CYBERPOLICY

Review

Biuletyn NASK

Strategia. Policy. Rekomendacje.

NASK

Biuletyn NASK

Strategia. Policy. Rekomendacje.

Nr 2/ kwiecień 2018

Redakcja: Magdalena Wrzosek

Słowo wstępu

Rok 2017 po wieloma względami był rokiem przełomowym w dziedzinie cyberbezpieczeństwa. Po przyjęciu w kwietniu *Krajowych Ram Polityki Cyberbezpieczeństwa* trwały prace nad projektem ustawy o Krajowym Systemie Cyberbezpieczeństwa, implementującej Dyrektywę NIS. W pracach tych uczestniczyli Eksperci PIB NASK, zwłaszcza w zakresie przygotowania prawnych ram współpracy zespołów CSIRT.

We wrześniu Komisja Europejska przedstawiła długo oczekiwany pakiet cyberbezpieczeństwa, a w nim nowelizację Strategii Bezpieczeństwa Cybernetycznego UE z 2013 roku, wytyczne w zakresie implementacji Dyrektywy NIS, propozycję nowego mandatu ENISA, rozwiązania legislacyjne w zakresie europejskiej certyfikacji oraz tzw. *Blueprint*, czyli propozycje działania w obliczu międzynarodowych incydentów cybernetycznych.

Najnowszy numer *Cyber Policy Review* porusza wszystkie te tematy. Zapraszam do lektury.

dr inż. Wojciech Kamieniecki, Dyrektor Państwowego Instytutu Badawczego NASK

Spis treści

Słowo wstępu
4

Krajowy System Cyberbezpieczeństwa
6

Kilka słów o RODO – ogólnym rozporządzeniu o ochronie danych
17

Nowy Pakiet Cyberbezpieczeństwa dla UE
25

Flash z Komisji Europejskiej
33

Krzysztof Silicki

Krajowy System Cyberbezpieczeństwa

Krzysztof Silicki – *Od września 2017 do marca 2018 Podsekretarz stanu w Ministerstwie Cyfryzacji, odpowiedzialny za kwestie cyberbezpieczeństwa. Ukończył studia na Politechnice Warszawskiej. Od 1992 roku związany z Państwowym Instytutem Badawczym NASK, gdzie w latach 2000-2012 pełnił funkcję dyrektora technicznego.*

Od roku 2004 reprezentuje Polskę w Radzie Zarządzającej Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz w Radzie Wykonawczej (od 2013 r.). W 2016 roku został mianowany Wiceprzewodniczącym Rady Zarządzającej ENISA.

W roku 1996 zorganizował pierwszy w kraju zespół reagujący na zagrożenia w Internecie – CERT NASK (Computer Emergency Response Team) – od roku 2000 funkcjonujący, jako CERT Polska. W latach 1997-1999 reprezentował NASK w FIRST (międzynarodowym forum zrzeszającym zespoły reagujące). Był również pomysłodawcą i koordynatorem odbywającej się, co roku konferencji SECURE – pierwszej w Polsce konferencji dotyczącej bezpieczeństwa teleinformatycznego. Jako dyrektor techniczny inicjował i nadzorował w NASK powstawanie kolejnych generacji sieci Internet, a także innowacyjnych projektów bezpieczeństwa, takich jak ARAKIS. i ARAKIS.GOV realizowany wspólnie z administracją państwową. W 2010 roku ARAKIS.GOV uhonorowany został godłem Teraz Polska w kategorii przedsięwzięć innowacyjnych.

Autor publikacji i opracowań w kraju i za granicą z dziedziny sieci teleinformatycznych ze szczególnym uwzględnieniem tematyki bezpieczeństwa. Współtworzył strategię i plan działania ENISA w dziedzinie bezpieczeństwa sieci i informacji a także współtworzył NC Cyber w NASK. Uczestniczy w wielu europejskich i polskich projektach, jako ekspert ds. bezpieczeństwa sieci i informacji. Nominowany do prestiżowej nagrody InfoStar w roku 2009 i 2011, laureat tej nagrody w roku 2011 w kategorii rozwiązania informatyczne.

Problematyka cyberbezpieczeństwa stanowi obecnie obowiązkowy komponent działań strategicznych każdego rozwiniętego kraju. Wraz z rozwojem technologii, wykorzystujących cyfrowe formy komunikacji, transakcji handlowych, dostępu do usług administracji publicznej, mediów czy realizacji procesów gospodarczych oraz społecznych – problem zagrożeń i incydentów cyberbezpieczeństwa wymaga systemowego podejścia zarówno ze strony państwa, organizacji międzynarodowych, jak i kluczowych sektorów gospodarki.

W Unii Europejskiej, w roku 2013, przyjęta została pierwsza strategia cyberbezpieczeństwa[1]. W ramach realizacji priorytetu: Osiągnięcie odporności na zagrożenia cybernetyczne, Komisja Europejska zaproponowała nową dyrektywę, której zamierzeniem jest właśnie systemowe podejście do problematyki cyberbezpieczeństwa w całej UE. Jest to tzw. Dyrektywa NIS[2], która w lipcu 2016 r. została przyjęta przez Parlament Europejski i Radę – po trzech latach trudnych negocjacji pomiędzy krajami członkowskimi i instytucjami Unii Europejskiej.

Dyrektywa NIS

Dyrektywa NIS wprowadza szereg mechanizmów współdziałania oraz obowiązków w dziedzinie cyberbezpieczeństwa. Główne z nich to:

- przyjęcie krajowych strategii bezpieczeństwa sieci i systemów teleinformatycznych,
- ustanowienie krajowych organów właściwych ds. bezpieczeństwa sieci i informacji oraz krajowych punktów kontaktowych do współpracy międzynarodowej,
- powołanie zespołów reagowania na incydenty komputerowe (CSIRT) obsługujących kluczowe sektory gospodarki,
- ustanowienie obowiązku wdrażania odpowiednich środków bezpieczeństwa oraz konieczności zgłaszania incydentów dla operatorów kluczowych usług w zdefiniowanych sektorach,
- określenie wymogów bezpieczeństwa także dla zdefiniowanych kategorii operatorów usług cyfrowych (lżejsze, zharmonizowane w UE podejście)
- powołanie Grupy Współpracy wspierającej współpracę krajów członkowskich na poziomie strategicznym,

[1] *„Wspólny komunikat Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń" z dnia 7.02.2013 r.*

[2] *„ Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii"*

wymianę informacji, opracowywanie rekomendacji,

- stworzenie sieci zespołów CSIRT (CSIRT network) dla wsparcia współpracy operacyjnej w UE w obszarze incydentów naruszających cyberbezpieczeństwo.

Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022

W naszym kraju w roku 2017, w wyniku prac międzyresortowego zespołu roboczego powstał dokument strategiczny o nazwie: Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022.[3] W pracach nad nim wzięli udział przedstawiciele wielu ministerstw (min. MON, MSWiA, MSZ, MZ, MNiSW, MR), przedstawiciele służb (min. Policji, ABW, SKW) i inne instytucje (BBN, PIB NASK). Koordynatorem procesu powstawania Krajowych Ram było Ministerstwo Cyfryzacji. Dokument, który na przełomie kwietnia i maja ub.r. został przyjęty uchwałą Rady Ministrów przewiduje kilka celów szczegółowych, w ramach realizacji celu głównego, zdefiniowanego jako: „Zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych". Tak więc wśród celów szczegółowych przewidziano:

- osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów,
- wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom,
- zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni,
- zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

W ramach celu pierwszego z powyższej listy zostały zdefiniowane takie zadania jak: dostosowanie krajowego otoczenia prawnego do potrzeb i wyzwań, udoskonalenie krajowego systemu cyberbezpieczeństwa czy zwiększenie bezpieczeństwa usług kluczowych i cyfrowych. Temu, miedzy innymi służy opracowywany przez MC projekt ustawy o krajowym systemie cyberbezpieczeństwa.

Ustawa o Krajowym Systemie Cyberbezpieczeństwa

Celem projektu ustawy jest przygotowanie uregulowań prawnych umożliwiających implementację dyrektywy NIS oraz stworzenie ram prawnych dla efektywnego funkcjonowania systemu bezpieczeństwa teleinformatycznego na poziomie krajowym.

Krajowy system cyberbezpieczeństwa jest rozumiany, jako zespół współpracujących ze sobą podmiotów zdefiniowanych w ustawie, w celu osiągania odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia usług kluczowych i usług cyfrowych oraz zapewnienie obsługi incydentów.

Do podmiotów krajowego systemu cyberbezpieczeństwa zalicza się:

- Organy właściwe do spraw cyberbezpieczeństwa
- Zespoły CSIRT poziomu krajowego
- Operatorów usług kluczowych i dostawców usług cyfrowych
- Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa
- Rządowe Centrum Bezpieczeństwa
- Podmioty świadczące usługi z zakresu cyberbezpieczeństwa
- Przedsiębiorców telekomunikacyjnych
- Podmioty administracji publicznej wraz z jednostkami podległymi i nadzorowanymi
- Inne podmioty wykonujące zadania publiczne
- Sądy i trybunały
- Uczelnie publiczne i Polską Akademię Nauk

W stosunku do sektorów usług kluczowych, zdefiniowanych w dyrektywie NIS i objętych ustawą, takich jak: energetyczny (elektryczny, paliwa płynne, gaz), transportowy (powietrzny, kolejowy, wodny, drogowy), bankowy, finansowy, zdrowia, wody pitnej (dostawa, dystrybucja) i infrastruktury cyfrowej (IXP, dostawcy usług DNS, rejestry TLD) przewidziano nadzór organów właściwych, którymi będą właściwi ministrowie działowi.

W projekcie przewidziano dodatkowo, ponieważ dyrektywa nie obejmuje tych sektorów, uwzględnienie w krajowym systemie także sektora telekomunikacyjnego oraz administracji publicznej. Sektor telekomunikacyjny ma już odrębne uregulowania, które nakładają na operatorów obowiązki podobne do tych, jakie przewidziane są w dyrektywie. Kwestia administracji publicznej zaś, została pozostawiona krajom członkowskim do samodzielnej decyzji.

W naszym kraju projektodawcy uznali, że nieuwzględnienie wspomnianych sektorów w ramach krajowego systemu cyberbezpieczeństwa byłoby podejściem cząstkowym, niegwarantującym osiągnięcia celu głównego wyrażonego w Krajowych Ramach Polityki Cyberbezpieczeństwa 2017-2022.

Dlatego też przewidziano objęcie przedsiębiorstw telekomunikacyjnych obowiązkiem zgłaszania incydentów do jednego systemu. Projekt uwzględnia możliwość włączenia w system przedsiębiorstw telekomunikacyjnych, za pośrednictwem

[3] *https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/0bbc7a32-64df-b45e-b08c-dac59415f109*

Prezesa UKE, na postawie obowiązku nałożonego na UKE przy wykorzystaniu obecnie obowiązujących przepisów. Prezes UKE (który będzie użytkownikiem systemu służącego m.in. do zgłaszania i obsługi incydentów) zgodnie z zapisami projektu przekazuje informacje do CSIRT, właściwego dla zgłaszającego przedsiębiorcy telekomunikacyjnego.

Z kolei włączenie administracji publicznej do systemu cyberbezpieczeństwa powoduje pewne dodatkowe obowiązki, głównie związane z obsługą incydentów, takie jak ich: identyfikacja, klasyfikacja, dokumentowanie obsługi oraz obowiązek zgłaszania incydentów poważnych do właściwego CSIRT poziomu krajowego.

Obowiązki operatorów usług kluczowych i dostawców usług cyfrowych

Rdzeniem dyrektywy NIS oraz projektowanej ustawy są zapisy, dotyczące operatorów, działających w zdefiniowanych, kluczowych sektorach gospodarki, wymienionych wyżej oraz dostawcy usług, takich jak internetowe platformy handlowe, wyszukiwarki on-line oraz usługi chmurowe.

Operatorzy usług kluczowych odpowiadają za bezpieczeństwo i ciągłość świadczonych usług. Dlatego są zobowiązani do wdrożenia systemu zarządzania bezpieczeństwem, szacowania i zarządzania ryzykiem, aby na tej podstawie stosować adekwatne środki bezpieczeństwa. Opracowują dokumentację, dotyczącą cyberbezpieczeństwa systemów teleinformatycznych. Wyznaczają osobę do kontaktów w obszarze cyberbezpieczeństwa świadczonych usług kluczowych. Powinni powołać wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawrzeć umowy z podmiotami zewnętrznymi, świadczącymi usługi z zakresu cyberbezpieczeństwa. Obowiązkowo operatorzy usług kluczowych przeprowadzają, co najmniej raz na dwa lata audyt bezpieczeństwa teleinformatycznego. Jednym z podstawowych obowiązków operatorów jest zgłaszanie poważnych incydentów (wg. kryteriów zdefiniowanych w ustawie oraz progów wyzwalających, określonych w aktach wykonawczych).

W stosunku do dostawców usług cyfrowych panują podobne, co do zasady, lecz nieco lżejsze obowiązki. Ze względu na konieczność harmonizacji w UE obowiązki te są identyczne w całej Unii – opisane w odpowiednim rozporządzeniu wykonawczym KE.

Dostawcy mają stosować środki bezpieczeństwa proporcjonalne do ryzyka oraz zgłaszać istotne incydenty do właściwych CSIRT, jednak po pierwsze mikro i małe przedsiębiorstwa są z tego obowiązku wyłączone, po drugie zaś organy właściwe mają uprawnienie do dokonywania kontroli jedynie ex-post, po wystąpieniu i ujawnieniu się istotnego incydentu.

Zespoły CSIRT

Kluczowe dla funkcjonowania KSC są rozstrzygnięcia w zakresie zespołów reagujących na poziomie krajowym. Sama dyrektywa NIS przewiduje powoływanie zespołów typu CSIRT (Computer Security Incident Response Team) dla koordynacji obsługi poważnych incydentów w sektorach zdefiniowanych, jako kluczowe. Jak przedstawiono na rysunku poniżej, w krajowej architekturze cyberbezpieczeństwa mamy do czynienia z trzema zespołami: CSIRT MON, CSIRT GOV i CSIRT NASK, z których każdy jest przypisany innym obszarom. Pierwszy obsługuje resort obrony narodowej i wszystkie podmioty podległe lub nadzorowane przez MON, drugi: podmioty infrastruktury krytycznej oraz administrację państwową, trzeci: dostawców usług cyfrowych, jednostki samorządu terytorialnego, podmioty niewpisane na listę infrastruktury krytycznej oraz osoby fizyczne.

Trzy CSIRTy poziomu krajowego współpracują przy koordynacji incydentów poważnych, w szczególności ponadsektorowych. Mogą także przeklasyfikować incydent na incydent krytyczny (zagrażający bezpieczeństwu narodowemu, powodujący sytuację kryzysową w kraju itp.) i uruchomić mechanizm zwany Zespołem Incydentów Krytycznych (trzy CSIRTy oraz RCB), który wprowadza jeszcze silniejszą koordynację oraz może z kolei uruchomić ścieżkę eskalacyjną na poziom Rządowego Zespołu Zarządzania Kryzysowego.

Projekt ustawy przewiduje także utworzenie sektorowych zespołów cyberbezpieczeństwa, ustanowionych przez organ właściwy dla danego sektora lub podsektora. Zadaniem tych zespołów będzie obsługa lub wsparcie obsługi incydentów sektorowych.

Organy właściwe

Ministrowie odpowiedzialni za dany dział – utożsamiany z sektorem kluczowym, pełnią rolę tzw. organów właściwych, które:

- Prowadzą analizę podmiotów w danym sektorze pod kątem uznania ich za operatorów usług kluczowych lub odebrania im statusu operatorów usług kluczowych;
- Wydają decyzję o uznaniu podmiotów za operatorów usług kluczowych lub decyzję o odebraniu podmiotom statusu operatorów usług kluczowych;
- Przygotowują rekomendacje do działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów;
- Mogą prowadzić współpracę z właściwymi organami państw członkowskich Unii Europejskiej za pośrednictwem Pojedynczego Punktu Kontaktowego;

- Przetwarzają informacje, dotyczące świadczonych usług kluczowych oraz operatorów usług kluczowych;
- Uczestniczą w ćwiczeniach w zakresie cyberbezpieczeństwa, uruchamianych na poziomie krajowym i w Unii Europejskiej.

Organy właściwe zyskają także uprawnienie do przeprowadzania kontroli wypełniania przez operatorów usług kluczowych obowiązków, wynikających z ustawy, a także nakładania kar, w przypadku stwierdzenia uchybień.

Pojedynczy Punkt Kontaktowy (PPK)

Organ ten, przewidziany w dyrektywie NIS, zapewnia reprezentację Rzeczypospolitej Polskiej w tzw. Grupie Współpracy odpowiadającej za współpracę strategiczną państw UE w obszarze cyberbezpieczeństwa oraz współpracuje w tej dziedzinie z Komisją Europejską.

PPK zajmuje się także koordynacją współpracy pomiędzy organami właściwymi i organami władzy publicznej w Rzeczpospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej. W projekcie ustawy rolę PPK pełni minister właściwy ds. informatyzacji.

Sektorowe zespoły cyberbezpieczeństwa

Projekt ustawy przewiduje, iż w ramach zapewniania przez operatorów i dostawców właściwego poziomu bezpieczeństwa i reagowania na incydenty mogą oni korzystać z usług wyspecjalizowanych podmiotów, świadczących usługi cyberbezpieczeństwa. Zakres tych usług i sposób ich realizacji zależy od decyzji operatora, który dokonuje wyboru modelu realizacji wymogów: budując własne struktury lub korzystając z usług zewnętrznych. W każdym przypadku odpowiedzialność pozostaje po stronie operatora i przykładowo, zawierając umowę z podmiotem zewnętrznym na świadczenie usług, musi on zadbać o to, by poziom tych usług był właściwy a dostawca gwarantował bezpieczeństwo.

Podmioty świadczące usługi cyberbezpieczeństwa będą mogły oczywiście świadczyć np. usługi ciągłego monitorowania i reagowania na incydenty dla wielu podmiotów w danym sektorze czy nawet w kilku sektorach – kwestie te pozostawione zostały procesom biznesowym i samoregulacji rynku.

Jednak organy właściwe będą mogły zdecydować o powołaniu w danym sektorze lub podsektorze zespołów reagowania przypisanych danej grupie przedsiębiorców. Takie sektorowe zespoły cyberbezpieczeństwa powstawać mogą w oparciu o przepisy sektorowe, które zdefiniują formę, sposób i zakres działania – pozostaje to w gestii ministrów odpowiedzialnych za poszczególne działy.

Idea funkcjonowania takich zespołów jest bardziej kompleksowa, bo uwzględnia specyfikę danego sektora, dostosowując do niej wsparcie w zakresie cyberbezpieczeństwa. W przypadku powołania takiego zespołu sektorowego, projekt ustawy przewiduje, że operatorzy usług kluczowych, w sektorze lub podsektorze, w którym działa zespół sektorowy, będą zgłaszali istotne incydenty zarówno do właściwego CSIRTu krajowego, jak też do zespołu sektorowego. Zespoły sektorowe i CSIRTy będą współpracowały w celu osiągnięcia optymalnego modelu koordynacji incydentów na poziomie sektorowym i ponadsektorowym.

Kolegium do spraw cyberbezpieczeństwa i Pełnomocnik Rządu ds. Cyberbezpieczeństwa

W trakcie procesu uzgodnień, konsultacji i opiniowania Ministerstwo Cyfryzacji otrzymało między innymi uwagi, odnoszące się do potrzeby ustanowienia w KSC ciała lub mechanizmu koordynacji na poziomie strategicznym. Wskazywano, że oprócz przewidzianych mechanizmów koordynacji w zakresie postępowania z incydentami (opisanymi wyżej) potrzebna jest także koordynacja na poziomie strategicznym, umożliwiająca takie działania jak ocena funkcjonowania KSC, wypracowywanie nowych kierunków strategicznych i rozwiązywanie problemów o charakterze systemowym.

W związku z tym w nowej wersji projektu ustawy, po konferencji uzgodnieniowej i konsultacjach społecznych, zostały wprowadzone zapisy o powołaniu Pełnomocnika ds. Cyberbezpieczeństwa oraz ustanowieniu Kolegium ds. Cyberbezpieczeństwa – inspirowane mechanizmem kolegium ds. służb specjalnych. Pełnomocnik odpowiadał będzie za koordynowanie na poziomie krajowym realizacji zadań dotyczących zapewnienia cyberbezpieczeństwa w kraju, w tym m.in. sprawował będzie nadzór nad procesem zarządzania ryzykiem w skali kraju oraz tworzył wytyczne dla opracowania rządowych dokumentów, dotyczących cyberbezpieczeństwa. Pełnomocnika powoływał i odwoływał będzie Prezes Rady Ministrów i będzie to Minister w randze Sekretarza Stanu.

Ponad dyrektywę...

Ustawa o Krajowym Systemie Cyberbezpieczeństwa, jak wspomniano na wstępie, stanowi implementację dyrektywy NIS. Nie znaczy to jednak, że się do tego ogranicza. W projekcie jest szereg rozwiązań, które wykraczają poza samą dyrektywę – do czego każdy kraj członkowski ma prawo, ponieważ dyrektywa

stanowi tzw. harmonizację minimalną

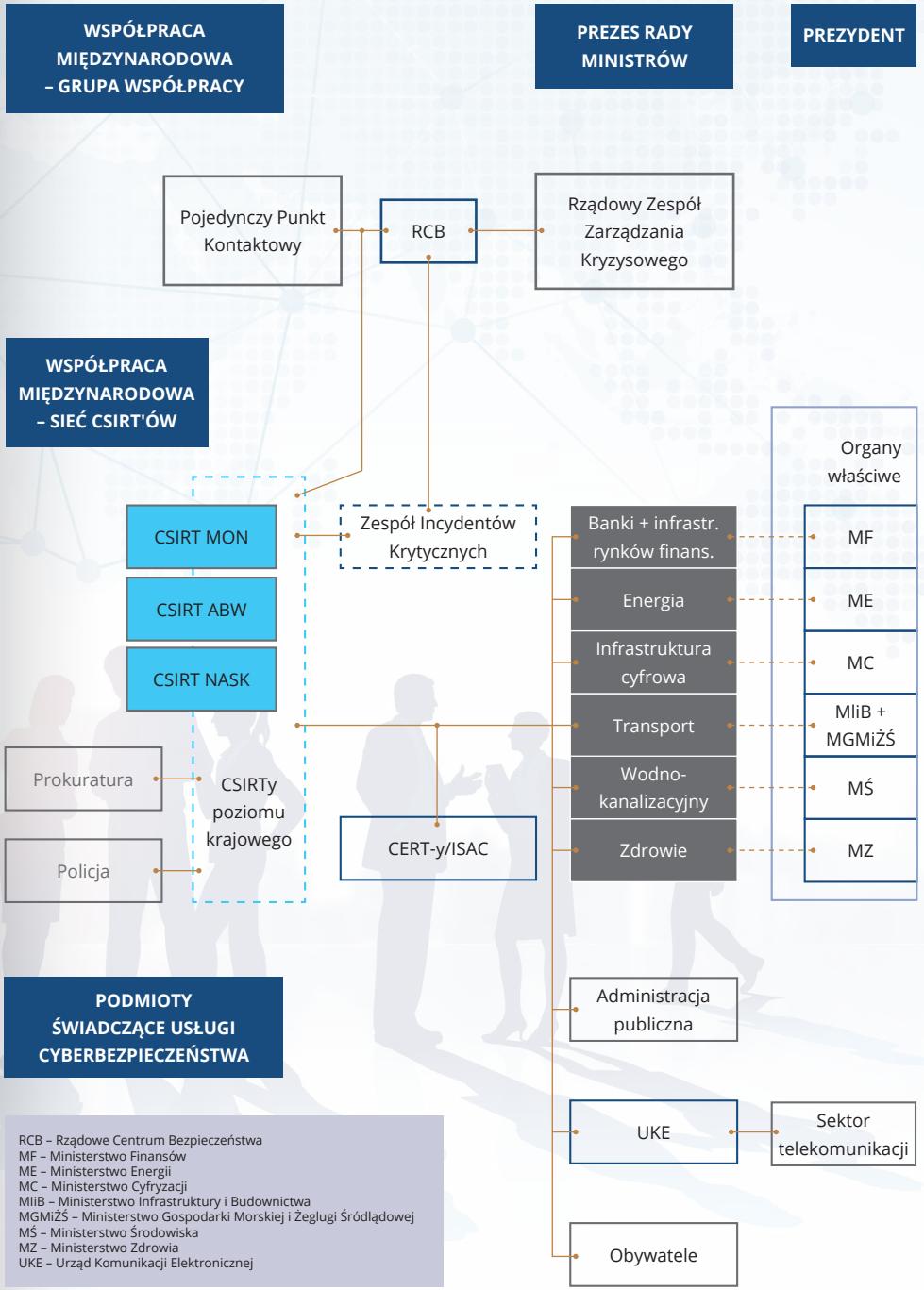
Przykładowo, ustawa operuje pojęciem incydentu szerszym niż to wprowadzone w dyrektywie, która mówi o zdarzeniach o określonym skutku zakłócającym i powodującym negatywny wpływ na działanie usługi (łącznie z przerwaniem jej działania). Ustawodawca zaproponował szersze rozumienie incydentu, który obejmuje również zagrożenie, które nie koniecznie się zmaterializowało. Podejście to pozwala na uzyskanie szerszego obrazu cyberbezpieczeństwa i podejmowanie działań, na przykład ostrzegających inne sektory czy podmioty w przypadku wystąpienia poważnych zagrożeń. Takie zagrożenia, np. wykryte i zneutralizowane przez zaawansowany system bezpieczeństwa w jednym podmiocie – mogą posłużyć do tworzenia ostrzeżeń dla innych uczestników KSC.

Także jeśli chodzi o sektory, wchodzące w skład krajowego systemu, mamy do czynienia z rozszerzeniem. Projekt ustawy przewiduje, bowiem, że sektor administracji publicznej (nieobjęty dyrektywą) także zostanie objęty określonymi wymogami KSC. Dodatkowo sektor telekomunikacyjny, w którym obowiązują już regulacje dotyczące zapewnienia integralności i bezpieczeństwa, będzie połączony z systemem krajowym poprzez włączenie do KSC regulatora sektorowego, czyli Urzędu Komunikacji Elektronicznej, do którego telekomy mają obowiązek zgłaszania incydentów, wynikający z ustawy Prawo telekomunikacyjne.

Stan aktualny

Projekt ustawy jest już na ostatniej prostej. Zakończył się proces uzgodnień, konsultacji i opiniowania. Za nami konferencja uzgodnieniowa, na której podjęto kluczowe decyzje, co do uwzględnienia uwag oraz Komisja Wspólna Rządu i Samorządu, która zaopiniowała projekt pozytywnie. Projekt został także przyjęty przez Komitet Rady Ministrów do Spraw Europejskich (KSE) oraz Komitet Rady Ministrów ds. Cyfryzacji (KRMC). 4 kwietnia br, projekt został przyjęty przez Stały Komitet Rady Ministrów.

Poniższy schemat przedstawia architekturę systemu reagowania.



Komentarz NASK

16 marca 2018 r. Rada Ministrów przyjęła Rozporządzenie w sprawie ustanowienia Pełnomocnika Rządu do spraw Cyberbezpieczeństwa. Funkcję tą pełni Podsekretarz Stanu w Ministerstwie Obrony Narodowej . Rozporządzenie obowiązuje od 21 marca 2018 roku.

Głównym zadaniem Pełnomocnika jest koordynacja działań oraz realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa. Za zapewnienie obsługi merytorycznej, organizacyjno-prawnej, technicznej, kancelaryjno-biurowej, oraz za pokrycie wydatków związanych z działalnością Pełnomocnika odpowiada Ministerstwo Obrony Narodowej. Organy administracji rządowej oraz jednostki im podległe lub przez nienadzorowane mają obowiązek współdziałania i udzielenia pomocy Pełnomocnikowi Rządu, w szczególności przez udostępnianie mu informacji niezbędnych do realizacji jego zadań, zdefiniowanych, jako:

1. Analiza i ocena stanu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników opracowanych przy udziale organów administracji rządowej oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego działających w Ministerstwie Obrony Narodowej, Agencji Bezpieczeństwa Wewnętrznego oraz Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym;
2. Opracowywanie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym;
3. Opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa
4. Prowadzenie i koordynowanie działań prowadzonych przez organy administracji rządowej mających na celu podnoszenie świadomości społeczeństwa w zakresie zagrożeń cyberbezpieczeństwa i bezpiecznego korzystania z Internetu;
5. Inicjowanie krajowych ćwiczeń z zakresu cyberbezpieczeństwa;
6. Współpraca w sprawach związanych z cyberbezpieczeństwem z innymi państwami, organizacjami oraz instytucjami międzynarodowymi;
7. Podejmowanie działań mających na celu wspieranie badań naukowych i rozwój technologii z zakresu cyberbezpieczeństwa.

Pełnomocnik będzie przedstawiał Radzie Ministrów coroczne sprawozdanie ze swojej działalności oraz analizy, oceny i wnioski związane z zakresem jego działania.

Michał Czerniawski

Kilka słów o RODO – ogólnym rozporządzeniu o ochronie danych

Michał Czerniawski *– prawnik, urzędnik państwowy, jeden z negocjatorów rozporządzenia 2016/679. Wykładowca na studiach podyplomowych oraz szkoleniach z zakresu ochrony danych osobowych. Specjalizuje się w ochronie danych osobowych, własności intelektualnej i prawie Internetu. Autor ponad 30 publikacji z zakresu prawnych aspektów nowych technologii. Absolwent Wydziału Prawa i Administracji Uniwersytetu Warszawskiego oraz Wydziału Prawa Uniwersytetu Ottawskiego (LL.M. with Concentration in Law and Technology). Publikował m.in. na łamach wydawanego przez Uniwersytet Oksfordzki „International Data Privacy Law". Doświadczenie zawodowe zdobywał w renomowanych warszawskich kancelariach prawniczych, a także w biurze Europejskiego Inspektora Ochrony Danych (EDPS) oraz w biurze Kanadyjskiego Komisarza ds. Prywatności (OPC). Stypendysta Edward Barry McDougall Memorial Scholarship na Uniwersytecie Ottawskim.*

Wraz z rozwojem społeczeństwa informacyjnego – społeczeństwa, w którym niezwykle cennym towarem stało się szczególne dobro niematerialne, jakim jest informacja – nastąpił rozwój technologii, które ułatwiają pozyskiwanie i przetwarzanie najróżniejszych rodzajów danych, w tym danych osobowych. Dotychczas obowiązujące przepisy o ochronie danych osobowych, negocjowane na początku lat dziewięćdziesiątych ubiegłego wieku, coraz bardziej odstają od obecnych realiów technologicznych. Stąd też zaistniała potrzeba opracowania nowego aktu prawnego. Inaczej niż obecnie obowiązująca dyrektywa[5], która wymaga implementacji do krajowego porządku prawnego, a przez to nie zapewnia jednolitych standardów w całej Unii Europejskiej, nowy akt prawny ma formę rozporządzenia. **Ogólne rozporządzenie o ochronie danych (dalej też: RODO)[6] ma służyć wzmocnieniu i ujednoliceniu poziomu ochrony danych osobowych w całej Unii Europejskiej.** Unijny prawodawca zdecydował się na formę prawną rozporządzenia, jako mającą zapewnić **wyższy poziom harmonizacji przepisów o ochronie danych pomiędzy poszczególnymi państwami członkowskimi.** Ze względu na zakres zmian, które wprowadza, jest ono nazywane Rewolucją Kopernikańską w prawie ochrony danych osobowych[7]. Reguluje ono nie tylko przetwarzanie danych wewnątrz Unii Europejskiej, ale odnosi się również do przekazywania danych osobowych poza terytorium Unii, a także znajduje zastosowanie wobec administratorów danych spoza Unii, gdy prowadzą oni działania na jej terytorium (np. Facebook lub wiele innych dużych amerykańskich podmiotów). Głównym celem RODO jest zwiększenie kontroli osób fizycznych nad dotyczącymi ich danymi, a także uproszczenie otoczenia regulacyjnego, które w szczególności ma ułatwić operacje przetwarzania danych w kilku państwach członkowskich UE jednocześnie. Jednolite przepisy o ochronie danych osobowych mają także ułatwić prowadzenie działalności gospodarczej w Unii.

RODO zastąpi dyrektywę 95/46/WE. Zostało ono przyjęte w dniu 27 kwietnia 2016 r., a **zacznie być bezpośrednio stosowane w dniu 25 maja 2018 r.** W przeciwieństwie do dyrektywy nie wymaga ono implementacji do krajowego porządku prawnego i może być stosowane bezpośrednio. Niemniej, w praktyce, wdrożenie ogólnego rozporządzenia do krajowych porządków prawnych wymaga podjęcia działań legislacyjnych na poziomie krajowym, choćby w zakresie kwestii proceduralnych, czy też wyłączeń od praw i obowiązków z rozporządzenia, które przewiduje art. 23 rozporządzenia. W Polsce odpowiednie przepisy przygotowuje Ministerstwo Cyfryzacji[8].

Warto pamiętać, że choć powszechnie wspomina się o RODO, unijna reforma ma postać pakietu, w skład którego prócz ogólnego rozporządzenia wchodzi także tzw. **dyrektywa policyjna[9]**. Dyrektywa **dotyczy zarówno transgranicznego, jak i krajowego przetwarzania danych przez właściwe organy państw członkowskich w celu ścigania sprawców przestępstw.** Jednocześnie, zakres objętego nią przetwarzania danych osobowych uwzględnia także ochronę i zapobieganie zagrożeniom dla bezpieczeństwa publicznego, czego nie obejmowała decyzja ramowa, którą dyrektywa ma zastąpić.[10] Celem dyrektywy jest także **uwzględnienie specyfiki współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych.** Dyrektywa ma na celu zapewnienie równowagi pomiędzy prawem do ochrony danych osobowych a możliwością prowadzenia przez policję dochodzeń. Zawiera ona wykaz informacji, do których uzyskania osoba, której dane dotyczą, jest zawsze uprawniona – tak, aby umożliwić jej ochronę swoich praw. Ponadto, dyrektywa m.in. nakłada na administratora danych osobowych obowiązek wyznaczenia inspektora ochrony danych, wprowadza ocenę skutków danego przetwarzania, a także reguluje kwestie przekazywania danych osobowych do państw trzecich.

Zgodnie z założeniem RODO, we wszystkich państwach członkowskich ma znaleźć zastosowanie jednakowy zestaw zasad przetwarzania danych osobowych. Każde państwo członkowskie ustanawia własny organ nadzorczy w zakresie ochrony danych, organy te współpracują jednak ze sobą w ramach **Europejskiej Rady Ochrony Danych** (zastąpi ona tzw. Grupę Roboczą Art. 29), a także **„mechanizmu kompleksowej współpracy" (ang. „one-stop-shop").** W przypadku, gdy konkretny administrator danych działa w więcej niż jednym państwie członkowskim, wskazuje się tzw. organ wiodący, w oparciu o lokalizację tzw. głównej jednostki organizacyjnej administratora.

Ogólne rozporządzenie sankcjonuje nieznane wcześniej uprawnienia osób, których dane dotyczą, takie jak prawo do przenoszenia danych (art. 20 rozporządzenia) czy też prawo do bycia zapomnianym (art. 17 rozporządzenia). Rozszerza także m.in. obowiązek informacyjny (art. 12-14), który administrator danych musi zrealizować wobec osoby, której dane dotyczą. Jedną z nowości, które wprowadza ogólne rozporządzenie jest też uregulowanie kwestii profilowania (art. 22). Przyznaje ono osobie, której dane doty-

[5] Dyrektywa 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

[6] 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)

[7] Zob. Ch. Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', Bloomberg BNA Privacy and Security Law Report, 6 lutego 2012 r., s. 1-15.

[8] Zob. Ministerstwo Cyfryzacji, Projekt ustawy o ochronie danych osobowych https://mc.gov.pl/aktualnosci/projekt-ustawy-o-ochronie-danych-osobowych, dostęp 16.01.2018.

[9] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

[10] Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, OJ L 350, 30.12.2008, s. 60–71.

czą, m.in. uprawnienie do żądania ludzkiej interwencji, w przypadku, gdy dotycząca jej decyzja ma być oparta wyłącznie na algorytmie.

RODO wprowadza także dwa nowe rozwiązania – ochronę danych osobowych w fazie projektowania oraz ochronę danych osobowych, jako ustawienie domyślne (art. 25 RODO). Zgodnie z pierwszą z tych zasad, administrator danych, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi rozporządzenia oraz chronić prawa osób, których dane dotyczą. Zgodnie z drugą z ww. zasad, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Celem obu tych zasad jest uwzględnienie ochrony danych osobowych na jak najwcześniejszym etapie projektowania danej technologii – najlepiej już na etapie projektowania określonych rozwiązań.

RODO wprowadza także nieznane polskiemu porządkowi prawnemu tzw. **podejście oparte na ryzyku (ang. risk-based approach), w którym obowiązki w zakresie ochrony danych są zróżnicowane w zależności od ryzyka, jakie wynika z konkretnych operacji przetwarzania danych.** W uproszczeniu, polega ono na tym, że to administrator danych sam decyduje, jakie organizacyjne i techniczne środki powinien zastosować dla ochrony danych osobowych. Podejście to znacząco różni się od obecnego stanu prawnego. W Polsce dotychczas obowiązywało rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[11], które w sposób kazuistyczny wskazywało, jakie środki techniczne i organizacyjne, w jakiej sytuacji należy zastosować w zależności od konkretnych operacji przetwarzania danych. W szczególności uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadzało ono trzy poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym: (i) podstawowy; (ii) podwyższony; (iii) wysoki. W zależności od poziomu przewidywało ono różne środki bezpieczeństwa. Natomiast zgodnie z ogólnym rozporządzeniem jedynie w określonych przypadkach, administrator danych jest zobowiązany przeprowadzić ocenę skutków dla ochrony danych (art. 35 RODO). Zgodnie z tym podejściem, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych, wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę. Jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym (art. 36 RODO).

Istotnym elementem RODO **jest obowiązek wyznaczenia w określonych sytuacjach inspektora ochrony danych.** Przejmie on część funkcji wykonywanych dotychczas w polskim porządku prawnym przez administratorów bezpieczeństwa informacji (dalej: ABI). Zgodnie z art. 37 RODO, administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze, gdy:

a) przetwarzania dokonuje organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych.

Kolejną ważną nowością, którą wprowadza ogólne rozporządzenie jest **tzw. pseudonimizacja.** Zgodnie z art. 4 pkt 5 RODO, pseudonimizacja oznacza **przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji,** pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Dane osobowe poddane pseudonimizacji wciąż pozostają danymi osobowymi (inaczej niż ma to miejsce w przypadku anonimizacji).

Wreszcie, warto także wspomnieć o **obowiązku notyfikacji naruszenia ochro-**

[11] *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U.2004.100.1024.*

ny danych – tak organowi ochrony danych (art. 33 RODO), jak i osobie, której dotyczy naruszenie (art. 34 RODO). Takiemu obowiązkowi podlegali dotychczas w Polsce wyłącznie operatorzy telekomunikacyjni, RODO wprowadza je jednak w odniesieniu do wszystkich administratorów danych. Co do zasady, organ nadzorczy powinien zostać powiadomiony o takim naruszeniu w ciągu 72 godzin, natomiast, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Wreszcie, kluczowym elementem nowego reżimu prawnego są bardzo **wysokie kary administracyjne, które mają skutecznie zniechęcać do naruszeń przepisów o ochronie danych. Maksymalny pułap kar to 20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa.** W mojej ocenie, taka wysokość kar została ustalona z myślą o administratorach danych z USA, gdzie nie ma kompleksowej regulacji w obszarze ochrony danych osobowych czy prywatności. Przeważnie administratorzy, z których wielu przetwarza dane osobowe z terytorium Unii, dotychczas w przypadku konfliktu systemów prawnych bardziej obawiali się sankcji nakładanych przez organy amerykańskie, stąd tylko kwotami tego rzędu można było skłonić ich do działania.

Ogólne rozporządzenie jest dużym wyzwaniem dla administratorów danych, którzy muszą dostosować się do całkowicie nowej rzeczywistości prawnej. Jest to także nowe wyzwanie dla organów nadzorczych, które będą dysponować szerszymi niż dotychczas uprawnieniami i będą mogły je egzekwować także poza terytorium swojego państwa członkowskiego. Wyzwaniem będzie także zapewnienie jednolitego stosowania ogólnego rozporządzenia we wszystkich państwach członkowskich.

Podsumowując, **RODO znacząco wzmacnia pozycję podmiotu danych (użytkownika) w społeczeństwie informacyjnym, w szczególności poprzez przyznanie mu nowych uprawnień takich jak prawo do przenoszenia danych czy prawo do bycia zapomnianym.** Rozporządzenie przyczyni się także do budowy Jednolitego Rynku Cyfrowego poprzez uproszczenie otoczenia regulacyjnego – mniej biurokracji za cenę podejścia opartego na ryzyku, a także większą niż dotychczas harmonizację prawa w poszczególnych państwach członkowskich. Warto pamiętać, że wyższy poziom ochrony danych osobowych w Internecie to wyższe zaufanie obywateli do środowiska cyfrowego. Bez tego zaufania, co bardzo dobrze pokazuje np. sprawa Snowdena, obywatele w wielu sferach swojego życia mogą obawiać się korzystania z nowych technologii. Dlatego też RODO w ostatecznym rozrachunku należy oceniać pozytywnie.

Komentarz NASK

Projekt ustawy implementującej RODO został przyjęty przez Radę Ministrów 26 marca 2018 r[12]. Natomiast 30 marca 2018 r. do Komitetu ds. Europejskich zostały skierowane Przepisy wprowadzające ustawę o ochronie danych osobowych.

Zgodnie z treścią RODO, dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), zatem adres IP również jest zaliczany do danych osobowych, a to oznacza, że RODO ma bezpośredni wpływ na działalność zespołów typu CSIRT/CERT. Bardzo istotną jest, więc ocena czy zespół CSIRT/CERT jest administratorem danych osobowych czy pełni rolę podmiotu przetwarzającego te dane.

Zgodnie z treścią rozporządzenia mianem administratora określa się właściwy organ, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, natomiast podmiot przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Zatem zespół CSIRT/CERT jest administratorem w momencie, gdy przetwarza dane na podstawie otrzymanego mandatu. W przypadku, gdy zespół CSIRT/CERT działa w imieniu organów ścigania lub innych zespół CSIRT/CERT, (np. poprzez zapewnienie pomocy technicznej) wtedy pełni rolę podmiotu przetwarzającego, ponieważ nie decyduje bezpośrednio o celach i sposobach przetwarzania danych osobowych.

Także udostępnianie i wymianę informacji pomiędzy zespołami CSIRT można uznać za przetwarzanie danych osobowych.

Oznacza to, że w zakresie zgłaszania incydentów zespoły typu CSIRT podlegają dwóm reżimom: temu wprowadzonemu przez Dyrektywę NIS i temu właściwemu RODO. Poniższe tabele prezentują wymagania w zakresie notyfikacji incydentów dla obu aktów prawnych.

[12] *https://legislacja.rcl.gov.pl/projekt/12302950/katalog/12457690#12457690*

RODO

Rodzaj incydentu	Podmiot notyfikujący	Odbiorca zgłoszenia	Termin
Naruszenie danych osobowych	Podmiot przetwarzający	Administrator	Bez zbędnej zwłoki
Naruszenie danych osobowych	Administrator	Właściwy organ ochrony danych	Bez zbędnej zwłoki, w miarę możliwości do 72 godzin od momentu otrzymania zgłoszenia
Naruszenie danych osobowych z dużym ryzykiem zagrożenia dla praw i wolności osób fizycznych	Administrator	Osoby, których dane dotyczą	Bez zbędnej zwłoki

Dyrektywa NIS

Rodzaj incydentu	Podmiot notyfikujący	Odbiorca zgłoszenia	Termin
Incydent mający znaczny wpływ na ciągłość usług kluczowych	Operatorzy usług kluczowych	Właściwy organ ochrony danych lub zespół CSIRT	Bez zbędnej zwłoki
Incydent mający znaczny wpływ na świadczenie usługi	Dostawcy usług cyfrowych	Właściwy organ ochrony danych lub zespół CSIRT	Bez zbędnej zwłoki

W związku z tym warto zadbać o właściwe przygotowanie nie tylko w zakresie implementacji Dyrektyw NIS, ale i RODO, oraz dokonać dokładnej oceny zakresu, w jakim zespół CSIRT może dokonywać przetwarzania danych osobnych w obrębie własnego constituency, a także czy jest procesorem (przetwarza dane osobowe), czy administratorem. Konieczne jest także dokumentowanie sposobu zbierania, przechowywania i przetwarzania danych osobowych, dokładnej analizy okresu i zasad przechowywania danych roboczych, anonimizacji danych osobowych, gdzie istnieje konieczność uzyskania zgody osoby, której te dane dotyczą. Natomiast w czasie procesu przekazywania danych konieczna będzie ocena nie tylko constituency swojego zespołu CSIRT, ale także CSIRT, któremu dane te mają być przekazywane.

Magdalena Wrzosek

Nowy Pakiet Cyberbezpieczeństwa dla UE

Magdalena Wrzosek – *Ekspert ds. policy w NC Cyber w NASK, gdzie odpowiada za kwestie strategiczne regulacyjne i organizacyjne związane z cyberbezpieczeństwem. Twórca projektu CyberPolicy (https://cyberpolicy.nask.pl). W 2017 roku koordynowała europejski projekt Cooperative Models for Public Private Partnership (PPPs) and Information Sharing and Analysis Centers (ISACs). Brała także udział w pracach międzyresortowego zespołu odpowiedzialnego za przygotowanie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.*

Od stycznia 2018 Oficer Łącznikowy Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA).

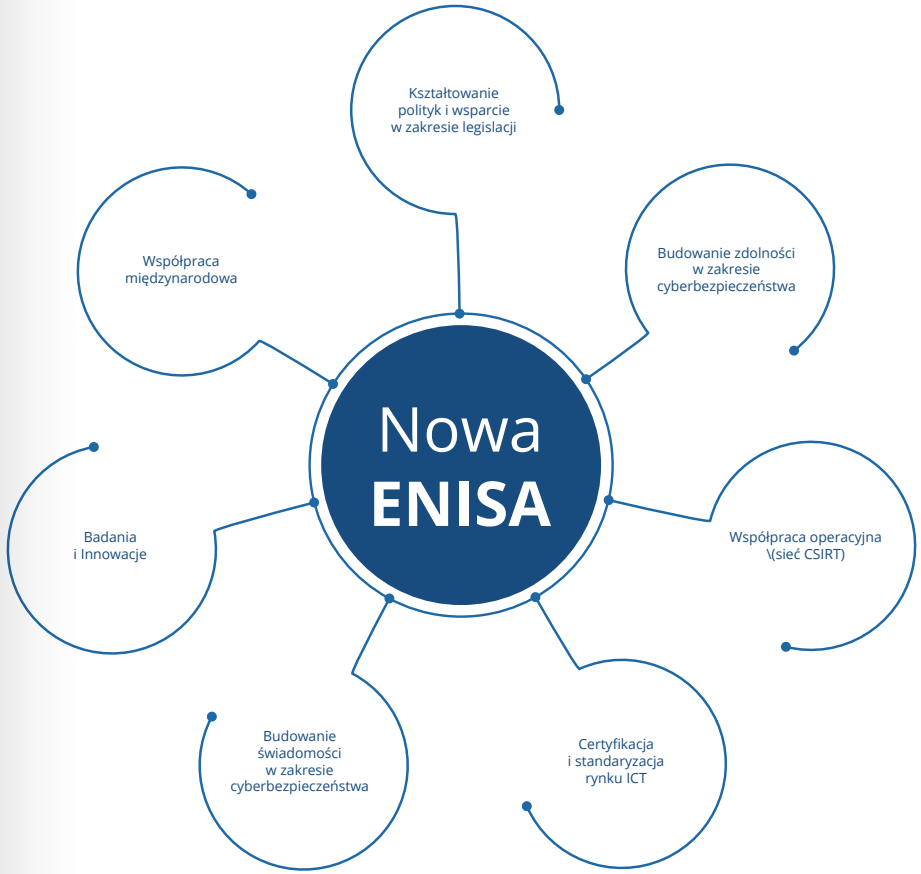
W latach 2014 – 2016 pracowała w Ministerstwie Cyfryzacji, gdzie odpowiadała m.in. za negocjacje Dyrektywy NIS, planowanie i koordynację europejskich ćwiczeń cybernetycznych Cyber Europe (edycja 2014, 2016), współpracę międzynarodową oraz implementację zapisów Polityki Ochrony Cyberprzestrzeni RP.

Politolog, kulturoznawca, absolwentka Uniwersytetu Warszawskiego i Uniwersytetu w Konstancji w Niemczech. Ukończyła studia podyplomowe z zarządzania projektami, zarządzania bezpieczeństwem informacji, prawa międzynarodowego i służby zagranicznej. Ukończyła także Europejskie

Centrum Studiów nad Bezpieczeństwem im. Greorgea' a Marshall'a w Garmisch – Partenkirchen (Program on Cyber Security Studies (PCSS) oraz Seminar on Regional Security (SRS)). W 2016 roku brała udział w programie „International Visitor Leadership Program" poświęconemu cyberbezpieczeństwu, organizowanego przez Departament Stanu USA. Doktorantka Akademii Sztuki Wojennej w Warszawie, gdzie wykłada zarządzanie kryzysowe i bezpieczeństwo publiczne.

13 września 2017 roku Komisja Europejska zaprezentowała długo zapowiadany pakiet cyberbezpieczeństwa – *cybersecurity package*. Wiele z tych inicjatyw zostało zapowiedzianych już w lipcu 2016 roku w Komunikacie KE **Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego[13].** W skład pakietu weszły propozycje legislacyjne związane z odnowieniem mandatu Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz europejskimi ramami certyfikacji, Komunikat **Odporność, prewencja i obrona: Budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej,** który jest aktualizacją Strategii Cyberbezpieczeństwa UE z 2013 roku[14], a także tzw. **Blueprint**, czyli zalecenia w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę oraz Komunikat mający za zadanie wspierać implementację Dyrektywy NIS w krajach członkowskich (Komunikat „Making the most of NIS"). „Pakiet" jest komplementarny w stosunku do tzw. Dyrektyw NIS, której czas implementacji do porządków prawnych państw członkowskich upływa 8 maja b.r. Przedstawione przez Komisję inicjatywy stanowią kolejny krok w procesie budowania bezpiecznego Jednolitego Rynku Cyfrowego.

Najważniejsza część pakietu to propozycja legislacyjna **Cybersecurity act**, w której połączono dwie kwestie: mandat ENISA i certyfikację. Pierwsza część dokumentu dotyczy regulacji Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA)[15], której nazwa została skrócona do „Europejskiej Agencji ds. Cyberbezpieczeństwa" (EU Cybersecurity Agency). ENISA to unijna agencja, stanowiąca ośrodek specjalistycznej wiedzy w zakresie bezpieczeństwa cybernetycznego w Europie, który pomaga Unii Europejskiej i należącym do niej krajom zapobiegać problemom, dotyczącym bezpieczeństwa ICT. Agencja została powołana w 2004 (Regulacja EC no 460/2004[16]). ENISA otrzymała wtedy mandat na 5 lat, ale był on przedłużany dwukrotnie w 2009 i 2011 roku. W 2013 roku Parlament Europejski przyjął nową regulacje 526/2013[17], która zastąpiła tę z 2004 roku i stanowi obecnie prawne podstawy działania Agencji. Mandat ENISA wygasa w czerwcu 2020 roku. Nowa propozycja zakłada przyznanie Agencji permanentnego statusu. KE argumentuje, że jest to związane ze wzrastającymi zagrożeniami i coraz istotniejszą rolą ICT oraz nowymi obowiązkami ENISA nałożonymi przez Dyrektywę NIS[18]. Poza tym Agencja ma zostać wyposażona w nowe kompetencje i wzmocniona poprzez zwiększenie zatrudnienia i dodatkowe fundusze. KE proponuje, aby ENISA stała się ośrodkiem wspierającym budowanie cyberbezpieczeństwa w UE poprzez promowanie europejskiej certyfikacji oraz wsparcie w jej tworzeniu. Dodatkowo Agencja ma wspierać instytucje unijne w przygotowaniu i implementacji właściwych polityk, asystować krajom członkowskim w budowaniu zdolności w zakresie cyberbezpieczeństwa, a także budować świadomość na temat zagrożeń i promować współpracę i koordynację działań w zakresie cyberbezpieczeństwa na poziomie europejskim. Poniższy schemat przedstawia obszary, w których ma działać ENISA, zgodnie z projektem zaproponowanym przez KE.



[13] http://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A52016DC0410

[14] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52013JC0001

[15] https://www.enisa.europa.eu/

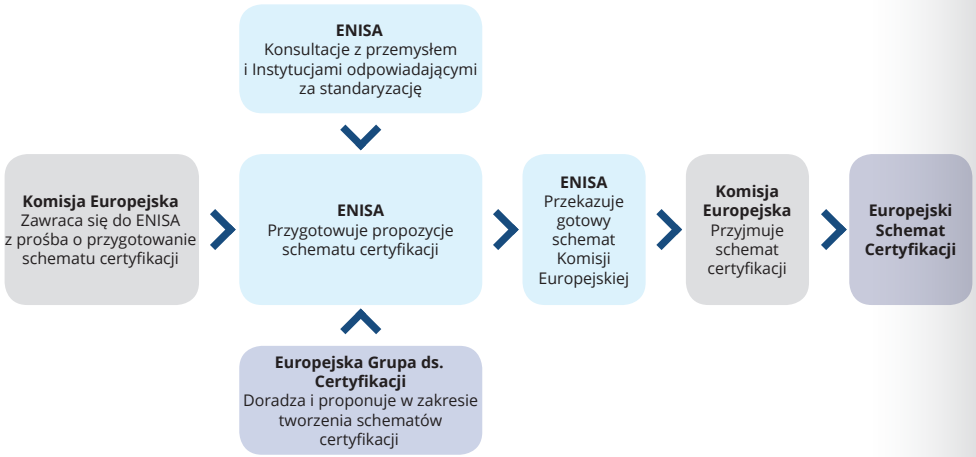
[16] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[17] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN

[18] zgodnie z zapisami tzw. Dyrektyw NIS (https://cyberpolicy.nask.pl/cp/ramy-prawne/dyrektywa-nis/24,Dyrektywa-Parlamentu-Europejskiego-i-Rady-UE-20161148-z-dnia-6-lipca-2016-r-w-sp.html), ENISA pełni rolę sekretariatu sieci CSIRT (https://cyberpolicy.nask.pl/cp/inicjatywy-zagraniczne/unia-europejska/csirt-network/71,Siec-CSIRT-CSIRT-network.html)

O ile kwestie dotyczące permanentnego mandatu nie są przedmiotem kontrowersji, o tyle jego zakres już tak. Chodzi zwłaszcza o tak zwane kwestie „współpracy operacyjnej" i obawy niektórych państw, że taki zapis może powodować pewnego rodzaju nadzór Agencji nad CSIRT poziomu krajowego, a tym samym zbytnie ingerowanie w kwestie wewnętrzne państw członkowskich.

Druga część Cybersecurity act to propozycja europejskich ram certyfikacji ICT. Komisja zakłada, że certyfikacja będzie wspierać budowanie zaufania w ramach usług na Jednolitym Rynku Cyfrowym[19]. Funkcjonujące obecnie mechanizmy certyfikacji na poziomie narodowym (np. we Francji, Wielkiej Brytanii, czy w Niemczech) powodują konieczność wzajemnego uznawania, a mechanizmy takie jak SOG-IS[20] nie obejmują wszystkich państw członkowskich[21]. Propozycja KE zakłada dobrowolną strukturę certyfikacji, w ramach której państwa UE będą mogły tworzyć własne schematy certyfikacji dla produktów i usług ICT, które byłyby uznawane w całej UE. Zakładane jest także powołanie Europejskiej Grupy ds. Certyfikacji, która doradzałaby ENISA w zakresie certyfikacji oraz proponowała KE schematy certyfikacji. Na tej podstawie ENISA przygotowywałaby schematy certyfikacji, które następnie przyjmowane będą przez KE, stając się powszechnie obowiązującymi. W efekcie powstałby mechanizm, w którym to Komisja, jako instytucja, która proponuje schematy certyfikacji i decyduje o ich zatwierdzeniu, odgrywałaby najważniejszą role, podczas kiedy Grupa ds. Certyfikacji (składająca się z przedstawicieli Państw Członkowskich) mogłaby tylko doradzać i proponować schematy, które w całości byłyby wypracowywane przez ENISA. Poniższy schemat przedstawia strukturę proponowanej certyfikacji:



[19] *https://cyberpolicy.nask.pl/cp/dokumenty-strategiczne/strategia-jednolitego-r/39,Strategia-Jednolitego-Rynku-Cyfrowego-dla-Europy-A-Digital-Single-Market-Strateg.html*

[20] *https://www.sogis.org/*

[21] *członkami SOG-IS jest 12 państw*

Obecnie na forum Rady trwają negocjacje Cybersecurity Act. Ze strony Polski proces negocjacji prowadzi Ministerstwo Cyfryzacji.

Ważnym elementem „Pakietu cybernetycznego" jest także aktualizacja Strategii Cyberbezpieczeństwa UE[22] przedstawiona, jako Komunikat Odporność, prewencja i obrona: Budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej. Komisja zapowiedziała wzmocnienie zdolności w zakresie technologii i umiejętności w dziedzinie cyberbezpieczeństwa, a także budowanie silnego Jednolitego Rynku Cyfrowego w ramach trzech filarów:

- Budowania odporności UE na ataki cybernetyczne,
- Kształtowania skutecznej prewencji cybernetycznej na poziomie UE
- Wzmocnienie współpracy międzynarodowej w zakresie bezpieczeństwa cybernetycznego[23].

Pewnego rodzaju nowością w kwestiach strategicznych jest zbliżenie bezpieczeństwa cywilnego z cyberbezpieczeństwem sfery wojskowej, np. poprzez postulaty wspólnych ćwiczeń. Do tej pory *Europejska Strategia Cyberbezpieczeństwa* miała typowo cywilny wydźwięk i nie poruszała kwestii związanych ze sferą militarną.

Bardzo interesującym elementem Pakietu jest tzw. Blueprint, czyli propozycja dotycząca zarządzania kryzysowego w obliczu incydentów cybernetycznych na dużą skalę. Dokument ma za zdanie zaprojektować schematy reagowania na kryzysy cybernetyczne w Europie w taki sposób, by odpowiedź państw członkowskich była jak najbardziej adekwatna i szybka. Dodatkowo Blueprint zakłada powiązanie kwestii cyberbezpieczeństwa z konwencjonalnymi mechanizmami zarządzania kryzysowego. Dokument został skonstruowany w oparciu o cztery zasady przewodnie:

- PROPORCJONALNOŚĆ – oznacza, że większość ataków nie spełnia kryteriów ani kryzysu na szczeblu krajowym, ani międzynarodowym, a co za tym idzie: podstawę współpracy państw członkowskich stanowić będzie sieć CSIRT;
- POMOCNICZOŚĆ – oznacza, że główna odpowiedzialność za reagowanie na kryzysy cybernetyczne leży po stronie państw członkowskich, a organy UE (m.in. Komisja, Europejska Służba Działań Zewnętrznych) tylko je w tym wspierają, w myśl uzgodnionych wcześniej procedur i obowiązujących przepisów prawa;
- KOMPLEMENTARNOŚĆ – oznacza, że Blueprint jest komplementarny w stosunku do funkcjonujących już procedur UE (m.in. zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych – IPCR, mechanizm

[22] *https://cyberpolicy.nask.pl/cp/dokumenty-strategiczne/strategia-cyberbezpiecz/22,Strategia-bezpieczenstwa-cybernetycznego-Unii-Europejskiej-otwarta-bezpieczna-i-.html*

[23] *więcej informacji na ten temat na stronie: https://cyberpolicy.nask.pl/cp/dokumenty-strategiczne/strategia-cyberbezpiecz/23,Komunikat-KE-Odpornosc-prewencja-i-obrona-Budowa-solidnego-bezpieczenstwa-cybern.html*

reagowania kryzysowego ESDZ);

- POUFNOŚĆ INFORMACJI – oznacza, że wszelka wymiana informacji w ramach opisanych w dokumencie procedur musi być zgodna z obowiązującymi zasadami bezpieczeństwa.

Blueprint ma umożliwić państwom członkowskim nie tylko skuteczne reagowanie na cyberzagrożenia, ale także uzyskanie wspólnej orientacji sytuacyjnej oraz zapewnić mechanizm wypracowywania zgody w kwestii kluczowych działań komunikacyjnych na wypadek kryzysu. Wszystkie te elementy muszą być zapewnione na trzech poziomach współpracy: technicznym, operacyjnym oraz polityczno-strategicznym.

1. Poziom techniczny

Dotyczy postępowania w odniesieniu do incydentu (procedury umożliwiające wykrywanie i analizowanie incydentu, ograniczenie jego skutków oraz reakcję) oraz monitorowania incydentu i nadzoru (łącznie z analizą zagrożeń i ryzyka). Centralnym mechanizmem współpracy jest sieć CSIRT.

2. Poziom operacyjny

Dotyczy przygotowania procesu decyzyjnego na poziomie politycznym, koordynacji zarządzania kryzysem cybernetycznym oraz oceny skutków i wpływu na szczeblu unijnym (w tym zaproponowanie możliwych środków zaradczych).

3. Poziom strategiczno-polityczny

Dotyczy strategicznego i politycznego zarządzania cybernetycznymi i poza cybernetycznymi aspektami kryzysu (z uwzględnieniem środków unijnej reakcji dyplomatycznej).

Poniższa tabela przedstawia mechanizmy reakcji Państw członkowskich na wszystkich poziomach

Poziom reagowania	Opis	Mechanizm współpracy	Zaangażowane podmioty
Poziom techniczny	Postępowanie w odniesieniu do incydentu (procedury umożliwiające wykrywanie i analizowanie incydentu, ograniczenie jego skutków oraz reakcje). Monitorowania incydentu i nadzoru (łącznie z analizą zagrożeń i ryzyka).	Sieć CSIRT	Państwa członkowskie: • właściwe organy i pojedyncze punkty kontaktowe powołane zgodnie z dyrektywą w sprawie bezpieczeństwa sieci i systemów informatycznych; • zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) Organy/urzędy/agencje UE: ENISA, • Europol/EC3, • CERT-UE; • Komisja Europejska: • Centrum Koordynacji Reagowania Kryzysowego (ERCC: działająca nieprzerwanie służba operacyjna zlokalizowana w DG ECHO) oraz wyznaczona • służba odpowiedzialna (do wyboru między DG CNECT i DG HOME w zależności od charakteru danego incydentu), Sekretariat Generalny (ARGUS), DG HR (dyrekcja ds. bezpieczeństwa), DG DIGIT (operacje w zakresie bezpieczeństwa IT); • w przypadku innych agencji UE odpowiednia macierzysta DG w Komisji lub ESDZ (pierwszy punkt kontaktowy). ESDZ: • SIAC (pojedyncza komórka analiz wywiadowczych: EU INTCEN i EUMS INT); • Centrum Sytuacyjne UE i wskazana służba właściwa pod względem geograficznym lub tematycznym; • komórka UE ds. syntezy informacji o zagrożeniach hybrydowych (część Centrum Analiz Wywiadowczych UE (INTCEN) – bezpieczeństwo cybernetyczne w kontekście hybrydowym).
Poziom operacyjny	Przygotowanie procesu decyzyjnego na poziomie politycznym. Koordynacja zarządzania kryzysem cybernetycznym (w razie potrzeby). Ocena skutków i wpływu na szczeblu unijnym i zaproponowanie możliwych środków zaradczych.		Państwa członkowskie: • Właściwe organy i pojedyncze punkty kontaktowe powołane zgodnie z dyrektywą w sprawie bezpieczeństwa sieci i informacji. • CSIRT, agencje ds. bezpieczeństwa cybernetycznego. • Inne krajowe organy sektorowe (w przypadku incydentu lub kryzysu o zasięgu ponadsektorowym). Organy/urzędy/agencje UE: • ENISA • Europol/EC3 • CERT-UE • Komisja Europejska • Sekretarz Generalny SG lub jego zastępca (procedura ARGUS) DG CNECT/HOME: • Organ Komisji ds. bezpieczeństwa. • Inne DG (w przypadku incydentu lub kryzysu o zasięgu ponadsektorowym). ESDZ: • Sekretarz Generalny ds. reagowania kryzysowego lub jego zastępca i SIAC (EU INTCEN i EUMS INT). • Komórka UE ds. syntezy informacji o zagrożeniach hybrydowych. Rada: Prezydencja (przewodniczący Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni lub COREPERU19) wspierana przez Sekretariat Generalny Rady lub Komitet Polityczny i Bezpieczeństwa (KPiB)20 oraz przy wsparciu ustaleń w ramach IPCR – jeżeli zostały aktywowane.
Poziom strategiczno – polityczny	Strategiczne i polityczne zarządzanie zarówno cybernetycznymi, jak i pozacybernetycznymi aspektami kryzysu z uwzględnieniem środków zgodnie z ramami wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne.		W imieniu państw członkowskich: ministrowie odpowiedzialni za bezpieczeństwo cybernetyczne. W imieniu Rady Europejskiej: Przewodniczący. W imieniu Rady: rotacyjna prezydencja. W przypadku zastosowania środków w ramach „zestawu narzędzi dla dyplomacji cyfrowej": KPiB i Horyzontalna Grupa Robocza. W imieniu Komisji Europejskiej: Przewodniczący lub oddelegowany wiceprzewodniczący Komisji/komisarz. Wysoki Przedstawiciel Unii ds. Zagranicznych i Polityki Bezpieczeństwa / wiceprzewodniczący Komisji.

Komunikat **Making the most of NIS**[24] został zaprojektowany, jako wsparcie państw członkowskich w implementacji Dyrektywy NIS. Komunikatowi towarzyszy szczegółowy aneks, który zawiera m.in. przykłady dobrych praktyk z krajów członkowskich, związane ze strategią cyberbezpieczeństwa, informacje na temat wyznaczania Organów właściwych, operatorów usług kluczowych i dostawców usług cyfrowych oraz analizę powiązań pomiędzy Dyrektywą NIS, a innymi aktami legislacyjnymi (przede wszystkim akty prawa sektorowego dla sektora finansowego, który został zidentyfikowany, jako lex specialis).

Bardzo ciekawym elementem „Pakietu cybernetycznego" jest także zapowiedź utworzenia Cybersecurity Emergency Response Fund. Ma być to fundusz wspierający państwa członkowskie w czasie kryzysu cybernetycznego. Z funduszu tego mają korzystać państwa, które spełnią konkretne wymagania, np. będą miały opracowaną strategie cyberbezpieczeństwa i będą odpowiednio zarządzać kryzysem cybernetycznym w skali kraju.

„Pakiet" to dość kompleksowa i interesująca propozycja KE, która wyraźnie pokazuje, że implementacja Dyrektywy NIS to dopiero początek działań zmierzających do podniesienia poziomu cyberbezpieczeństwa w Europie. Warto zaznaczyć, że dla KE tematyka cyberbezpieczeństwa jest związana nie tylko z bezpieczeństwem narodowym, ale także z rozwojem gospodarczym – budowa Jednolitego Rynku Cyfrowego w taki sposób, aby obywatele mieli zaufanie do świadczonych na nim usług.

[24] *https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52017DC0476*

Flash z Komisji Europejskiej

Michał Czerniawski, Justyna Romanowska

Stałe Przedstawicielstwo przy Unii Europejskiej w Brukseli

Komentarz NASK:

Od stycznia Prezydencję w Radzie UE sprawuje Bułgaria, która jako jeden z priorytetów zdefiniowała Gospodarkę Cyfrową[25]. Tematy takie jak Jednolity Rynek Cyfrowy[26] oraz dostęp do innowacji były także priorytetowo traktowane przez Prezydencję Estonii (czerwiec – grudzień 2017) oraz będą kontynuowane w czasie Prezydencji Austrii (czerwiec – grudzień 2018).

Rozporządzenie o e-prywatności i Cybersecurity act

Wciąż toczą się intensywne prace nad dwoma projektami legislacyjnymi: rozporządzeniem o e-prywatności oraz aktem ws. cyberbezpieczeństwa. Przyspieszeniu prac nad tym pierwszym nie sprzyja zbliżające się rozpoczęcie stosowania RODO (ogólne rozporządzenie o ochronie danych), które absorbuje większość państw członkowskich, oraz wątpliwości, co do możliwości praktycznego zastosowania niektórych z propozycji Komisji, np. wyrażania zgody przez ustawienia przeglądarki. Jeśli chodzi o akt ws. cyberbezpieczeństwa, to podczas negocjacji wyraźnie uwidocznił się zróżnicowany stan zaawansowania w tym obszarze poszczególnych państw członkowskich, co w wielu przypadkach przekłada się na rozbieżne interesy, tak w obszarze certyfikacji, jak i roli ENISA. Na chwilę obecną wydaje się, że obecnej Prezydencji Bułgarskiej nie uda się sfinalizować prac nad żadną z powyższych inicjatyw legislacyjnych.

Reforma sektora telekomunikacji – Europejski Kodeks Łączności Elektronicznej

Prace nad tym dokumentem są bardzo zaawansowane. Prezydencja bułgarska ma realne szanse na zakończenie ich w tym półroczu oraz ogłoszenie sukcesu podczas czerwcowej Rady ds. telekomunikacji w Brukseli (8.06). Dotychczas odbyło się 5 intensywnych trilogów[27] z Parlamentem Europejskim. Kolejne trilogi planowane są na koniec kwietnia (25.04) oraz początek czerwca. Prezydencji bułgarskiej udało się wstępnie zamknąć negocjacje nad rozdziałem dotyczącym widma radiowego, istotne rozbieżności między Radą UE a Parlamentem utrzymują się nadal w kwestiach dostępu telekomunikacyjnego, usług łączności elektronicznej oraz praw użytkowników końcowych.

Komentarz NASK:

Dyrektywa NIS[28] nie obejmuje sektora telekomunikacyjnego, który został włączony do Krajowego Systemu Cyberbezpieczeństwa w projekcie ustawy o KSC. W związku z tym reforma prawa telekomunikacyjnego jest bardzo istotną kwestią[29]. Zapisy dotyczące bezpieczeństwa sieci, a więc art. 40 i 41 oraz motywy 90 – 92 także nie zostały jeszcze uzgodnione.

Z nadchodzących wydarzeń warto wspomnieć o zaplanowanym na 10 kwietnia Digital Day 2 w Brukseli (udział tylko na zaproszenie KE, kontakt do organizatorów CNECT-DIGITAL-DAY-2018@ec.europa.eu) oraz Digital Assembly 25-16 czerwca 2018 w Sofii (kontakt do organizatorów pod adresem e-mail: CNECT-DA-2018-SOFIA@ec.europa.eu)

[25] *https://eu2018bg.bg/en/priorities*

[26] *https://cyberpolicy.nask.pl/cp/dokumenty-strategiczne/strategia-jednolitego-r/39,Strategia-Jednolitego-Rynku-Cyfrowego-dla-Europy-A-Digital-Single-Market-Strateg.html*

[27] *negocjacje pomiędzy Komisją Europejską, Radą oraz Parlamentem Europejskim*

[28] *https://cyberpolicy.nask.pl/cp/ramy-prawne/dyrektywa-nis/24,Dyrektywa-Parlamentu-Europejskiego-i-Rady-UE-20161148-z-dnia-6-lipca-2016-r-w-sp.html*

[29] *https://cyberpolicy.nask.pl/cp/ramy-prawne/europejski-kodeks-laczn/72,Europejski-Kodeks-Lacznosci-Elektronicznej.html*

CYBERPOLICY

NASK

cyberpolicy.nask.pl