TOM LXXII • NR 3 (849) • DOI 10.33226/0137-5490.2019.3.13

Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych

Cybersecurity and personal data protection in the light of European and domestic regulations

mgr Władysław Hydzik

E-mail: w.hydzik@wpia.uw.edu.pl

Streszczenie

Artykuł porusza problematykę regulacji prawnej obszaru cyberbezpieczeństwa i ochrony danych osobowych. Omówiono kluczowe założenia Dyrektywy NIS i Ustawy o krajowym systemie cyberbezpieczeństwa, zwracając uwagę na zdublowanie się wymogów regulacyjnych, np. w zakresie obowiązku zgłaszania incydentów. Na ustawodawcę krajowego nałożono szereg obowiązków w zakresie nadzorowania stosowania przez podmioty nowych przepisów. Liczne głosy krytyczne wskazują na potencjalne trudności w wdrożeniu szeregu wymogów, a ich skuteczne wdrożenie niekoniecznie przełoży się na poprawę cyberbezpieczeństwa krajowego, w tym bezpieczeństwa danych osobowych.

Słowa kluczowe: ochrona danych osobowych, cyberbezpieczeństwo, NIS, RODO, ryzyko.

Summary

The article addresses the issues of legal regulation of the cybersecurity area and the protection of personal data. The key assumptions of the NIS Directive and the Act on the National Cyber Security System were discussed, paying attention to the doubling of regulatory requirements, e.g. regarding the obligation to report incidents. A number of obligations were imposed on the National Legislator to supervise the application of new provisions by entities. Numerous critical voices indicate potential difficulties in implementing a number of requirements, and their effective implementation will not necessarily translate into improvement of national cyber security, including the security of personal data.

Key words: personal data protection, cybersecurity, NIS, GDPR, risk.

1. Wprowadzenie

Wzrasta liczba europejskich i krajowych regulacji prawnych, które tworzą liczne wymogi dotyczące cyberbezpieczeństwa i ochrony danych dla instytucji publicznych i podmiotów gospodarczych i uzupełniają regulacje sektorowe, np. Ustawę o usługach płatniczych[1]. Poszczególne branże także ustanawiają zbiory dobrych praktyk w zakresie cyberbezpieczeństwa. Złożoność środowiska regulacyjnego jest dodatkowo komplikowana przez niedostosowanie przepisów do zmieniających się zagrożeń, niejednoznaczność lub niewystarczające wsparcie regulacji przez międzynarodowe standardy, społeczności lub niespójne z innymi przepisami prawnymi, tworząc w ten sposób ogromne zapotrzebowanie na specjalistyczną interpretację prawną ich wdrożenia.

W odpowiedzi na rosnące zagrożenia cyberprzestępczością, Unia Europejska zintensyfikowała działania związane z ochroną Europejczyków korzystających z usług „online". Na wzór swobód traktatowych w 2015 roku powstała Strategia Jednolitego Rynku Cyfrowego (ang. *Digital Single Market Strategy*), której podstawowe cele obejmują[2]:

– lepszy dostęp europejskich konsumentów i przedsiębiorców do „dóbr cyfrowych";

– utworzenie odpowiednich warunków i równych szans dla rozwoju sieci cyfrowych oraz innowacyjnych usług;

– maksymalizacja potencjału wzrostu ekonomii cyfrowej.

Szczególnie drugi i trzeci cel był podstawą sformułowania głównych wyzwań dla wdrożenia Strategii Jednolitego Rynku Cyfrowego. Podstawą cyberbezpieczeństwa Strategii jest wdrożenie pakietu aktów prawnych, z których dwa najistotniejsze to Dyrektywa NIS[3] oraz Rozporządzenie RODO[4].

2. Założenia systemu cyberbezpieczeństwa oraz ochrony prywatności wynikające z Dyrektywy NIS i Rozporządzenia ODO

Przepisy krajowe wdrażające Dyrektywę NIS to przede wszystkim Ustawa o krajowym systemie cyberbezpieczeństwa[5] wraz rozporządzeniami wykonawczymi.

Obowiązki wynikające z Rozporządzenia ODO już są lub powinny być wdrażane przez krajowe instytucje i przedsiębiorstwa, a zmiany w Ustawie o ochronie danych osobowych[6] dotyczą głównie zasad funkcjonowania nowego organu nadzorczego — Urząd Ochrony Danych Osobowych. O Rozporządzeniu ODO mówi się intensywnie w ostatnim czasie, głównie w kontekście kar administracyjnych sięgających nawet 20 milionów EURO lub 4% światowego obrotu przedsiębiorstwa za naruszenie postanowień Rozporządzenia ODO. Brak faktycznej transpozycji wytycznych Grupy roboczej Art. 29[7] dotyczących wdrożenia Rozporządzenia ODO, powoduje, że odpowiedź na pytanie jak wdrożyć przedmiotowe przepisy, wciąż rodzi niepewność. Na stronie[8] GIODO opublikowano wprawdzie wytyczne w języku angielskim zaznaczając, że ich wersje angielskie są wersjami wiążącymi, jednocześnie zachęcając do zgłaszania uwag do treści opublikowanych dokumentów. Ze względu na brak umocowania dla wytycznych w polskim prawodawstwie oraz znowelizowanej ustawy o ochronie danych osobowych rodzi się wątpliwość o faktycznie związanie przedsiębiorców i instytucji takim komunikatem po powołaniu nowego organu regulacyjnego i podejścia nowego organu do orzeczeń i stanowisk zajmowanych przez GIODO w okresie sprzed wejścia w życie Rozporządzenia ODO.

Do najogólniej pojętego celu Dyrektywy NIS należy (...) *zwiększenie bezpieczeństwa Internetu oraz prywatnych sieci i systemów informatycznych stanowiących podstawę funkcjonowania naszych społeczeństw i gospodarek* (...)[9]. Powyżej postawiony cel nie obliguje organów, instytucji i przedsiębiorców państw członkowskich do zapewnienia całkowitej odporności systemów, urządzeń tworzących sieć Internet, czy sieci prywatne, a jedynie zwiększenie poziomu ich bezpieczeństwa.

Transpozycja Dyrektywy NIS do prawa krajowego opiera się na kilku filarach:

1) Identyfikacja operatorów usług kluczowych i dostawców usług kluczowych. Proces ustalenia podmiotów jest dwuetapowy, etap pierwszy wynika z załącznika do Ustawy, który opiera się na załączniku do Dyrektywy NIS, a który zawiera rodzaje podmiotów w podziale na sektory. Drugi etap to wpis konkretnego podmiotu na listę operatorów kluczowych poradzoną przez Ministra Cyfryzacji. Dodatkowo Dyrektywą NIS i Ustawą będą objęte podmioty świadczące usługi wymienione w załączniku 3 do Dyrektywy NIS.

2) Obowiązek przeprowadzenia analizy ryzyka przed podmioty objęte Dyrektywą NIS. Szerzej podejście oparte na ryzyku opisano w dalszej części artykułu.

3) Zaprojektowanie, wdrożenie i utrzymywanie przez podmioty objęte Dyrektywą NIS systemów teleinformatycznych, zapewniających bezpieczeństwo świadczonych przez nich kluczowych usług oraz ciągłości świadczenia tych usług.

4) Zapewnienie bezpieczeństwa dla usług przetwarzanych w chmurze.

5) Obowiązek przekazywania przez podmioty objęte Dyrektywą NIS informacji o podatnościach na incydenty, incydentach i zagrożeniach cyberbezpieczeństwa oraz o poziomie ryzyka wystąpienia incydentów gromadzone przez podmioty krajowego systemu cyberbezpieczeństwa.

6) Skatalogowanie i certyfikowanie podmiotów świadczących usługi z zakresu cyberbezpieczeństwa zdefiniowanego w projekcie Ustawy.

3. Pojęcie cyberbezpieczeństwa i ryzyka

Warto porównać ewolucję pojęcia cyberbezpieczeństwa, jaka miała miejsce na etapie konstruowania Dyrektywy NIS:

We wniosku Komisji Europejskiej z dnia 7 lutego 2013 roku cyberbezpieczeństwo zostało zdefiniowane jako (...) *odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na zdarzenia przypadkowe lub działania złośliwe naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przekazywanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy* (...).

W tekście przyjętym przez Parlament Europejski definicja cyberbezpieczeństwa jest sformułowana jako (…) *odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność, przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne* (...). Powyższa definicja została przeniesiona bez zmian do ustawy.

Zmiany, które zaszły w definicji cyberbezpieczeństwa polegały na zastąpieniu katalogu zdarzeń przypadkowych i złośliwych, pojęciem wszelkich działań, na które odporne mają być sieci i systemy informatyczne. W ostatecznym tekście Dyrektywy NIS nie znalazło się także pojęcie zagrożenia, czyli zdarzenia, które potencjalnie może mieć wpływ na bezpieczeństwo. Unijny ustawodawca zawarł zagrożenie w definicji ryzyka, które określił jako każdą dającą się racjonalnie określić okoliczność lub zdarzenie, które ma potencjalny niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych. Ustawodawca krajowy z kolei zaproponował w ustawie następującą definicję ryzyka — wielkość charakteryzująca prawdopodobieństwo oraz skutek wystąpienia potencjalnego negatywnego zdarzenia w systemie informacyjnym lub mającego wpływ na system informacyjny, w szczególności służący do świadczenia usług kluczowych lub usług cyfrowych. O ile zmiany w Dyrektywie NIS można określić, jako pewne dopuszczalne uproszczenie postrzegania bezpieczeństwa, to już modyfikacje na poziomie ustawy wprowadzają istotną nieścisłość. Różnica polega na tym, że Dyrektywa NIS z jed-

nej strony wyraża oczekiwanie reagowania na wszelkie działania naruszające bezpieczeństwo, niemniej poprzez definicję ryzyka doprecyzowuje, że chodzi o zdarzenia „dające się racjonalnie określić". W przypadku projektu ustawy w definicji ryzyka ustawodawca odwołuje się jedynie do tzw. zdarzeń kwantyfikowalnych, czyli takich, które można określić za pomocą parametru prawdopodobieństwa i skutku. Definicja nie uwzględnia zdarzeń niekwantyfikowalnych, czyli np. ryzyka prawnego, czy ryzyka utraty zaufania. Powyższe zawężenie może prowadzić do nieosiągnięcia celu Dyrektywy NIS, jakim jest podniesienie poziomu zaufania społeczeństwa do usług świadczonych w cyberprzestrzeni. Dyrektywa w swoich założeniach w zakresie zarządzania ryzykiem odwołuje się do obowiązku łagodzenia wpływu incydentów, a utrata reputacji, czy naruszenia prawa, niewątpliwie do skutków incydentów należą.

4. Rola zespołów reagujących na zagrożenia i incydenty

Doskonalenie procesu zarządzania ryzykiem bezpieczeństwa systemów informatycznych będzie zależeć od skuteczności systemu wymiany informacji o zagrożeniach, którego kluczowym elementem określonym w Dyrektywie NIS oraz ustawie jest obowiązek zgłaszania incydentów bezpieczeństwa przez podmioty objęte Ustawą. Zgodnie z wytycznymi Dyrektywy NIS każdy kraj członkowski jest zobowiązany powołać krajowy zespół reagujący na zagrożenia i incydenty bezpieczeństwa w cyberprzestrzeni, tzw. CSIRT (ang. *Computer Security Incident Response Team*).

Projekt ustawy przewiduje powołanie trzech CSIRT sektorowych na poziomie krajowym:

– istniejący CSIRT NASK prowadzony przez Naukową Akademicką Sieć Komputerową,

– CSIRT MON prowadzony przez Ministerstwo Obrony Narodowej oraz

– CSIRT GOV prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego.

Najogólniej pojętą rolą CISRT sektorowych będzie *(…) współpraca ze sobą, aby zapewnić spójny i kompletny system zarządzania ryzykiem w zakresie cyberbezpieczeństwa państwa oraz obsługę zgłoszonych incydentów, w tym zwłaszcza incydentów poważnych i krytycznych, najpoważniejszych z punktu widzenia państwa*. Nie brak głosów krytycznych, wskazujących na niezasadność tworzenia trzech CSIRT, zamiast jednego. Wśród najczęściej powtarzanych argumentów jest wydłużanie ścieżki komunikacyjnej przy reagowaniu na atak, który swoim zakresem obejmie podmioty „przynależne" do różnych CSIRT, a także ryzyko, że podmiot objęty Ustawą będzie zmuszony raportować do więcej niż jednego CSIRT, jeżeli usługi kluczowe prowadzone przez podmiot podlegają pod różne CSIRT.

5. Podobieństwa i różnice między Dyrektywą NIS a Rozporządzeniem ODO

Zapewnienie bezpieczeństwa systemów informatycznych jako kolejny obowiązek wymieniony w projekcie Ustawy może zostać zrealizowany z wykorzystaniem istniejących norm i standardów branżowych. Kiedy jest mowa o bezpieczeństwie pojawia się termin dany poziom zaufania. Poziom uzasadnionego zaufania do zabezpieczeń to termin pochodzący ze standardu ISO/IEC 15408 Common Criteria, czyli normy pozwalającej w sposób formalny weryfikować bezpieczeństwo systemów informatycznych. Poziom zaufania jest mierzony w skali 7 stopniowej EAL, gdzie EAL 7 stanowi najwyższy poziom uzasadnionego zaufania. Istotne jest, że już na etapie projektowania określonego systemu informatycznego, ustawodawca będzie wymagał określania poziomu wymaganego zaufania do danego systemu oraz zbioru wymagań bezpieczeństwa, jakie dany system powinien spełnić.

Warto tu także podkreślić związek pomiędzy wymogami Dyrektywy NIS, a założeniami Rozporządzenia ODO. Obydwa akty prawne obejmują swym zakresem ochronę danych, niemniej o ile Dyrektywa NIS koncentruje się przede wszystkim na zapewnieniu ciągłości usług kluczowych, to Rozporządzanie ODO wymaga przede wszystkim zapewnienia bezpieczeństwa danych z punktu widzenia zachowania reputacji oraz zaufania podmiotów danych, którego naruszenie jest sankcjonowane wysokimi karami. Powyższe podejście świadczy o tym, że przynajmniej w tej części cyberbezpieczeństwa, które dotyczy danych osobowych ryzyko reputacyjne, czy utraty zaufania powinno być traktowane na równi ze skutkami matematycznie mierzalnymi (dodatkowe koszty, przerwa w działaniu procesów, itd.).

Kolejnym istotnym punktem wspólnym obydwu aktów prawnych jest obowiązek zgłaszania incydentów. Dyrektywa NIS narzuca znacznie szerszy zakres ochrony danych niż Rozporządzenie ODO, w tym także szerszy obowiązek zgłaszania incydentów. Rozporządzenie ODO wymaga skupienia się nie tylko na ryzyku naruszeń cyber, ale przede wszystkim na skutkach tych naruszeń dla ochrony prywatności podmiotów danych.

Istotnym podobieństwem obydwu aktów prawnych jest także obowiązek wdrożenia zabezpieczeń, których skuteczność została wyznaczona w oparciu o analizę ryzyka. Dodatkowym źródłem informacji odnośnie prawidłowego wdrożenia Rozporządzenia ODO są wytyczne Grupy Roboczej art. 29, które w sposób spójny i szczegółowy wytyczają ścieżkę dojścia do zgodności „problematycznych" zapisów Rozporządzenia ODO. Słabością regulacyjną pozostaje brak transpozycji wytycznych do prawa krajowego. Dla przykładu w Opinii 2/2017 Grupy Roboczej Art. 29 dotyczącej przetwarzania danych w pracy (WP 249), sformułowano obowiązek przeprowadzenia przez podmioty wdrażające Rozporządzenie ODO konsultacji społecznych przed wdrożeniem niektórych Polityk dotyczących bezpieczeństwa, jeżeli prawo lokalne tego wymaga. Ocena zasadności przeprowadzenia takich konsultacji będzie leżała indywidualnie po stronie każdego podmiotu, zamiast być dookreślona przez lokalny organ regulacyjny. Nieprzeprowadzenie takiej oceny w wyniku niewłaściwej interpretacji zapisów Rozporządzenia ODO może

skutkować karami ze strony organu regulacyjnego oraz stanowić ryzyko dla ochrony prywatności.

Inne kluczowe podobieństwa i różnice w zakresie stosowana dyrektywy NIS oraz Rozporządzenia ODO to:

1) Cel wdrożenia Rozporządzenia ODO to bezpieczeństwo danych osobowych, cel dyrektywy NIS to bezpieczeństwo sieci.

2) Obydwa akty prawne wymagają wdrożenia opartego na analizie ryzyka.

3) Rozporządzenie ODO stosuje się do prawie każdego podmiotu, który przetwarza dane osobowe, dyrektywa NIS do bardzo wąskiej liczby podmiotów świadczących usługi kluczowe, przy czym niemal pewne jest, że wszystkie podmioty podlegające pod Dyrektywę NIS będą także podlegać pod Rozporządzenie ODO.

4) Obydwa akty prawne wymagają wdrożenia zgłaszania incydentów, ale chodzi o różne typy incydentów. Zgłaszanie incydentów zgodnie z Rozporządzeniem ODO jest wymagane, kiedy zagrożona jest poufność danych osobowych, dyrektywa NIS wymaga, aby zgłaszać incydenty, które mogą zagrozić ciągłości działania usług. Rozporządzenie ODO obok zgłoszenia incydentów do odpowiednich organów, często wymaga także powiadomienia podmiotów danych, których dane uległy lub mogły ulec wyciekowi.

5) Inna jest także konstrukcja sankcji. Zgodnie z Rozporządzeniem ODO wyciek danych osobowych może podlegać karze. W przypadku Dyrektywy NIS sankcjami jest objęte niewdrożenie określonych środków zabezpieczających.

Niewątpliwie obydwa akty prawne przenikają się regulacyjnie w wielu obszarach, a ich skuteczne stosowanie będzie istotnie uzależnione od spójnego podejścia ustawodawcy i właściwej koordynacji prac zespół przygotowujących poszczególne ustawy wdrażające. Nie brak takich niespójności na poziomie samych aktów unijnych. Dyrektywa NIS przyjęta 6 lipca 2016 roku odwołuje się do ówcześnie już nieobowiązującej Dyrektywy 95/46/EC dotyczącej ochrony danych osobowych. Ze wstępu do Dyrektywy wynika, że Europejski Inspektor Ochrony Danych Osobowych — organ nadzorczy Unii Europejskiej odpowiedzialny za ochronę za ochronę danych osobowych, mający istotny wpływ na kształt Rozporządzenia ODO wyraził opinię na temat Dyrektywy NIS 14 czerwca 2013 roku, czyli prawie 3 lata przed przyjęciem Rozporządzenia ODO w obowiązującym kształcie.

6. Podsumowanie

Przed krajowym prawodawcą stoi wyzwanie w postaci zapewnienia spójnych i kompletnych ram prawnych zarówno dla ochrony przed atakami cybernetycznymi, jak i w zakresie ochrony danych osobowych. Jeszcze większe wyzwanie stoi przed przedsiębiorcami i instytucjami, które podlegają pod obydwa akty prawne. Krajowe przepisy wdrażające wciąż nie doczekały się ostatecznych kształtów, a jednocześnie terminy wdrożenia działań wynikających z RODO i Dyrektywy NIS biegną, czasu jest coraz mniej.

---

[1] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. 2011 nr 199, poz. 1175).

[2] Założenia strategii Jednolitego Rynku Cyfrowego dostępne na stronie https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market, (dostęp w dniu 8.11.2018 r.).

[3] 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

[4] 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) (Tekst mający znaczenie dla EOG) zwane dalej Rozporządzeniem ODO.

[5] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560).

[6] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000).

[7] Zespół roboczy ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (ang. *Working Party on the Protection of Individuals with regard to the Processing of Personal Data*) — niezależny podmiot o charakterze doradczym, powołany na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych

[8] https://giodo.gov.pl/pl/259/9718

[9] Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii, dostępny pod adresem http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52013PC0048&from=PL, (dostęp w dniu 6.11.2017 r.).

Bibliografia

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. 2011 nr 199, poz. 1175).
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000).
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560).
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.
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) (Tekst mający znaczenie dla EOG) zwane dalej Rozporządzeniem ODO.

Źródła internetowe:
Strona Generalnego Inspektora Ochrony Danych Osobowych — https://giodo.gov.pl/.