu, jeżeli dostawca chmurowy będzie w posiadaniu kluczy szyfrujących.
- Sekcja 702 FISA upoważnia amerykańskie służby do uzyskiwania informacji o „osobach niebędących obywatelami USA", co do których można w sposób uzasadniony oczekiwać, że znajdują się poza USA w celu zbierania „informacji obcego wywiadu". Odbywa się to poprzez wydawanie poleceń dostawcom usług łączności elektronicznej, aby dostarczyli lub zorganizowali dostarczenie służbom danych osobowych przetwarzanych przez dostawcę.

Audyt dostawcy usług chmurowych oraz jego podwykonawców

Zdaniem Datatilynet administrator korzystający z usług chmurowych powinien:

- dokładnie zbadać przed powierzeniem dostawcy danych osobowych do przetwarzania, czy taki podmiot zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą;
- móc wskazać, którzy z podwykonawców dostawcy usług chmurowych biorą udział w przetwarzaniu – jeżeli ADO nie jest w stanie tego zrobić, powinien założyć, że wszyscy podwykonawcy dostawcy odgrywają rolę w przetwarzaniu powierzonych danych w ramach usługi;
- dokonywać większej liczby audytów lub inspekcji u dostawcy usług chmurowych, któremu powierzył przetwarzanie danych, jeżeli dostawca często zmienia podwykonawców.

Wytyczne

Czy blockchain zrewolucjonizuje komunikację z klientem? Rośnie popularność trwałego nośnika opartego na technologii „łańcucha bloków"

Agnieszka Wachowska, Kamila Dymek

Blockchain kojarzony jest głównie jako technologia leżąca u podstaw znanej kryptowaluty. Jego potencjał jest jednak znacznie większy, na co wskazuje coraz więcej zastosowań w różnych sektorach gospodarki, m.in. w celu realizacji prawnego wymogu przekazywania informacji na trwałym nośniku.

Trwały nośnik w rozumieniu prawa

Przepisy prawa w zakresie praw konsumenckich, działalności bankowej i telekomunikacyjnej czy też usług płatniczych w pewnych sytuacjach wymagają, aby przedsiębiorca przekazał określone informacje lub utrwalił dane oświadczenie na „trwałym nośniku". Wprowadzenie takiego wymogu ma na celu przede wszystkim ochronę praw wynikających ze stosunków łączących podmiot z przedsiębiorcą, w szczególności ochronę prawa do dochodzenia roszczeń. Trwały nośnik ma zatem zabezpieczać interesy słabszej strony obrotu gospodarczego (np. konsumenta lub abonenta). Dotyczy to przykładowo informowania o zmianach w usługach płatniczych świadczonych przez banki lub o automatycznym przedłużeniu umowy o świadczenie usług telekomunikacyjnych.

„Trwały nośnik" (lub „trwały nośnik informacji") został zdefiniowany w różnych aktach prawnych, zarówno w prawie europejskim, jak i w polskich przepisach stanowiących implementację odpowiednich dyrektyw unijnych. Pojęciem tym posługuje się m.in. ustawa o prawach konsumenta[1], ustawa o usługach płatniczych[2], Prawo bankowe[3], Prawo telekomunikacyjne[4] oraz ustawa o kredycie konsumenckim[5]. Wszystkie definicje trwałego nośnika pozostają zbieżne co do podstawowych kryteriów, jakie powinien on wypełniać.

Żeby określony środek mógł zostać uznany za trwały nośnik, musi łącznie spełniać następujące przesłanki:

1. musi umożliwiać przechowywanie i odczytywanie informacji;
2. musi pozwalać na przechowywanie (i odczytywanie) informacji przez czas odpowiedni do celów, jakim służą;
3. musi pozwalać na dostęp do informacji i ich odtworzenie w tym czasie w niezmienionej postaci.

Definicja trwałego nośnika jest neutralna technologicznie, a zatem nie jest istotne, czym jest konkretny nośnik, lecz to, czy wypełnia powyższe funkcje wymagane przez prawo.

Trwały nośnik w praktyce

Wskazuje się, że trwałym nośnikiem są w szczególności tradycyjne formy utrwalania informacji, takie jak papier, ale też formy zapisu elektronicznego, np. pamięć USB, płyty CD-ROM lub karty pamięci. W dobie wszechobecnej cyfryzacji i rosnącej świadomości związanej ze zrównoważonym rozwojem coraz więcej organizacji zadaje sobie pytanie, jakie rozwiązania technologiczne dla trwałego nośnika można zastosować w obrocie cyfrowym, zapewniając przy tym zgodność z prawem.

Niektóre strony internetowe i portale przedsiębiorców przeznaczone dla klientów (np. systemy bankowości elektronicznej) nie spełniają funkcji wymaganych przez prawo

[1] Ustawa z dnia 30 maja 2014 r. o prawach konsumenta (t.j. Dz. U. z 2020 r., poz. 287, ze zm.).
[2] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz. U. z 2021 r., poz. 1907, ze zm.).
[3] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j. Dz. U. z 2021 r., poz. 2439, ze zm.).
[4] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2021 r., poz. 576).
[5] Ustawa z dnia 12 maja 2011 r. o kredycie konsumenckim (t.j. Dz. U. z 2019 r., poz. 1083, ze zm.).

w zakresie trwałego nośnika. Wynika to z tego, że rozwiązania te nie gwarantują braku zmian informacji przez stosowny czas, pozwalając na jednostronną modyfikację lub usuwanie ich przez przedsiębiorcę czy też blokowanie dostępu do informacji. Istnienie narzędzi gwarantujących, że po wprowadzeniu do systemów informacje nie będą mogły być zmieniane, stało się zatem warunkiem możliwości uznania tego typu systemów za trwały nośnik.

Poza wymienionymi już wyżej cechami dla spełnienia wymogu dostarczenia informacji na trwałym nośniku wymagana jest także aktywność po stronie przedsiębiorcy, np. w formie przesłania powiadomienia SMS w momencie pojawienia się nowej informacji[6].

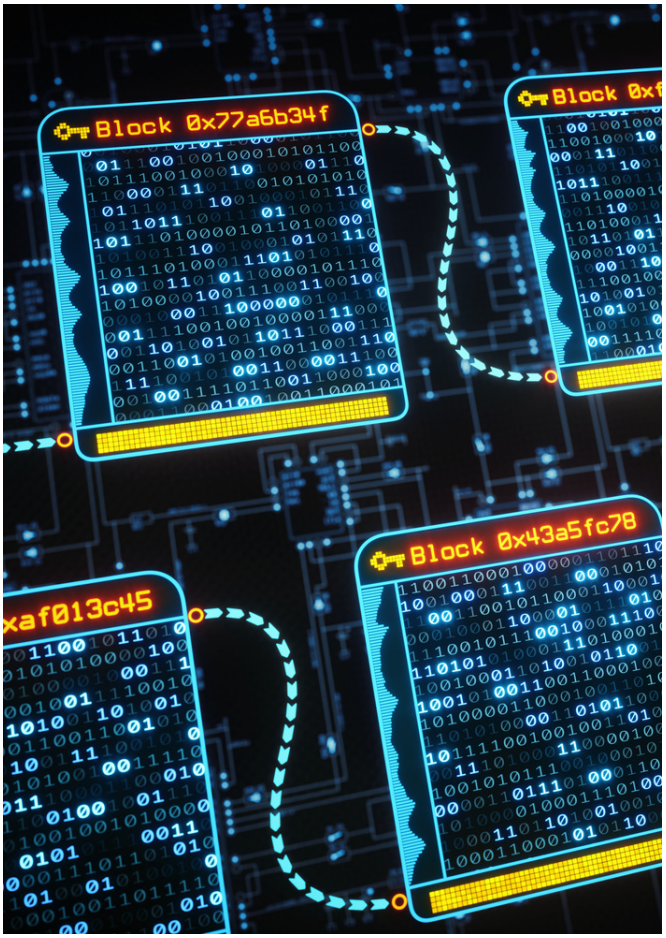
Technologia blockchain a trwały nośnik

Zgodnie z poglądami prezentowanymi w orzecznictwie TSUE oraz decyzjach Prezesa UOKiK[7] jako trwałe nośniki akceptowane są jedynie takie rozwiązania, które zapewniają integralność, niezmienność i autentyczność przesyłanych informacji oraz nieusuwalność przechowywanych dokumentów. Aby zapewnić te cechy pod względem technicznym, do przechowywania informacji wykorzystuje się m.in. rozwiązania oparte właśnie na technologii blockchain. Takie rozwiązanie zaproponowane w odniesieniu do trwałego nośnika zostało pozytywnie ocenione w praktyce Prezesa UOKiK[8].

Blockchain, jako architektura przechowywania informacji, ma parę szczególnych właściwości, które sprawiają, że może być wykorzystywany w powyższym celu. Dane zapisywane są bowiem w łańcuchu bloków, połączonych ze sobą w taki sposób, że nie można ingerować w historię zapisu, tj. w kolejność i treść zapisywanych informacji. Dodatkowo dane te są rozproszone pomiędzy tzw. węzłami, tworzącymi łącznie sieć blockchain. Taka decentralizacja sprawia, że nie ma możliwości jednostronnej kontroli nad strukturą danych ani jednostkowego punktu awarii.

Systemy wykorzystujące blockchain nadają się zatem do stosowania w obrocie cyfrowym przez przedsiębiorców, których dotyczą obowiązki przekazywania informacji na trwałym nośniku. Dla dostawców tych systemów otwiera to drogę do tworzenia takich rozwiązań lub dostosowywania istniejących i oferowania ich szerokiemu gronu podmiotów z wielu różnych branż, w tym podmiotom regulowanym.

Przy tworzeniu i wdrażaniu narzędzi mających spełniać funkcje trwałego nośnika należy jednak każdorazowo wziąć pod uwagę całokształt kryteriów, jakie powinny zostać wypełnione na gruncie przepisów prawa, uwzględniając także wykładnię TSUE i Prezesa UOKiK. Takie narzędzie musi w sobie łączyć wszystkie wymienione wyżej cechy, przy czym zastosowanie blockchaina gwarantuje integralność i niezmienność informacji. Ponadto trzeba pamiętać, że blockchain jest bardzo szerokim pojęciem i istnieją różne warianty wykorzystania tej technologii w zależności od np. zastosowanych protokołów konsensu, zasad dostępu do sieci blockchain lub sposobu zarządzania nią. Poszczególne warianty mogą być mniej lub bardziej odpowiednie dla danego przedsiębiorcy, w zależności od specyfiki branży, tego, czy jest on podmiotem regulowanym, bądź tego, jaki rodzaj informacji będzie przekazywał (np. czy będą to informacje wrażliwe).



Powyższe kwestie powinny zatem zostać uwzględnione jak najwcześniej – na etapie tworzenia, a także wyboru odpowiedniego rozwiązania przez przedsiębiorcę, tak aby było ono dostosowane do potrzeb konkretnego rynku. Wiele podmiotów już dziś wykorzystuje narzędzia oparte na blockchainie w celu realizacji obowiązków związanych z trwałym nośnikiem. Są to m.in. instytucje bankowe, towarzystwa ubezpieczeniowe czy podmioty z branży e-commerce.

[6] Por. decyzja Prezesa UOKiK z dnia 14 grudnia 2021 r. nr DOZIK – 13/2021, str. 62.
[7] Por. decyzja Prezesa UOKiK z dnia 30 maja 2018 r. nr RBG – 7/2018, str. 44, decyzja Prezesa UOKiK z dnia 5 września 2018 r. nr RBG – 12/2018, str. 15–16, wyrok TSUE z dnia 25 stycznia 2017 r. w sprawie o sygn. C-375/15, pkt 44.
[8] Por. decyzja Prezesa UOKiK z dnia 27 sierpnia 2018 r., nr RBG – 11/2018, str. 18 i n.

Stanowisko amerykańskiego Copyright Office dot. ochrony prawnoautorskiej utworów stworzonych przez systemy tzw. sztucznej inteligencji

MarcinRęgorowicz, Aleksandra Nycz

14 lutego 2022 r.[1] the Review Board of the United States Copyright Office (organ odwoławczy w ramach Copyright Office) stanął na stanowisku, że prawo autorskie chroni jedynie owoce pracy intelektualnej („the fruits of intellectual labor"), które opierają się na twórczych mocach ludzkiego umysłu („that are founded in the creative powers of the [human] mind"). Tym samym the Review Board odrzucił wniosek o rejestrację obrazu, którego autorstwo zostało przypisane systemowi tzw. sztucznej inteligencji o nazwie Creativity Machine[2]. Przedmiotem wniosku było dzieło (obraz) utworzone autonomicznie przez algorytm działający na maszynie. Copyright Office stanęło na stanowisku, że obraz stworzony przez taki system nie spełnia niezbędnej przesłanki do udzielenia ochrony na gruncie amerykańskiego prawa autorskiego, ponieważ brak jest ludzkiego autorstwa.

Sprawa przed Copyright Office

W 2018 r. Stephen Thaler złożył w Copyright Office (amerykańskim Urzędzie ds. Praw Autorskich) wniosek o zarejestrowanie utworu – obrazu o nazwie „A Recent Entrance to Paradise". We wniosku wskazano jako autora utworu system Creativity Machine, działający autonomicznie na komputerze, a jako wnioskodawcę – właściciela tejże maszyny. Istotne, że według wnioskodawcy dzieło zostało stworzone autonomicznie przez algorytm komputerowy działający na maszynie bez jego udziału. Rejestracja została zgłoszona w ramach instytucji prawa amerykańskiego „work-for-hire" dla właściciela Creativity Machine.

W 2019 r. Copyright Office odrzuciło wniosek, uznając, że ludzkie autorstwo jest elementem niezbędnym do zgłoszenia utworu. W ocenie Copyright Office dzieła wytworzone przez maszynę lub zwykły proces mechaniczny, który działa losowo lub automatycznie bez twórczego wkładu lub interwencji ze strony autora, nie powinny zostać objęte ochroną prawnoautorską na gruncie amerykańskiego prawa autorskiego („*the Office will not register works produced by a machine or mere mechanical process that operates randomly or automatically without any creative input or intervention from a human author*"[3]. Kluczowy element, na który zwróciło uwagę Copyright Office, to pytanie, czy dany utwór jest dziełem autorstwa człowieka, a komputer jest jedynie instrumentem pomocniczym, czy też tradycyjne elementy autorstwa w dziele (ekspresja literacka, artystyczna lub muzyczna lub elementy doboru, rozmieszczenia etc.) zostały wymyślone i wykonane nie przez człowieka, lecz przez maszynę.

Po powyższym orzeczeniu wnioskodawca złożył wniosek o ponowne rozpatrzenie, argumentując, że wymóg autorstwa człowieka byłby sprzeczny z konstytucją USA i nie byłby poparty ani ustawą, ani orzecznictwem. W odpowiedzi organ odwoławczy w ramach Copyright Office (The Review Board) podtrzymał wcześniejsze stanowisko, wskazując, że autorstwo człowieka jest warunkiem niezbędnym ochrony praw autorskich w Stanach Zjednoczonych i dlatego przedmiotowe dzieło nie może zostać zarejestrowane. The Review Board zaznaczył, że wyrażenie wskazane w przepisie Section 102, Chapter 1, Title 17 of the United States Code (wersja skodyfikowana Copyright Act of 1976) „original works of authorship"[4] wyznacza granice tego, co może być chronione prawem autorskim. Odnosząc się do orzecznictwa amerykańskiego ądu Najwyższego dot. kwestii autorstwa, wskazano, że chociaż żaden z wyroków nie rozstrzygał wprost kwestii kwalifikacji i ochrony utworów powstających bez udziału człowieka, wskazówki z dotychczasowego orzecznictwa pozwalają postawić tezę, że dzieła w całości stworzone przez maszyny nie kwalifikują się do ochrony prawnoautorskiej.

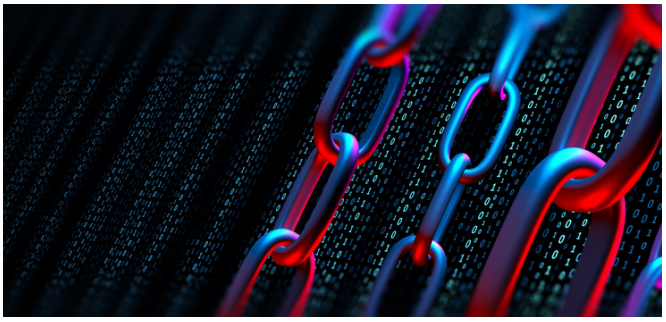
[1] The Copyright Office Review Board's Opinion from 14 February 2022 „A Recent Entrance to Paradise", https://www.copyright.gov/rulings-filings/review-board/docs/a-recent-entrance-to-paradise.pdf (dostęp: 25.04.2022).
[2] https://imagination-engines.com/cm.html (dostęp: 25.04.2022).
[3] The Copyright Office Review Board's Opinion from 14 February 2022 „A Recent Entrance to Paradise", https://www.copyright.gov/rulings-filings/review-board/docs/a-recent-entrance-to-paradise.pdf (dostęp: 25.04.2022).
[4] https://www.copyright.gov/title17/92chap1.html (dostęp: 25.04.2022).

The Review Board odniósł się również do podniesionego przez wnioskodawcę argumentu, że sztuczna inteligencja może być autorem w ramach instytucji „work made for hire"[5], która umożliwia wykonywanie pracy na zlecenie przez podmioty inne niż osoby fizyczne („non-human"), takie jak przedsiębiorstwa. The Review Board zdecydowanie odrzucił ten argument, podkreślając, że praca w ramach „work made for hire" musi być przygotowana przez pracownika lub przez jedną lub więcej stron, którzy wyraźnie zgadzają się w ramach umowy, że praca jest wykonywana na zlecenie. Według The Review Board w obu przypadkach tego rodzaju praca powstaje w wyniku wiążącej prawnie umowy. Ponieważ Creativity Machine jako system sztucznej inteligencji nie ma zdolności do zawarcia ważnej umowy, nie może spełnić tego wymogu, wobec czego instytucja „work made for hire" nie może mieć zastosowania[6].

Prawo europejskie a ochrona prawnoautorska AI

Kwestia przyznania ochrony prawnoautorskiej dziełom stworzonym przez systemy tzw. sztucznej inteligencji została poruszona w Rezolucji Parlamentu Europejskiego w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji[7]. Pisaliśmy o niej na naszym blogu w artykule "Kolejny krok w kierunku regulacji sztucznej inteligencji – rezolucje Parlamentu Europejskiego"[8]. Zgodnie z przywołaną rezolucją objęcie dzieł stworzonych samodzielnie przez systemy tzw. sztucznej inteligencji ochroną prawnoautorską może stać w sprzeczności z poszanowaniem zasady oryginalności oraz mieć negatywny wpływ na motywacje dla twórców będących ludźmi. Pojęcie twórczości intelektualnej odnosi się do osobowości autora, osoby fizycznej.

Analizując pojęcie autorstwa z perspektywy regulacji UE, należy podkreślić panujący konsensus wskazujący twórcę jako osobę fizyczną, grupę osób fizycznych lub osobę prawną, które stworzyły dzieło. Ponadto obliczanie czasu ochrony prawa autorskiego odnosi się do życia autorów jako osób fizycznych. Trybunał Sprawiedliwości Unii Europejskiej nie zajął się jeszcze konkretnie kwestią, kim lub czym jest autor. Niemniej jednak w świetle dotychczasowego orzecznictwa TSUE wydaje się, że jego autonomiczne rozumienie oryginalności zakłada, że twórcą utworu może być tylko człowiek. Trybunał w swoich orzeczeniach określał utwór jako twórczość intelektualną „odzwierciedlającą osobowość twórcy i przejawiającą się swobodnymi i twórczymi wyborami"[9], która stanowi „własną własność intelektualną autora"[10]. Do przyznania ochrony przewidzianej w prawie autorskim konieczne jest zaistnienie sytuacji, która pozwala autorowi na wyrażenie swojej twórczej inwencji w sposób oryginalny, i stworzenie rezultatu stanowiącego własną twórczość intelektualną autora.



Podsumowanie

Ze względu na ogromne znaczenie rozwoju sztucznej inteligencji dla rynku Unii Europejskiej istnieje dostrzegalna potrzeba zmian i stworzenia przepisów unijnych dostosowanych do dynamicznie rozwijającej się nowej rzeczywistości[11]. Obecnie większość prawodawstw Unii Europejskiej wciąż milczy na temat utworów stworzonych przez systemy tzw. sztucznej inteligencji. W nauce prawa i w orzecznictwie unijnych sądów przeważa stanowisko, iż w istniejącym stanie prawnym prawa autorskie są przyznawane jedynie „owocom ludzkiego umysłu".

W powyższym kontekście, wobec faktu trwających prac nad stworzeniem systemu regulacji związanych ze sztuczną inteligencją w ramach europejskiego porządku prawnego oraz rosnącej popularności wykorzystania systemów sztucznej inteligencji[12], stanowisko amerykańskiego Copyright Office stanowi bez wątpienia kolejny głos w dyskusji na poparcie stanowiska, że konieczność istnienia istotnego wkładu intelektualnego twórcy oraz wymóg oryginalności uzasadnia, aby chronić na gruncie prawa autorskiego tylko te utwory, których twórcą jest człowiek. Przyjęcie jednak takiego stanowiska stwarza pilną potrzebę uregulowania kwestii ochrony oraz praw do wytworów generowanych przez sztuczną inteligencję, a w szczególności określenie jakim prawem ochronnym powinny być chronione takie wytwory i kto powinien czerpać korzyści ekonomiczne z ich eksploatacji.

[5] 17 U.S.C. § 101, https://www.copyright.gov/title17/92chap1.html (dostęp: 25.04.2022).
[6] J. Turner, *Robot rules. Regulating artificial intelligence*, 2019.
[7] https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_PL.html (dostęp: 25.04.2022).
[8] „Kolejny krok w kierunku regulacji sztucznej inteligencji – rezolucje Parlamentu Europejskiego" www.traple.pl/2021/01/26/kolejny-krok-w-kierunku-regulacji-sztucznej-inteligencji-rezolucje-parlamentu-europejskiego (dostęp: 25.04.2022).
[9] https://curia.europa.eu/juris/liste.jsf?language=pl&num=C-145/10 (dostęp: 25.04.2022).
[10] https://curia.europa.eu/juris/liste.jsf?num=C-833/18&language=PL (dostęp: 25.04.2022).
[11] N. Selvadurai, R. Matulionyte, *Reconsidering creativity: copyright protection for works generated using artificial intelligence*, „Journal of Intellectual Property Law & Practice", 2020.
[12] https://www.nextrembrandt.com/, https://www.ai-darobot.com/, https://www.aiva.ai/ (dostęp: 25.04.2022).

WYDARZENIA

10.05.2022
szkolenie

PRAWO AUTORSKIE I OCHRONA KNOW-HOW W UMOWACH IT – UJĘCIE PRAKTYCZNE

Agnieszka Wachowska, MarcinRęgorowicz

Więcej informacji >>

17.05.2022
kongres

KONGRES CYBERBEZPIECZEŃSTWA

Granice odpowiedzialności dostawców IT za incydenty bezpieczeństwa i cyberzagrożenia – Agnieszka Wachowska

Więcej informacji >>

24.05.2022
szkolenie

UMOWY NA KORZYSTANIE Z OPROGRAMOWANIA W CHMURZE OBLICZENIOWEJ

Xawery Konarski, Agnieszka Wachowska

Więcej informacji >>

NR 2 - MAJ 2022

PUBLIKACJE

IT Professional nr 3 marzec 2022 r.

- Agnieszka Wachowska – Migracja do chmury publicznej w kontekście przepisów z zakresu cyberbezpieczeństwa

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

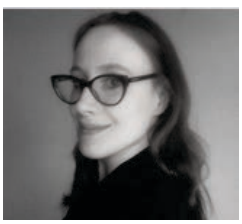
Karolina Grochecka-Goljan
Adwokat, Senior Associate
karolina.grochecka@traple.pl

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

Marcin Ręgorowicz
Radca prawny, Senior Associate
marcin.regorowicz@traple.pl

Małgorzata Kotwica
Associate
malgorzata.kotwica@traple.pl

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



Kamila Dymek
Junior Assosiate
kamila.dymek@traple.pl

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

Redaktorka newslettera:
adw. Karolina Grochecka-Goljan