***Przegląd Europejski*, ISSN: 1641-2478**
vol. 2022, no. 2

DOI: https://doi.org/10.31338/1641-2478pe.2.22.6

Dostarczanie usług cyfrowych i cyberbezpieczeństwo na gruncie Dyrektywy NIS i aktów ją wdrażających w Republice Malty oraz w Rzeczypospolitej Polskiej

Hieronim Dąbrowski, *Institute of Legal Sciences of the Polish Academy of Sciences (Warsaw, Poland)*
E-mail: hieronim.dabrowski@gmail.com
ORCID ID: 0000-0002-6265-9869

Streszczenie
Za pośrednictwem Internetu świadczone są, pełniące ważną rolę w społeczeństwie, usługi cyfrowe, od których mogą być zależni niektórzy przedsiębiorcy. Cyberbezpieczeństwo dostawców usług cyfrowych jest istotne, nie tylko jeżeli chodzi o takie aspekty jak techniczne czy organizacyjne, ale również aspekty prawne – z uwagi na to, że niektórych dostawców usług cyfrowych mogą jeszcze dotyczyć dodatkowe obowiązki prawne. W niniejszym artykule przedstawiono analizę porównawczą przepisów dotyczących dostarczania usług cyfrowych i cyberbezpieczeństwa na gruncie Dyrektywy NIS i aktów ją wdrażających w Republice Malty oraz w Rzeczypospolitej Polskiej. Dyrektywa NIS odnosi się do dostarczania jedynie trzech rodzajów usług cyfrowych – tj. internetowej platformy handlowej, wyszukiwarki internetowej i usługi przetwarzania w chmurze. Dostawcą usług cyfrowych jest osoba prawna, która podlega pod przepisy danego krajowego aktu prawnego wdrażającego Dyrektywę NIS po spełnieniu pewnych warunków. W analizowanych w niniejszym artykule aktach prawnych występują pewne różnice, w szczególności w zakresie obowiązków prawnych lub kar pieniężnych.
Słowa kluczowe: cyberbezpieczeństwo, usługi cyfrowe, dostawcy usług cyfrowych, bezpieczeństwo, dyrektywa NIS, prawo UE, ochrona danych

Provision of digital services and cybersecurity under the NIS Directive and its implementing acts in the Republic of Malta and the Republic of Poland

Abstract
The Internet provides digital services that play an important role in society and on which some entrepreneurs may depend. Cybersecurity is important for digital service providers, not only in terms of technical or organisational aspects, but also legal aspects, because some digital service providers may still be affected by additional legal obligations. This article presents a comparative analysis of the provisions concerning digital services and cybersecurity under the NIS Directive and its implementing acts in the Republic of Malta and the Republic of Poland. The NIS Directive addresses the provisions of only three types of digital services – i.e. the online marketplace, internet search engine and cloud computing services. A digital service provider is a legal entity that is subject to the provisions of a given national legal act implementing the NIS Directive under certain conditions. There are some differences in the acts analysed in this article, particularly in terms of legal obligations or financial penalties.
Keywords: cybersecurity, digital services, digital service providers, security, NIS directive, EU Law, data protection

Internet odgrywa istotną rolę w ułatwianiu transgranicznego przepływu towarów, usług czy nawet osób – za jego pośrednictwem świadczone są pełniące ważną rolę w społeczeństwie usługi cyfrowe. Takie usługi mogą stać się celem cyberprzestępców, co niekiedy może zagrozić ich funkcjonowaniu (Dyrektywa 2016/1148: motyw 3). Przy tym, skala, częstotliwość czy wpływ incydentów rośnie. Z raportu rocznego 2021 z działalności CERT Polska[1] wynika, że zespół ten zarejestrował łącznie 29 483 unikalne incydenty cyberbezpieczeństwa, co stanowi wzrost liczby obsłużonych incydentów w 2021 roku o 182% w porównaniu do 2020 roku (CERT Polska 2022: s. 12). Niektórzy przedsiębiorcy są zależni od dostawców usług cyfrowych, a zakłócenie funkcjonowania takich usług mogłoby uniemożliwić świadczenie przez nich usług, co w efekcie może mieć wpływ na kluczową działalność gospodarczą i społeczną w Unii Europejskiej (Dyrektywa 2016/1148: motyw 48).

Z uwagi m.in. na powyższe kwestie, uchwalona została Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii z dnia 6 lipca 2016 r. (Dyrektywa 2016/1148, tzw. Dyrektywa NIS). Następnie wymagała ona wdrożenia do krajowych porządków prawnych państw członkowskich Unii Europejskiej. W niniejszym artykule rozpatrywane będą dwa przykłady wdrożenia: w Republice Malty – Legal Notice 216 of 2018 *The Measures for High Common Level of Security of Network and Information Systems Order* (Legal Notice 2018/216; dalej: Maltański

[1] CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty związane z cyberbezpieczeństwem. Zespół działa w strukturach NASK – Państwowego Instytutu Badawczego, prowadzi działalność naukową, a także krajowy rejestr domen .pl i dostarcza zaawansowane usługi teleinformatyczne. Dzięki prężnej działalności od 1996 roku w środowisku zespołów reagujących, CERT Polska stał się rozpoznawalnym i doświadczonym podmiotem w dziedzinie bezpieczeństwa komputerowego. Od początku istnienia zespołu rdzeniem działalności jest obsługa incydentów bezpieczeństwa i współpraca z podobnymi jednostkami na całym świecie, zarówno w działalności operacyjnej, jak i badawczo-wdrożeniowej. (CERT Polska WWW)

Akt Prawny) oraz w Rzeczypospolitej Polskiej – *Ustawą o krajowym systemie cyberbezpieczeństwa* z dnia 5 lipca 2018 r. (dalej: Ustawa 2018/1560).

W ramach niniejszego artykułu, zostaną omówione i porównane prawne aspekty świadczenia usług cyfrowych i cyberbezpieczeństwa na gruncie Dyrektywy NIS oraz aktów ją wdrażających do porządków prawnych w Republice Malty i w Rzeczypospolitej Polskiej, w szczególności celem wskazania – z wykorzystaniem odpowiednio metody formalno-dogmatycznej oraz metody prawno-porównawczej – ich stosowności oraz ewentualnych podobieństw lub różnic. Analizie zostaną poddane nie tylko podstawowe definicje, ale także wpływ incydentów dotyczących bezpieczeństwa sieci i systemów informatycznych na świadczenie usług cyfrowych, sposób zapewniania bezpieczeństwa oraz sankcjonowanie jego niedostatecznego poziomu zarówno w regulacjach unijnych, jak i krajowych. Stanowi to bowiem interesujący przykład znaczenia wspólnych i zsynchronizowanych działań na rzecz bezpieczeństwa. Co więcej, aktualne pozostają pytania m.in. o dotkliwość wspomnianych sankcji, jak też podobieństwa i różnice zauważalne w regulacjach krajowych państw członkowskich Unii Europejskiej.

Wybór do analizy Maltańskiego Aktu Prawnego oraz Ustawy 2018/1560 jest zasadny z uwagi na możliwe różne podejścia państw do implementacji Dyrektywy NIS, a także na zainteresowanie niektórych polskich przedsiębiorców prowadzeniem działalności w Republice Malty. Przy tym, z uwagi na zasadę tzw. prounijnej wykładni przepisów prawa krajowego, celowe jest odwoływanie się do Dyrektywy NIS przy wykładni krajowych przepisów takich jak zawarte w Ustawie 2018/1560 (Wajda 2020).

I. Usługa cyfrowa i jej rodzaje

1. Wstęp

Usługa cyfrowa w Dyrektywie NIS została zdefiniowana jako usługa w rozumieniu art. 1 ust. 1 lit. b) Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 i określona w załączniku III do Dyrektywy NIS. Zgodnie ze wspomnianym art. 1 ust. 1 lit. b Dyrektywy 2015/1535 „usługa" oznacza każdą usługę społeczeństwa informacyjnego tj. usługę:

- normalnie świadczoną za wynagrodzeniem, przy tym, takim wynagrodzeniem mogą też być np. dane osobowe, a nie tylko pieniądze;
- na odległość, tj. usługa świadczona jest bez równoczesnej obecności stron;
- świadczona drogą elektroniczną, tj. „usługa jest wysyłana i odbierana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania danych, i która jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych" (Dyrektywa 2015/1535: art. 1, ust. 1b);
- na indywidualne żądanie odbiorcy usług, tj. „usługa świadczona jest poprzez przesyłanie danych na indywidualne żądanie" (Dyrektywa 2015/1535: art. 1, ust. 1b).

Maltański odpowiednik usługi społeczeństwa informacyjnego został analogicznie zdefiniowany, jak we wspomnianej Dyrektywie 2015/1535 – dokonano tego w ramach

Legal Notice 2003/373. W Rzeczypospolitej Polskiej ww. usługa społeczeństwa informacyjnego została wdrożona w ramach *Ustawy o świadczeniu usług drogą elektroniczną* z dnia 18 lipca 2002 r. (obecnie: Ustawa 2020/344). Przez świadczenie usługi drogą elektroniczną rozumie się „wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne" (Ustawa 2020/344: art. 2, ust. 4).

Powyższe definicje mają istotne znaczenie, ponieważ nie tylko na gruncie Dyrektywy NIS, ale również w ramach Ustawy 2018/1560 – usługa cyfrowa została zdefiniowana właśnie poprzez odwołanie do usługi świadczonej drogą elektroniczną (usługi społeczeństwa informacyjnego) w rozumieniu przepisów *Ustawy o świadczeniu usług drogą elektroniczną* z dnia 18 lipca 2002 r. (zob.: Ustawa 2020/344) i ograniczona do usług wymienionych w załączniku nr 2 do ustawy. Podobnie zresztą jest w Maltańskim Akcie Prawnym, gdzie w art. 2 wskazano, że usługa cyfrowa oznacza usługę w rozumieniu art. 2[2] (Legal Notice 2003/373) i która została wymieniona w załączniku III do Maltańskiego Aktu Prawnego.

Wspomniany załącznik III Dyrektywy NIS, jak i przytoczone załączniki z Ustawy 2018/1560 oraz z Maltańskiego Aktu Prawnego ograniczają zakres usług cyfrowych jedynie do internetowej platformy handlowej, wyszukiwarki internetowej i usługi przetwarzania w chmurze. To ważne, bo gdyby nie takie ograniczenie – usługą cyfrową w rozumieniu aktów prawnych wdrażających Dyrektywę NIS mogłaby być każda usługa społeczeństwa informacyjnego (usługa świadczona drogą elektroniczną) jak np. *newsletter* czy sklep internetowy z produktami dostarczanymi wyłącznie przez jednego przedsiębiorcę.

2. Internetowa platforma handlowa

Na gruncie art. 4 ust. 17 Dyrektywy NIS, internetowa platforma handlowa została zdefiniowana jako usługa cyfrowa, która umożliwia konsumentom lub przedsiębiorcom[3] zawieranie *online* umów dotyczących sprzedaży lub usług z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który używa usług komputerowych świadczonych przez internetową platformę handlową.

---

[2] Z niego wynika: „usługa" oznacza każdą usługę społeczeństwa informacyjnego, to znaczy każdą usługę zwykle świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. Dla celów niniejszej definicji: (a) „na odległość" oznacza, że usługa jest świadczona bez równoczesnej obecności stron; (b) „drogą elektroniczną" oznacza, że usługa jest wysyłana pierwotnie i otrzymywana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania danych, oraz w całości przesyłana, przekazywana i otrzymywana za pomocą kabla, odbiornika radiowego, środków optycznych lub innych środków elektromagnetycznych; (c) „na indywidualne żądanie odbiorcy usług" oznacza, że usługa jest świadczona poprzez przekazywanie danych na indywidualne żądanie. Orientacyjny wykaz usług nieobjętych niniejszą definicją jest zawarty w załączniku III do tego aktu prawnego.

[3] Zdefiniowanym odpowiednio w art. 4 ust. 1 lit. a) i lit. b) Dyrektywy Parlamentu Europejskiego i Rady 2013/11/UE.

Jak wskazano w motywie (15) Dyrektywy NIS, internetowa platforma handlowa ma być ostatecznym miejscem zawierania takich umów, a świadczone w ramach niej usługi mogą obejmować przetwarzanie transakcji, agregowanie danych lub profilowanie użytkowników. Jednak, co wynika z tego motywu, z zakresu jej definicji powinny zostać wyłączone usługi, które:

- spełniają wyłącznie funkcję pośredniczącą wobec usług stron trzecich, gdy jest możliwe ostateczne zawarcie umowy;
- „porównują cenę poszczególnych produktów lub usług różnych przedsiębiorców handlowych, a następnie przekierowują użytkownika do preferowanego przedsiębiorcy handlowego w celu zakupu produktu" (Dyrektywa 2016/1148: motyw 15).

Przykładem internetowej platformy handlowej mogą być sklepy z aplikacjami, które działają jako sklepy internetowe umożliwiające cyfrową dystrybucję aplikacji lub oprogramowania stron trzecich (Dyrektywa 2016/1148: motyw 15).

W Maltańskim Akcie Prawnym (art. 2) internetowa platforma handlowa została zdefiniowana w sposób identyczny jak w Dyrektywie NIS. Natomiast w załączniku nr 2 do Ustawy 2018/1560, internetowa platforma handlowa została zdefiniowana jako: „Usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową." (Ustawa 2018/1560: zał. 2).

Po porównaniu omówionych wyżej definicji internetowej platformy handlowej należy stwierdzić, że nie ma pomiędzy nimi istotnych różnic – w efekcie dostawca usługi cyfrowej, takiej jak internetowa platforma handlowa, na gruncie wymienionych wyżej aktów prawnych, pod pewnym warunkami może podlegać pod przepisy prawne dotyczące świadczenia takiej usługi cyfrowej.

3. Wyszukiwarka internetowa

W art. 4 ust. 18 Dyrektywy NIS, wyszukiwarka internetowa została zdefiniowana jako usługa cyfrowa, „która umożliwia użytkownikom wyszukiwanie – co do zasady – wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania na jakikolwiek temat przez podanie słowa kluczowego, wyrażenia lub innej wartości wejściowej; w wyniku tego wyszukiwarka internetowa przedstawia odnośniki, pod którymi można znaleźć informacje związane z zadanym zapytaniem" (Dyrektywa 2016/1148: art. 4, ust. 18). W motywie (16) Dyrektywy NIS wskazano, że wyszukiwarka internetowa ma umożliwić użytkownikowi wykonywanie przeszukań na wszystkich stronach internetowych poprzez wpisane zapytania na jakikolwiek temat – ewentualnie takie wyszukiwanie może zostać zawężone wyłącznie do stron internetowych w konkretnym języku. Jednocześnie definicja wyszukiwarki internetowej nie powinna obejmować:

- funkcji wyszukiwania, które ograniczają się jedynie do treści na konkretnej stronie internetowej – nawet jeśli taka funkcja wyszukiwania jest zapewniana przez zewnętrznego dostawcę;

- „usług online, które porównują cenę poszczególnych produktów lub usług różnych przedsiębiorców handlowych", by następnie przekierować użytkownika do wybranego przedsiębiorcy, celem sfinalizowania transakcji (Dyrektywa 2016/1148: motyw 16).

Załącznik 2 do Ustawy 2018/1560 zawiera następującą definicję wyszukiwarki internetowej: „Usługa, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiającą w wyniku odnośniki, odnoszące się do informacji związanych z zapytaniem."

W Maltańskim Akcie Prawnym wyszukiwarkę internetową zdefiniowano jako usługę cyfrową, która umożliwia użytkownikowi przeszukiwanie w zasadzie wszystkich stron internetowych lub stron internetowych w odrębnych językach na podstawie zapytania na dowolny temat w formie słowa kluczowego, frazy lub innych danych wejściowych i która zwraca odnośniki, w których można znaleźć informacje związane z żądaną treścią (Legal Notice 2018/216: art. 2).

W zakresie wszystkich tych definicji wyszukiwarki internetowej w ramach Dyrektywy NIS, Ustawy 2018/1560 czy Maltańskiego Aktu Prawnego nie można dostrzec znaczących różnic – dlatego taki dostawca usługi cyfrowej w postaci wyszukiwarki internetowej, w każdym z tych krajów, pod pewnym warunkami, może podlegać pod odpowiedni akt prawny.

4. Usługa przetwarzania w chmurze

Usługa przetwarzania w chmurze została zdefiniowana w Dyrektywie NIS jako usługa cyfrowa umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania. Definicja obejmuje szeroki zakres działań i realizowany według różnych modeli (Dyrektywa 2016/1148: motyw 17).

Motyw (17) Dyrektywy NIS zawiera wyjaśnienia dla pojęć wykorzystanych w ramach definicji usługi przetwarzania w chmurze i zgodnie z nim: (a) „zasoby obliczeniowe" obejmują takie zasoby jak pamięć, sieci, serwery lub inną infrastrukturę, a także aplikacje i usługi; (b) „skalowalne" oznacza zasoby komputerowe, które są elastycznie przydzielane, niezależnie od położenia geograficznego zasobów, przez dostawcę usługi, co stanowi reakcję na fluktuacje zapotrzebowania; (c) „elastyczny zbiór" odnosi się do opisu zasobów obliczeniowych, które są przydzielane i uwalniane w zależności od zapotrzebowania, aby zależnie od obciążenia – szybko zwiększać lub zmniejszać dostępne zasoby; natomiast (d) „wspólne wykorzystywanie" oznacza opis zasobów obliczeniowych, udostępnianych wielu odbiorcom, dzielącym wspólny dostęp do usługi. Przy tym, takie przetwarzanie odbywa się oddzielnie dla każdego z tych odbiorców, mimo, że taka usługa jest świadczona z tego urządzenia (Dyrektywa 2016/1148: motyw 17).

W Maltańskim Akcie Prawnym usługa przetwarzania w chmurze została zdefiniowana jako usługa cyfrowa, umożliwiająca dostęp do skalowalnej i elastycznej puli udostępnianych zasobów obliczeniowych. Natomiast w Ustawie 2018/1560 usługa przetwarzania w chmurze wyjaśniona została jako: „Usługa umożliwiającą dostęp do skalowalnego

i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników." (Ustawa 2018/1560: zał. 2).

Po porównaniu odpowiednich definicji usługi przetwarzania w chmurze w Dyrektywie NIS, Maltańskim Akcie Prawnym i Ustawie 2018/1560 – nie można stwierdzić istotnych różnić. W konsekwencji, na gruncie wszystkich tych aktów prawnych, ci sami dostawcy usług przetwarzania w chmurze mogą zostać zakwalifikowani jako dostawcy usług cyfrowych w rozumieniu wszystkich wspomnianych wyżej aktów prawnych i pod pewnymi warunkami podlegać pod te przepisy prawne. Przy tym, jak wskazują niektórzy autorzy – usługa przetwarzania w chmurze odnosi się do świadczenia takich usług przez danego dostawcę na rzecz jego klientów i z zakresu tej definicji powinny zostać wyłączone przypadki chmury wykorzystywanej wewnątrz organizacji (Besiekierska 2019: art. 2).

II. Dostawca usług cyfrowych

1. Kiedy podmiot zostaje uznany za dostawcę usług cyfrowych?

Jak określono w art. 4 ust. 6 Dyrektywy NIS – dostawcą usług cyfrowych jest osoba prawna, która świadczy usługi cyfrowe. Podobnie jest w Maltańskim Akcie Prawnym, gdzie w art. 2, dostawca usług cyfrowych został zdefiniowany jako każda osoba prawna, która świadczy usługę cyfrową. W Ustawie 2018/1560 dostawca usług cyfrowych nie został zdefiniowany w ramach objaśnień pojęć z art. 2, ale odpowiednie warunki uznania za dostawcę usługi cyfrowej określone zostały w art. 17 ww. ustawy, z którego wynika: „Dostawcą usług cyfrowych jest osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej i mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową" (Ustawa 2018/1560: art. 17, ust. 1).

Zgodnie z Dyrektywą NIS, Rozdział V dotyczący dostawców usług cyfrowych nie powinien mieć zastosowania do mikroprzedsiębiorstw i małych przedsiębiorstw zdefiniowanych w zaleceniu Komisji 2003/361/WE (Dyrektywa 2016/1148: art. 16 ust. 11). Podobnie jest w Maltańskim Akcie Prawnym, gdzie wskazano, że jego Część V nie ma zastosowania do mikroprzedsiębiorstw i małych przedsiębiorstw określonych w zaleceniu Komisji 2003/361/WE. W art. 17 ust. 1 Ustawy 2018/1560 wskazano, że dostawcą usług cyfrowych jest podmiot, który został omówiony już powyżej, ale z wyjątkiem mikroprzedsiębiorców i małych przedsiębiorców, o których mowa w art. 7 ust. 1 pkt 1 i 2 ustawy *Prawo przedsiębiorców* z dnia 6 marca 2018 r.

Przy tym należy mieć na względzie, że inaczej niż w przypadku operatorów usługi kluczowej, gdzie zgodnie z art. 5 Ustawy 2018/1560 musi zostać wydana decyzja w przedmiocie uznania za operatora usługi kluczowej (por. Legal Notice 2018/216: art. 9), w tym przypadku nie ma konieczności wydawania takiej decyzji, a dostawcą usługi cyfrowej jest się w przypadku Ustawy 2018/1560, jak również Maltańskiego Aktu Prawnego – z mocy samego prawa. Co ważne, dany podmiot, by został uznany za dostawcę usług cyfrowych, musi spełnić omówione wyżej kryteria łącznie, w tym świadczyć odpowied-

nią usługę cyfrową. Niespełnienie jakiegokolwiek ze wskazanych kryteriów uniemożliwia nałożenie na taki podmiot obowiązków prawnych (Lewoszewski 2019).

Sam zakres usług cyfrowych w rozumieniu omawianych aktów prawnych jest wąski, a zakres podmiotów, które można uznać za dostawców usług cyfrowych został zawężony (Szpor et al. 2019: s. 153). W każdym z powyższych przypadków ograniczono katalog dostawców usług cyfrowych jedynie do osób prawnych o określonym statusie, co prowadzi do wyłączenia z zakresu stosowania omawianych aktów prawnych obok mikro i małych przedsiębiorców, także jednoosobowej działalności gospodarczej, mimo że takie usługi cyfrowe mogą być również świadczone przez tego typu podmioty (Krasuski 2018: s. 99).

Szerszy katalog podmiotów objętych zakresem stosowania tych aktów prawnych w Rzeczpospolitej Polskiej czy w Republice Malty mógłby przyczynić się do zapewnienia cyberbezpieczeństwa usług cyfrowych w większym zakresie. Z drugiej strony, poszerzenie takiego katalogu można by było uznać za nadmiarowe. W szczególności, jak wskazują niektórzy autorzy, powodem wyłączenia małych i mikro przedsiębiorców z zakresu dostawców usług cyfrowych w rozumieniu Ustawy 2018/1560 – może być fakt, że wymagane przez tę ustawę środki bezpieczeństwa lub nałożone obowiązki mogą stanowić dla nich nieproporcjonalne obciążenie (Kruk 2019).

2. Jaki akt prawny będzie mieć zastosowanie?

Wątpliwości może budzić to, który akt wdrażający Dyrektywę NIS do krajowego porządku prawnego może mieć zastosowanie do danego dostawcy usługi cyfrowej – co w szczególności ma znaczenie w przypadku, gdy dostawca usługi cyfrowej dostarcza swoje usługi na terytorium kilku państw członkowskich Unii Europejskiej.

W art. 18 ust. 1 Dyrektywy NIS uregulowano, że „dostawca usług cyfrowych podlega jurysdykcji państwa członkowskiego, w którym posiada główną jednostkę organizacyjną", tzn. gdy „dostawca usług cyfrowych posiada główną jednostkę organizacyjną w państwie członkowskim" oraz ma w nim siedzibę zarządu (Dyrektywa 2016/1148: art. 18, ust. 1). Jeśli dostawca usługi cyfrowej nie posiada jednostki organizacyjnej w Unii Europejskiej, to zobowiązany jest wyznaczyć swojego przedstawiciela w Unii Europejskiej (w jednym z tych państw członkowskich, w których oferowane są usługi, taki przedstawiciel musi posiadać jednostkę organizacyjną). Przy tym, właściwa jest jurysdykcja państwa członkowskiego, w którym taki przedstawiciel posiada jednostkę organizacyjną (Dyrektywa 2016/1148: art. 18 ust. 2). Jak wynika z art. 18 ust. 3 Dyrektywy NIS – wyznaczenie przedstawiciela przez dostawcę usług cyfrowych nie ma znaczenia dla działań prawnych, które mogłyby zostać podjęte przeciwko dostawcy usług cyfrowych.

W art. 16 ust. 1 Maltańskiego Aktu Prawnego uregulowano, że w przypadku, gdy dostawca usługi cyfrowej ma główne miejsce prowadzenia działalności w Republice Malty, to uznaje się go za podlegającego jurysdykcji Republiki Malty. Główne miejsce prowadzenia działalności w Republice Malty jest wtedy, gdy dostawca usługi cyfrowej ma tam swoją siedzibę (Legal Notice 2018/216: art. 16 ust. 1). Oprócz tego, gdy dostawca usług cyfrowych, nie ma siedziby w Unii Europejskiej, ale świadczy usługi cyfrowe w Unii

Europejskiej, to uznaje się, w przypadku, gdy jego przedstawiciel ma siedzibę w Republice Malty, że podlega jurysdykcji Republiki Malty (Legal Notice 2018/216: art. 16, ust. 2).

Zgodnie z art. 17 ust.1 Ustawy 2018/1560, dostawcą usługi cyfrowej jest osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej i mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela, który ma jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej i który świadczy usługę cyfrową.

Ponadto, co wynika z art. 17 ust. 4 Ustawy 2018/1560, gdy dostawca usługi cyfrowej nie posiada jednostki organizacyjnej w jednym z państw członkowskich Unii Europejskiej, ale świadczy w Rzeczypospolitej Polskiej usługi cyfrowe, to wtedy ma obowiązek wyznaczyć przedstawiciela posiadającego jednostkę organizacyjną w RP, chyba że przedstawiciel został przez niego wyznaczony już w innym państwie Unii Europejskiej (Ustawa 2018/1560: art. 17 ust. 4).

3. Jakie są obowiązki prawne?

Obowiązki prawne odnoszące się do dostawców usług cyfrowych określone zostały w Rozdziale V Dyrektywy NIS. Art. 16 ust. 1 Dyrektywy NIS wskazuje, że, państwa członkowskie są zobowiązane zapewnić, by „dostawcy usług cyfrowych określali i podejmowali odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami, na jakie narażone są sieci i systemy informatyczne" wykorzystywane przez nich w zakresie dostarczanych usług cyfrowych. Przy tym, ważne jest, że „środki te muszą zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka i brać pod uwagę najnowszy stan wiedzy oraz uwzględniać: (a) bezpieczeństwo systemów i obiektów; (b) postępowanie w przypadku incydentu; (c) zarządzanie ciągłością działania; (d) monitorowanie, audyt i testowanie; (e) zgodność z normami międzynarodowymi" (Dyrektywa 2016/1148: art. 16, ust. 1).

Art. 16 ust. 1 Dyrektywy NIS ma swoje odzwierciedlenie w:

- art. 13 ust. 1 Maltańskiego Aktu Prawnego, z którego wynika, że dostawcy usług cyfrowych określają oraz podejmują odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykiem stwarzanym dla bezpieczeństwa sieci i systemów informacyjnych, z których korzystają w kontekście dostarczania usług cyfrowych w Republice Malty. Przy uwzględnieniu aktualnego stanu wiedzy, środki te mają zapewnić poziom bezpieczeństwa sieci i systemów informacyjnych odpowiedni do istniejącego ryzyka i uwzględniający następujące elementy: (a) bezpieczeństwo systemów i urządzeń; (b) obsługę incydentów; (c) zarządzanie ciągłością działania; (d) monitorowanie, audyt i testowanie; oraz (e) zgodność z normami międzynarodowymi.
- art. 17 ust. 2 Ustawy 2018/1560, gdzie dostawca usługi cyfrowej zobowiązany jest podjąć właściwe i proporcjonalne środki techniczne i organizacyjne określone w Rozporządzeniu wykonawczym 2018/151 „w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej". Takie środki mają za zadanie zapewnić cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz uwzględnić: (a) bezpieczeństwo systemów

informacyjnych i obiektów; (b) postępowanie w przypadku obsługi incydentu; (c) zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej; (d) monitorowanie, audyt i testowanie; oraz (e) najnowszy stan wiedzy, obejmujący zgodność z normami międzynarodowymi, wspomnianymi w Rozporządzeniu wykonawczym 2018/151.

Co można stwierdzić po powyższym, analizowane przepisy wdrażające Dyrektywę NIS nie różnią się w znacznym stopniu. W przypadku Ustawy 2018/1560 jedynie dodane zostało, że dostawcy usług cyfrowych mają uwzględniać najnowszy stan wiedzy, obejmujący zgodność z normami międzynarodowymi, wspomnianymi w Rozporządzeniu wykonawczym 2018/151. Istotą i treścią wspomnianych środków, które zostały wskazane w Rozporządzeniu wykonawczym 2018/151, jest zarządzanie ryzykiem w sposób skuteczny w ramach świadczenia danej usługi cyfrowej (Banasiński, Rojszczak 2020: s. 25).

Wspomniany najnowszy stan wiedzy czy konieczność działania zgodnie z normami międzynarodowymi wiąże się ze stosowaniem norm przyjętych przez Międzynarodową Organizację Normalizacyjną (ang. *International Organization for Standardization,* ISO), Międzynarodową Komisję Elektrotechniczną (ang. *International Electrotechnical Commission,* IEC) lub Międzynarodowy Związek Telekomunikacyjny (ang. *International Telecommunication Union,* ITU). Oprócz tego, zastosowanie mogą mieć również europejskie lub międzynarodowe normy i specyfikacje, w tym normy krajowe (Kitler et al. 2019: art. 17).

Wskazuje się, że głównym międzynarodowym standardem przyjętym w Republice Malty przez szereg organizacji i organów rządowych jest ISO 27001, dodatkowo niektóre organizacje decydują się na wdrożenie tego standardu bez uzyskania odpowiedniej certyfikacji. Przyjęcie takiego standardu następuje na zasadzie dobrowolności i wiąże się z domniemaniem, że podjęto odpowiednie środki w tym zakresie (Finkel, Zammit 2019: s. 67). W przypadku Ustawy 2018/1560, jeśli chodzi o normatywne wzorce właściwej organizacji cyberbezpieczeństwa w przedsiębiorstwie, niektórzy autorzy nakazują odwołanie się w tym zakresie do norm ISO, np. ISO 27001 dotyczącej systemów bezpieczeństwa informacji czy ISO 27005 dotyczącej oceny ryzyka w bezpieczeństwie informacji, a także do wytycznych OWASP (ang. *Open Web Application Security Project*) czy NIST (ang. *National Institute of Standards and Technology*) (Ćwiakowski, Gawroński 2020).

***

Zgodnie z art. 16 ust. 2 Dyrektywy NIS, państwa członkowskie zostały zobowiązane do zapewnienia, by dostawcy usług cyfrowych podejmowali środki zapobiegające i minimalizujące wpływ incydentów dotyczących bezpieczeństwa ich sieci i systemów informatycznych w zakresie usług cyfrowych, które są dostarczane w Unii Europejskiej, z myślą o zapewnieniu ciągłości takich usług. Omawiany art. 16 ust. 2 Dyrektywy NIS został wdrożony w:

- art. 13 ust. 2 Maltańskiego Aktu Prawnego, zgodnie z którym dostawcy usług cyfrowych podejmują środki mające na celu zapobieganie i minimalizowanie wpływu incydentów na bezpieczeństwo sieci i systemów informacyjnych w zakresie dostarczanych usług cyfrowych w Republice Malty, w celu zapewnienia ciągłości tych usług;

- art. 17 ust. 3 Ustawy 2018/1560, zgodnie z którym dostawca usługi cyfrowej zobowiązany jest podjąć środki zapobiegające i minimalizujące wpływ incydentów na usługę cyfrową w celu zapewnienia ciągłości świadczenia tej usługi.

Art. 17 ust. 3 Ustawy 2018/1560, jak i art. 13 ust. 2 Maltańskiego Aktu Prawnego – nie różnią się w znaczący sposób w stosunku do art. 16 ust. 2 Dyrektywy NIS.

***

Jeżeli chodzi o przepisy prawne odnoszące się do incydentów, to w art. 16 ust. 3 Dyrektywy NIS wskazano, że państwa członkowskie zapewniają, by dostawcy usług cyfrowych niezwłocznie zgłaszali właściwemu organowi ds. cyberbezpieczeństwa lub CSIRT[4] wszelkie incydenty mające istotny wpływ na świadczenie usług cyfrowych. Takie zgłoszenie musi zawierać informacje umożliwiające właściwemu organowi lub CSIRT określenie istotności wpływu transgranicznego. Przy tym, takie zgłoszenie nie może wiązać się dla strony zgłaszającej ze zwiększoną odpowiedzialnością.

Ponadto w art. 16 ust. 4 Dyrektywy NIS wskazano parametry, które w szczególności powinny mieć zastosowanie przy szacowaniu czy wpływ danego incydentu jest istotny: (a) liczba użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług; (b) czas trwania incydentu; (c) zasięg geograficzny, którego dotyczy incydent; (d) zasięg zakłócenia funkcjonowania usługi; (e) zasięg wpływu na działalność gospodarczą i społeczną (Dyrektywa 2016/1148: art. 16, ust. 4). Jak wynika z omawianego artykułu Dyrektywy NIS, „obowiązek zgłoszenia incydentu ma zastosowanie wyłącznie wówczas, gdy dostawca usług cyfrowych ma dostęp do informacji niezbędnych do oceny wpływu incydentu" względem omówionych powyżej w lit. od (a) do (e) parametrów.

Art. 16 ust. 5 Dyrektywy NIS statuuje natomiast: „W przypadku gdy do celów świadczenia usługi, która ma istotne znaczenie dla utrzymania krytycznej działalności społecznej i gospodarczej, operator usług kluczowych jest zależny od dostawcy usług cyfrowych będącego stroną trzecią, operatorowi temu zgłasza się wszelki istotny wpływ na ciągłość usług kluczowych związany z incydentem, który dotyczy dostawcy usług cyfrowych." (Dyrektywa 2016/1148: art. 16, ust. 5). Zgodnie z tym przepisem wątpliwe jest, kto powinien być zobowiązany do dokonania tego typu zgłoszenia na rzecz operatora usługi kluczowej – czy dostawca danej usługi cyfrowej czy inny podmiot.

W zakresie wdrożeń powyższych artykułów Dyrektywy NIS do krajowych porządków prawnych, to zgodnie z art. 13 ust. 3 Maltańskiego Aktu Prawnego – dostawcy usług cyfrowych są zobowiązani powiadomić niezwłocznie Jednostkę CIIP[5] o wszelkich incydentach mających istotny wpływ na świadczenie usług cyfrowych, które są dostarczane na Malcie. Takie powiadomienia muszą zawierać informacje umożliwiające Jednostce CIIP określenie znaczenia wszelkich skutków lokalnych i transgranicznych. Powiadomienie nie powoduje zwiększenia odpowiedzialności strony powiadamiającej.

---

[4] Sieć CSIRT utworzono zgodnie z art. 12 Dyrektywy NIS w celu rozwoju pewności i zaufania między państwami członkowskimi UE oraz propagowania szybkiej i skutecznej współpracy.

[5] Jednostka Ochrony Krytycznej Infrastruktury Informatycznej, ang. *CIIP Unit*.

Jak wskazano w art. 13 ust. 4 Maltańskiego Aktu Prawnego – w celu ustalenia, czy wpływ incydentu jest istotny, uwzględnia się m.in. następujące parametry: (a) liczbę użytkowników dotkniętych incydentem, w szczególności użytkowników polegających na usłudze w celu świadczenia własnych usług; (b) czas trwania incydentu; (c) rozpiętość geograficzną w odniesieniu do obszaru dotkniętego incydentem; (d) zakres zakłócenia funkcjonowania usługi; (e) zakres wpływu na działalność gospodarczą i społeczną; (f) znaczenie podmiotu dla utrzymania wystarczającego poziomu usług, z uwzględnieniem dostępności alternatywnych sposobów świadczenia tych usług; (g) zależność krytycznej infrastruktury informatycznej od usług świadczonych przez taki podmiot.

Ponadto, jak określono przy końcu w art. 13 ust. 4 Maltańskiego Aktu Prawnego: obowiązek zgłoszenia incydentu ma zastosowanie wyłącznie w przypadku, gdy dostawca usług cyfrowych ma dostęp do informacji potrzebnych do oceny wpływu incydentu na parametry, o których mowa w akapicie poprzedzającym. Przy tym, jeśli świadczenie usługi kluczowej przez operatora usług polega na dostawcy usług cyfrowych, który jest wobec niego osobą trzecią – w celu świadczenia usługi, która ma zasadnicze znaczenie dla utrzymania krytycznej działalności społecznej i gospodarczej, operator usługi kluczowej powiadamia dostawcę usług cyfrowych o jakimkolwiek znaczącym wpływie na ciągłość świadczenia usługi kluczowej spowodowanym zdarzeniem mającym wpływ na dostawcę usług cyfrowych – niezwłocznie i na piśmie (Legal Notice 2018/216: art. 13 ust. 5).

Jeśli chodzi o ustawodawstwo Rzeczypospolitej Polskiej, to w art. 18 ust. 1 Ustawy 2018/1560 uregulowano, że taki dostawca zobowiązany jest: (a) przeprowadzić „czynności umożliwiające wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów"; (b) zapewnić „w niezbędnym zakresie dostęp do informacji dla właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV o incydentach zakwalifikowanych jako krytyczne przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV"; (c) dokonać klasyfikacji incydentu jako incydentu istotnego; (d) zgłosić taki „incydent istotny niezwłocznie, nie później jednak niż w ciągu 24 godzin od momentu jego wykrycia, do odpowiedniego CSIRT jak CSIRT MON, CSIRT NASK lub CSIRT GOV"; (e) zapewnić „obsługę incydentu istotnego i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe"; (f) usunąć podatności, o których mowa w art. 32 ust. 2 Ustawy 2018/1560; oraz (g) przekazać „operatorowi usługi kluczowej, który świadczy usługę kluczową za pośrednictwem tego dostawcy usługi cyfrowej, informacje dotyczące incydentu mającego wpływ na ciągłość świadczenia usługi kluczowej tego operatora" (Ustawa 2018/1560: art. 18, ust. 1). Wspomniany punkt (g) odnosi się do konieczności przekazania operatorowi usługi kluczowej informacji o incydencie każdego rodzaju, a nie tylko o incydencie istotnym w rozumieniu ustawy (Szpor i in. 2019: s. 163).

W art. 18 ust. 2 Ustawy 2018/1560 określono, że „dostawca usługi cyfrowej w celu sklasyfikowania incydentu jako istotnego" uwzględnia: (a) liczbę użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług; (b) czas trwania incydentu; (c) zasięg geograficzny ob-

szaru, którego dotyczy incydent; (d) zakres zakłócenia funkcjonowania usługi; (e) zakres wpływu incydentu na działalność gospodarczą i społeczną.

Z art. 18 ust. 3 Ustawy 2018/1560 wynika, że: gdy dostawca usługi cyfrowej klasyfikuje incydent jako istotny, to wtedy zobowiązany jest ocenić istotność wpływu incydentu na świadczenie usługi cyfrowej na podstawie parametrów, o których mowa w akapicie poprzedzającym, oraz na podstawie progów określonych w Rozporządzeniu wykonawczym 2018/151. Obowiązek zgłoszenia incydentu jest wyłączony, gdy taki dostawca „nie posiada informacji pozwalających na ocenę istotności wpływu incydentu na świadczenie usługi cyfrowej" – co uregulowano w art. 18 ust. 4 Ustawy 2018/1560. Wymogi w zakresie zawartości zgłoszenia incydentu istotnego określone są w art. 19.

W ramach omówionych powyżej przepisów, jedna z najistotniejszych odmienności odnosi się do terminu zgłoszenia istotnego incydentu. W Maltańskim Akcie Prawnym jest to – bez zbędnej zwłoki, natomiast w Ustawie 2018/1560 – niezwłocznie, nie później jednak niż 24 godziny od momentu jego wykrycia. Rozwiązanie zastosowane w ustawie należy ocenić pozytywnie, ma dla jego odbiorców dyscyplinujący charakter – przy tym, jest to termin krótszy niż np. ten określony na zgłoszenie naruszenia ochrony danych osobowych w Ogólnym Rozporządzeniu o Ochronie Danych (tam – bez zbędnej zwłoki, w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia).

Kolejna różnica jaką można odnotować odnosi się do kwestii wymiany informacji dotyczących incydentów pomiędzy operatorem usług kluczowych a dostawcą usług cyfrowych. W Ustawie 2018/1560 dostawca usługi cyfrowej jest zobowiązany przekazać operatorowi usługi kluczowej informacje dotyczące incydentu mającego wpływ na ciągłość świadczenia usługi kluczowej tego operatora, dla odróżnienia – w Maltańskim Akcie Prawnym, operator usługi kluczowej powiadamia niezwłocznie na piśmie o jakimkolwiek znaczącym wpływie na ciągłość świadczenia usługi kluczowej spowodowanym zdarzeniem mającym wpływ na dostawcę usług cyfrowych – Dyrektywa NIS nie precyzuje tego na kim spoczywa przedmiotowy obowiązek.

Oprócz tego, w zakresie parametrów określenia incydentu jako istotnego - Maltański Akt Prawny w stosunku do Dyrektywy NIS i Ustawy 2018/1560 ma uregulowane dodatkowo znaczenie podmiotu dla utrzymania wystarczającego poziomu usług i zależność infrastruktury krytycznej, krytycznej infrastruktury informatycznej lub obu tych elementów od usług świadczonych przez taki podmiot.

4. Sankcje

W odniesieniu do sankcji, które mogą zostać nałożone na dostawców usług cyfrowych, w art. 21 Dyrektywy NIS wskazano jedynie, że: „Państwa członkowskie ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszeń krajowych przepisów przyjętych na podstawie niniejszej dyrektywy i podejmują wszystkie niezbędne środki w celu zapewnienia ich wykonania. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające." (Dyrektywa 2016/1148: art. 21). W związku z tym, by uzyskać informacje o wysokości potencjalnych sankcji za naruszenie przepisów, należy zajrzeć do poszczególnych krajowych aktów prawnych wdrażających Dyrektywę NIS.

W Maltańskim Akcie Prawnym za naruszenie przepisów prawnych przez dostawców usług cyfrowych przewidziano kary pieniężne. W przypadku naruszenia, na podstawie art. 20 ust. 1 Maltańskiego Aktu Prawnego, przedsiębiorca w postaci dostawcy usługi cyfrowej, który nie wdroży odpowiednich i proporcjonalnych środków bezpieczeństwa określonych w art. 13 Maltańskiego Aktu Prawnego, lub nie współpracuje z Jednostką CIIP przy wykonywaniu swoich obowiązków na mocy Maltańskiego Aktu Prawnego w zakresie monitorowania – podlega karze administracyjnej w wysokości co najmniej 1000 EUR ale nie większej niż 100 000 EUR za każde takie naruszenie. Oprócz tego, kara w wysokości 100 EUR może zostać nałożona za każdy dzień, w którym takie naruszenie trwa, w przypadku, gdy taka kara zostanie przez Jednostkę CIIP ustalona i nałożona.

Ponadto, jak wskazano w art. 20 ust. 2 Maltańskiego Aktu Prawnego, przedsiębiorca w postaci dostawcy usług cyfrowych, w przypadku gdy: nie powiadomił o wystąpieniu incydentu (a miał taki obowiązek); nie zastosował się do instrukcji Jednostki CIIP, które są zgodne z prawem; lub narusza przepisy Maltańskiego Aktu Prawnego, inne niż te omówione w ramach akapitu poprzedzającego – podlega karze administracyjnej w wysokości nie niższej niż 500 EUR, ale nie przekraczającej 50 000 EUR za każde naruszenie, a oprócz tego – w wysokości 50 EUR za każdy dzień, w którym naruszenie trwa.

W każdym z wymienionych wyżej przypadków w ramach Maltańskiego Aktu Prawnego – taka nałożona dzienna kara pieniężna może być datowana wstecz na dzień popełnienia lub rozpoczęcia naruszenia. Sama procedura nakładania powyższych kar przez Jednostkę CIIP, zawarta jest w art. 19 Maltańskiego Aktu Prawnego. Kwota takiej kary pieniężnej ustalana jest z uwzględnieniem w szczególności charakteru oraz zakresu naruszenia, czasu jego trwania, a także wpływu na krytyczną działalność społeczną i gospodarczą.

Natomiast w Ustawie 2018/1560 przewidziano dla dostawców usług cyfrowych karę pieniężną, gdy taki dostawca nie wykonuje obowiązku w zakresie niezwłocznego zgłaszania incydentu istotnego, nie później jednak niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV, który określono w art. 18 ust. 1 pkt 4 Ustawy 2018/1560 – za każdy stwierdzony przypadek niezgłoszenia incydentu istotnego w wysokości do 20 000 PLN.

Dodatkowo, dostawca usługi cyfrowej może dostać karę pieniężną w wysokości do 20 000 PLN, gdy nie wykonuje obowiązku, z art. 18 ust. 1 pkt 5 Ustawy 2018/1560, tj. jak nie zapewni obsługi incydentu istotnego i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując im niezbędne dane, co obejmuje także dane osobowe; a także gdy nie usuwa podatności, wskazanych w art. 32 ust. 2 Ustawy 2018/1560, tj. gdy taki dostawca nie zrealizuje wezwania organu właściwego do spraw cyberbezpieczeństwa do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogłyby doprowadzić do wystąpienia incydentu.

W wyjątkowych przypadkach, jak określono w art. 73 ust. 5 Ustawy 2018/1560, organ właściwy do spraw cyberbezpieczeństwa może nałożyć na dostawcę usług cyfrowych karę w wysokości nawet do 1 000 000 PLN. Ma to miejsce, jeżeli taki organ w wyniku kontroli stwierdzi, że dostawca usługi cyfrowej uporczywie narusza przepisy Ustawy

2018/1560, powodując: (a) bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi; (b) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych.

Omawiane kary z art. 73 Ustawy 2018/1560, mogą być także nałożone przez organ właściwy do spraw cyberbezpieczeństwa, „w przypadku, gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę", jeżeli wspomniany organ „uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia" (Ustawa 2018/1560: art. 76).

Co można zauważyć po powyższym, kary pieniężne w przypadku Ustawy 2018/1560 nakładane są na dostawców usług cyfrowych jedynie w związku z sytuacjami, w których doszło do incydentu, w przypadku niewypełnienia obowiązków informacyjnych lub nieusunięcia podatności zidentyfikowanej podczas obsługi incydentu – mimo, że art. 21 Dyrektywy NIS uprawnia krajowego ustawodawcę do wprowadzenia sankcji za naruszenia obowiązków prawnych związanych z zapewnieniem odpowiedniego poziomu cyberbezpieczeństwa (Proć 2020). Z takiego uprawnienia skorzystano w ramach Maltańskiego Aktu Prawnego – i w efekcie, możliwe jest nałożenie kary pieniężnej na przedsiębiorcę w postaci dostawcy usługi cyfrowej, który nie wdroży odpowiednich i proporcjonalnych środków bezpieczeństwa. Jest to kierunek trafny i podobny do zastosowanego w Ogólnym Rozporządzeniu o Ochronie Danych.

Sama Dyrektywa NIS nie precyzuje wysokości kar pieniężnych, określone one zostały w aktach ją wdrażających. W Maltańskim Akcie Prawnym przewidziano kary pieniężne w walucie EURO, a w Ustawie 2018/1560 zostały one określone w PLN. Kary pieniężne uregulowane w Maltańskim Akcie Prawnym, które mogą być nałożone na dostawców usług cyfrowych, wydają się być w praktyce jednak wyższe, niż te wynikające z ustawy. Przy tym, w porównaniu do innych aktów prawnych (jak np. Ogólne Rozporządzenie o Ochronie Danych) określone w Ustawie 2018/1560 czy w Maltańskim Akcie Prawnym kary nie są wysokie i mogą nie zostać uznane za takie, które są skuteczne, proporcjonalne i odstraszające.

Wprowadzenie omawianych wyżej kar pieniężnych, jak wskazują niektórzy autorzy, może mieć uzasadnienie w tym, że „cyberprzestrzeń jako wspólne dobro musi być chroniona w jednakowym stopniu przez wszystkich jej użytkowników. Brak synergii w działaniach na poziomie krajowym czy europejskim będzie wpływał na skuteczność oddziaływania na niepożądane zdarzenia w cyberprzestrzeni" (Banasiński 2018: s. 170). W tym zakresie może nasuwać się pytanie, czy ich obecna forma przynosi postulowane efekty.

Podsumowanie

W zakresie Dyrektywy NIS i aktów ją wdrażających w postaci Ustawy 2018/1560 i Maltańskiego Aktu Prawnego nie można dostrzec znaczących różnic. Dyrektywa NIS odnosi się do dostarczania jedynie trzech rodzajów usług cyfrowych: internetowej platformy handlowej, wyszukiwarki internetowej i usługi przetwarzania w chmurze. Analogicznie jest w Ustawie 2018/1560 i w Maltańskim Akcie Prawnym.

Dostawcą usług cyfrowych jest osoba prawna, która dostarcza usługi cyfrowe. Jednak taki dostawca usługi cyfrowej podlega pod przepisy danego krajowego aktu prawnego wdrażającego Dyrektywę NIS po spełnieniu pewnych warunków, o których mowa w odpowiednim akcie prawne: przedmiotowe przepisy prawne nie mają zastosowania do mikro przedsiębiorców i małych przedsiębiorców oraz nie odnoszą się one także np. do jednoosobowej działalności gospodarczej. Po łącznym spełnieniu wszystkich wymaganych prawnie kryteriów do uznania za dostawcę usług cyfrowych – takim dostawcą zostaje się z mocy prawa. Wydaje się, że dla zapewnienia wyższego poziomu cyberbezpieczeństwa, krąg takich podmiotów czy usług cyfrowych mógłby zostać rozszerzony.

W przypadku uznania za dostawcę usług cyfrowych, taki dostawca powinien mieć na względzie obowiązki prawne, m.in. w zakresie właściwych i proporcjonalnych środków technicznych i organizacyjnych, bezpieczeństwa systemów informacyjnych i obiektów, zarządzania ciągłością działania, monitorowania, postępowania w przypadku obsługi incydentu, audytu i testowania oraz uwzględniania najnowszego stanu wiedzy. Do ciekawszych odmienności w ramach badanych aktów prawnych można zaliczyć termin na zgłaszanie incydentu istotnego czy powiadamiania o znaczącym wpływie na ciągłość świadczenia usługi kluczowej spowodowanym zdarzeniem mającym wpływ na dostawcę usług cyfrowych.

Za nieprzestrzeganie przez dostawców usług cyfrowych omówionych obowiązków prawnych przewidziano kary pieniężne, które mogą różnić się w zależności od przepisów wdrażających Dyrektywę NIS do krajowego porządku prawnego. W aktach prawnych Republiki Malty i Rzeczypospolitej Polskiej podstawowe różnice odnoszą się do wskazanej w przepisach waluty, możliwych do naruszenia obowiązków prawnych i wysokości potencjalnej kary. Wydaje się, że wysokość kar pieniężnych w obydwu przypadkach mogłaby zostać zwiększona, gdyż mogą one nie zostać uznane za takie, które są skuteczne, proporcjonalne i odstraszające – w szczególności porównując je do kar z innych aktów prawnych (np. takich jak Ogólne Rozporządzenie o Ochronie Danych). W przypadku Ustawy 2018/1560, pod rozwagę można wziąć także rozszerzenie możliwości nałożenia kar pieniężnych na kwestie niepodjęcia właściwych i proporcjonalnych środków technicznych i organizacyjnych przez dostawcę usług cyfrowych.

Hieronim Dąbrowski – absolwent prawa na Uniwersytecie Warszawskim, Center for American Law Studies, a także Zarządzania Bezpieczeństwem Informacji w Szkole Głównej Handlowej. Uczestnik Prawniczych Seminariów Doktorskich w Instytucie Nauk Prawnych Polskiej Akademii Nauk. Doświadczenie zawodowe zdobywał w Polskiej Izbie Informatyki i Telekomunikacji, w polskich i w międzynarodowych kancelariach prawnych oraz w spółkach. Laureat II miejsca w IX edycji konkursu dla studentów zorganizowanego przez Urząd Ochrony Danych Osobowych. Współzałożyciel i były wiceprezes Koła Naukowego Komparatystyki Prawniczej na Uniwersytecie Warszawskim.

Hieronim Dąbrowski – Graduate of Law at the University of Warsaw, Center for American Law Studies, and Information Security Management at the Warsaw School of Economics. A parti-

cipant of Legal Doctoral Seminars at the Institute of Legal Sciences of the Polish Academy of Sciences. He gained professional experience in the Polish Chamber of Information Technology and Telecommunications, in Polish and international law firms and companies. Second place winner in the IX edition of the competition for students organised by the Personal Data Protection Office. Co-founder and former vice-president of the Comparative Law Society at the University of Warsaw.

Bibliografia:

BANASIŃSKI Cezary (red.) (2018), *Cyberbezpieczeństwo Zarys wykładu*, Warszawa.

BANASIŃSKI Cezary, ROJSZCZAK Marcin (red.) (2020), *Cyberbezpieczeństwo*, Warszawa.

BESIEKIERSKA Agnieszka (red.) (2019), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa.

CERT Polska (2021), *Raport roczny z działalności CERT Polska: Krajobraz bezpieczeństwa polskiego internetu w 2021 roku*, https://cert.pl/uploads/docs/Raport_CP_2021.pdf (07.02.2022).

CERT Polska (WWW), *O nas*, https://cert.pl/o-nas/ (07.02.2022).

ĆWIAKOWSKI Michał, GAWROŃSKI Maciej (2020), *Cloud computing – czy i jak korzystanie z usług chmurowych może pomóc w realizacji obowiązków regulacyjnych w obszarze cyberbezpieczeństwa,* Warszawa.

DYREKTYWA (2015/1535) Parlamentu Europejskiego i Rady (UE) z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego, Dz. U. UE, L 241, 17.09.2015.

DYREKTYWA (2016/1148) Parlamentu Europejskiego i Rady (UE) z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. U. UE L 194, 19.07.2016.

FINKEL Olga, ZAMMI Robert (2019), *Malta*, in: Benjamin A. Powell, Jason C. Chipman (eds), *Cybersecurity*, London.

KITLER Władysław, TACZKOWSKA-OLSZEWSKA Joanna, RADONIEWICZ Filip (red.) (2019), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa.

KRASUSKI Andrzej (2018), *Chmura obliczeniowa Prawne aspekty zastosowania*, Warszawa.

KRUK Marta (2019), *Obowiązki dostawców usług cyfrowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa jako element poprawy bezpieczeństwa w świecie cyfrowym oraz przeciwdziałaniu cyberprzestępstwom*, „Prawo Mediów Elektronicznych", nr 1.

LEGAL NOTICE (2003/373) *Notification Procedure Regulations*, Subsidiary Legislation 419.06, https://legislation.mt/eli/sl/419.6/eng (07.02.2022)

LEGAL NOTICE (2018/216) *Measures for High Common Level of Security of Network and Information Systems Order*, Subsidiary Legislation 460.35, https://legislation.mt/eli/sl/460.35/eng (07.02.2022).

LEWOSZEWSKI Marcin (2019), *Wybrane obowiązki dostawców usług cyfrowych na gruncie ustawy o cyberbezpieczeństwie*, „Informacja w Administracji Publicznej", nr 1(9).

PROĆ Tomasz (2020), *Odpowiedzialność dostawcy usług cyfrowych w Krajowym Systemie Cyberbezpieczeństwa*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny", nr 2 (9). DOI: 10.7172/2299-5749.IKAR.2.9

ROZPORZĄDZENIE Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE (Ogólne Rozporządzenie o Ochronie Danych), Dz. U. UE L 119, 04.05.2016.

ROZPORZĄDZENIE wykonawcze Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia czy incydent ma istotny wpływ, Dz. U. UE L 26, 31.01.2018.

SZPOR Grażyna, GRYSZCZYŃSKA Agnieszka, CZAPLICKI Kamil (2019), *Ustawa o Krajowym Systemie Cyberbezpieczeństwa. Komentarz*, Warszawa.

USTAWA (2018/1560) z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. z 2018 r., poz. 1560 z późn. zmianami.

USTAWA (2020/344) z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. z 2020 r., poz. 344.

WAJDA Paweł (2020), *Cyberbezpieczeństwo – sektorowe aspekty regulacyjne*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny", nr 2 (9). DOI: 10.7172/2299-5749.IKAR.2.9

Received: 21.02.2022. Accepted: 30.06.2022.