UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Jacek Jastrzębski
Przewodniczący
Komisji Nadzoru Finansowego

DCO-DCOZDO.0126.2.2020

Warszawa, 22 stycznia 2020 r.

Pan
Jan Nowak
Prezes Urzędu
Ochrony Danych Osobowych

Szanowny Panie Prezesie,

W nawiązaniu do wystąpienia Pana Prezesa z dnia 4 listopada 2019 r., (sygn. ZSPR.027.431.2019 , które wpłynęło do Urzędu Komisji Nadzoru Finansowego, zwanego dalej „UKNF", w dniu 15 listopada 2019 r.), dotyczącego sprzedaży przez pracowników podmiotów rynku finansowego, podlegających nadzorowi Komisji Nadzoru Finansowego, zwanej dalej „KNF" lub „organ nadzoru", baz danych klientów zawierających dane osobowe, uprzejmie informuję, że w zakresie kompetencji określonych w ustawie z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. z 2019 r., poz. 298 z późn. zm.) zwanej dalej NadzRFinU, KNF od lat podejmuje działania oraz prowadzi inicjatywy mające na celu zapewnienie bezpieczeństwa informacji przetwarzanych przez podmioty nadzorowane.

KNF jest powołana do realizacji celów nadzorczych, czyli innymi słowy wartości mających charakter uniwersalny jak również partykularny. W art. 2 NadzRFinU do celów uniwersalnych (wspólnych dla całego rynku finansowego) zalicza się: prawidłowe funkcjonowanie tego rynku, jego stabilność, bezpieczeństwo oraz przejrzystość i zaufanie do rynku finansowego, natomiast cele partykularne (szczegółowe, przede wszystkim sektorowe - z wyjątkiem celu dotyczącego nadzoru uzupełniającego) zostają wskazane poprzez odesłania do odpowiednich ustaw odrębnych. Ustawodawca wskazał ponadto łącznik pomiędzy celami uniwersalnymi a szczegółowymi, stwierdzając, że te pierwsze są realizowane „przez realizację celów określonych w szczególności" w rzeczonych ustawach odrębnych. Cele z ustaw odrębnych stanowią zatem kwantyfikator dla celów wskazanych bezpośrednio w NadzRFinU, pozwalając organowi nadzoru na dostosowanie zakresu i metod ingerencji nadzorczej w poszczególnych sektorach do bieżących potrzeb przy jednoczesnym zachowaniu ogólnego

Piękna 20 · skrytka pocztowa nr 419 · 00-549 Warszawa · tel. +48 22 262 50 00 · fax +48 22 262 51 11 · www.knf.gov.pl

kierunku działań KNF[1]. W swoich działaniach organ nadzoru uwzględnia więc wszelkie przekazywane sygnały, mogące wpływać na bezpieczeństwo nadzorowanych sektorów. Dotyczy to w szczególności ochrony właściwych dla poszczególnych sektorów tajemnic (w ,których katalogu mieszczą się również dane osobowe), realizowanych przez podmioty nadzorowane na podstawie powszechnie obowiązujących regulacji prawnych w kontekście zindywidualizowanego ryzyka.

Przedstawiony przez Pana Prezesa problem dotyczy kwestii związanych z szeroko pojętymi zagadnieniami bezpieczeństwa informacji i obejmuje zarówno aspekty organizacyjne, jak i technologiczne. W tym kontekście, odnosząc się do działań KNF należy zwrócić szczególną uwagę na publikowane przez organ nadzoru rekomendacje, wytyczne, stanowiska i komunikaty dla rynku finansowego – zamieszczane i dostępne na stronie internetowej KNF, określone m.in. w:

1. Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach – określającej zasady dobrej praktyki w zakresie ostrożnego i stabilnego zarzadzania ryzykiem operacyjnym w bankach, w szczególności w odniesieniu do jego identyfikacji, oceny, przeciwdziałania, kontroli, monitorowania i raportowania.
2. Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach oraz wytycznych dla pozostałych sektorów rynku finansowego.
3. Komunikacie UKNF z dnia 23 października 2017 r. dotyczącym korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej.
4. Stanowisku przekazanym pismem z dnia grudnia 2016 r. (sygn.) zalecającym podmiotom nadzorowanym monitorowanie serwisów ogłoszeniowych celem wykrywania m. in procederu sprzedaży rachunków oraz praktyk zakładania rachunków imiennych, a następnie ich nieuprawnionej sprzedaży osobom trzecim (zmiana numeru telefonu w bankowości internetowej, w kontekście wykrywania procederu sprzedaży rachunków).

[1] „Ustawa o nadzorze nad rynkiem finansowym. Komentarz." pod red. prof. dr hab. Marka Wierzbowskiego, dr Ludwika Sobolewskiego, dr hab. Pawła Wajdy, 2018

Należy podkreślić, że zgodnie z powszechnie panującą opinią, ww. rekomendacje i wytyczne wydane przez KNF w zakresie bezpieczeństwa informacji uznawane są – nie tylko przez rynek finansowy, ale również przez innych uczestników obrotu gospodarczego – za kompleksowe i uniwersalne, stanowiąc swoistego rodzaju standard w zakresie zapewnienia bezpieczeństwa informacji przetwarzanych w organizacjach.

Organ nadzoru na bieżąco kontroluje i monitoruje podmioty sektora finansowego w zakresie ryzyka związanego z bezpieczeństwem informacji, m.in. poprzez badanie stopnia dostosowania tych podmiotów do standardów określonych we wskazanych powyżej rekomendacjach, wytycznych i komunikatach, w tym:

1. w zakresie aspektów organizacyjnych, m.in. poprzez wdrożenie odpowiedniej polityki bezpieczeństwa informacji, struktury organizacyjnej, wprowadzenie procedur identyfikacji, szacowania, kontroli, przeciwdziałania, monitorowania i raportowania ryzyka bezpieczeństwa informacji, wewnętrznej polityki szkoleniowej banku, procedur bezpiecznego korzystania z komputerów i urządzeń przenośnych przez pracowników banku, zakresu i jakości badań audytu wewnętrznego oraz ew. zewnętrznego,
2. w zakresie aspektów technologicznych, m.in. kontrolowanie i monitorowanie nieuprawnionych działań zewnętrznych i wewnętrznych naruszających bezpieczeństwo systemów informatycznych, a także sposób kontroli przez bank ryzyka związanego z wykorzystywaniem przez pracowników urządzeń prywatnych do celów służbowych.

W przypadku zidentyfikowania, w wyniku przeprowadzonych czynności kontrolnych, nieprawidłowości w tych obszarach, do podmiotu kierowane są zalecenia KNF ze wskazaniem terminu ich wdrożenia. Kolejne etapy realizacji harmonogramu wdrożenia zaleceń są raportowane do KNF, a końcowy stan wdrożenia zaleceń co do zasady weryfikowany jest podczas procesu inspekcyjnego.

W zakresie monitorowania stanu bezpieczeństwa przetwarzania danych w systemach informacyjnych, organ nadzoru monitoruje podmioty nadzorowane poprzez pozyskiwanie od nich informacji dotyczących m.in.:

1. liczby zidentyfikowanych podatności krytycznych, które nie zostały usunięte:

a) w sektorze banków komercyjnych, dla poszczególnych kwartałów, zidentyfikowano następującą liczbę podatności krytycznych, które nie zostały usunięte: na koniec I kwartału 2019 r. – (średnia liczba nieusuniętych podatności przypadająca na bank – , na koniec II kwartału 2019 r. – , na koniec III kwartału 2019 r. – . Dla każdego z kwartałów 6 banków wykazało, że nie posiada podatności krytycznych, które byłyby nieusunięte,

b) w sektorze banków spółdzielczych, dla poszczególnych kwartałów, zidentyfikowano następującą liczbę podatności krytycznych, które nie zostały usunięte: na koniec I kwartału 2019 r. – (średnia liczba nieusuniętych podatności przypadająca na bank –), na koniec II kwartału 2019 r. – (średnia –), na koniec III kwartału 2019 r. – (średnia –);

2. efektywności usuwania podatności krytycznych:

a) w sektorze banków komercyjnych, dla poszczególnych kwartałów, występowała następująca liczba podatności krytycznych, dla których czas ich usunięcia przekroczył 50 dni od momentu zidentyfikowania: na koniec I kwartału 2019 r. – (średnia liczba podatności przypadająca na bank – na koniec II kwartału 2019 r. – (średnia –), na koniec III kwartału 2019 r. – (średnia –),

b) w sektorze banków spółdzielczych, dla poszczególnych kwartałów, występowała następująca liczba podatności krytycznych, dla których czas ich usunięcia przekroczył 50 dni od momentu zidentyfikowania: na koniec I kwartału 2019 r. (średnia liczba podatności przypadająca na bank –), na koniec II kwartału 2019 r. – (średnia –), na koniec III kwartału 2019 r. – (średnia –);

3. liczby incydentów bezpieczeństwa środowiska teleinformatycznego:

a) w sektorze banków komercyjnych, dla poszczególnych kwartałów, występowała następująca liczba incydentów bezpieczeństwa środowiska teleinformatycznego: na koniec I kwartału 2019 r. – (średnia liczba

incydentów przypadająca na bank , na koniec II kwartału 2019 r. – (średnia –), na koniec III kwartału 2019 r. – (średnia –);

b) w sektorze banków spółdzielczych, dla poszczególnych kwartałów, występowała następująca liczba incydentów bezpieczeństwa środowiska teleinformatycznego: na koniec I kwartału 2019 r. – (średnia liczba incydentów przypadająca na bank –), na koniec II kwartału 2019 r. – (średnia –), na koniec III kwartału 2019 r. – (średnia –);

4. liczby incydentów bezpieczeństwa o najwyższym poziomie krytyczności:

a) w sektorze banków komercyjnych, dla poszczególnych kwartałów, występowała następująca liczba incydentów krytycznych: na koniec I kwartału2019 r. – (średnia liczba incydentów krytycznych przypadająca na bank -), na koniec II kwartału 2019 r. – (średnia –), na koniec III kwartału 2019 r. – (średnia –),

b) w sektorze banków spółdzielczych, dla poszczególnych kwartałów, występowała następująca liczba incydentów krytycznych: na koniec I kwartału 2019r. – (średnia liczba incydentów krytycznych przypadająca na bank -), na koniec II kwartału 2019 r. – (średnia – , na koniec III kwartału 2019 r. – (średnia –).

Banki, realizując rekomendacje i wytyczne KNF, proaktywnie chronią wszystkie swoje zasoby informacyjne, implementując w tym celu szereg rozwiązań proceduralnych, do których zaliczyć można zasadę need to know, zarządzanie uprawnieniami, dezaktywację kont informatycznych, procedury bezpiecznego rozwiązywania umowy, szereg innych procedur mających na celu zapewnienie bezpieczeństwa informacji, wynikających z rekomendacji D i M. Oprócz powyższych, banki stosują rozwiązania wspomagające proces zapewnienia bezpieczeństwa informacji, poprzez np. wykupienie usług i aktywne monitorowanie Internetu i Darknetu pod kątem wykrywania wycieku danych, w tym danych osobowych, jak również stosując wewnętrzne procedury w zakresie wykrywania tego typu incydentówa w przypadku ich wykrycia – współpracę z organami ścigania, prokuraturą oraz Związkiem Banków Polskich.

Podmioty sektora finansowego konsekwentnie budują również świadomość pracowników oraz wzmacniają kulturę organizacyjną w zakresie ryzyka, poprzez m.in. szkolenia z zakresu bezpieczeństwa informacji i ochrony danych osobowych.

Oczywistym jest również stosowanie nowoczesnych technologii oraz systemów dedykowanych do ochrony przetwarzanych informacji, takich jak systemy oraz ich aktywny monitoring przez dedykowane zespoły ds. wykrywania fraudów wewnętrznych, systemy , systemy nadzoru wydruku, systemy monitorujące ruch internetowy pracowników oraz inne systemy bezpieczeństwa zapewniające wspomniane wyżej zarządzanie uprawnieniami.

Urząd Komisji Nadzoru Finansowego, w zakresie swoich kompetencji, na bieżąco analizuje informacje przekazywane również przez nieprofesjonalnych uczestników rynku, dotyczące działalności podmiotów nadzorowanych. Większość sygnałów w zakresie przetwarzania przez podmioty nadzorowane danych osobowych, które napływają do UKNF, dotyczy przekazywania informacji na temat zobowiązań kredytowych klientów do Biura Informacji Kredytowej S.A. W zakresie nieuprawnionego posługiwania się danymi osobowymi klientów podmiotów nadzorowanych, zgłaszane problemy i prowadzone analizy koncentrują się głównie na sprawach związanych z:

1. posługiwaniem się przez osobę trzecią dowodem osobistym uzyskanym w wyniku kradzieży i w związku z tym próbą wyłudzenia kredytu, pożyczki lub próbą otwarcia rachunku bankowego,
2. wyłudzeniem danych klienta (w tym danych do logowania do serwisu transakcyjnego banku) przez osoby trzecie niebędące pracownikami banków celem wyprowadzenia środków pozostających na rachunkach bankowych danej osoby (phishing, smishing i inne techniki wyłudzania danych),
3. próbą zawierania umów rachunku bankowego na tzw. „słupa",
4. procederem „sprzedaży rachunku" celem wykorzystania do działalności przestępczej, zakładania rachunków „na przelew",
5. tzw. „fraudami pracowniczymi" polegającymi na dokonywaniu przez pracownika banku dyspozycji nieautoryzowanych przez klienta.

Należy stwierdzić, że wspomniany przez Pana Prezesa obowiązek, wynikający z art. 104 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2018 r., poz. 2187 z późn. zm.) do zachowywania tajemnicy bankowej, jest w ocenie KNF powszechnie znany i respektowany przez sektor bankowy, co nie stoi w sprzeczności ze stwierdzeniem o możliwym *„nielegalnym pozyskaniu danych osobowych i wykorzystywania ich bez wiedzy i zgody osób, których dane dotyczą, przez pracowników banku"*. Odpowiedzialność za wykrywanie takich przypadków oraz podejmowanie stosownych działań leży po stronie podmiotów nadzorowanych przez KNF.

Również w przypadku przedstawionym w reportażu emitowanym w telewizji [redacted], dane osobowe, które zostały udostępnione w portalach sprzedażowych, zostały uzyskane w wyniku popełnienia przestępstwa, dlatego też o naruszeniu zostały zawiadomione właściwe organy (UODO, organy ścigania).

Reasumując pragnę poinformować, iż KNF na bieżąco analizuje dynamiczny rozwój technologii i kanałów dostarczania usług finansowych oraz dostrzega problem nowych zagrożeń dla rynku finansowego. Dla przykładu w najbliższym czasie planowany jest przegląd rekomendacji i wytycznych dotyczących zarządzania bezpieczeństwem informacji oraz ryzykami IT na rynku finansowym, a także rozpoczęcie prac nad stworzeniem jednolitego modelu oceny ryzyka obszaru cyberbezpieczeństwa podmiotów nadzorowanych, czy opublikowanie nowego stanowiska KNF w zakresie przetwarzania przez podmioty nadzorowane danych w chmurze obliczeniowej.

Ponadto UKNF, wzorem poprzednich lat, kontynuuje aktywne działania edukacyjne dotyczące tematyki bezpieczeństwa informacji i cyberbezpieczeństwa w ramach projektu CEDUR (Centrum Edukacji Dla Uczestników Rynku) dla przedstawicieli sektorów rynku finansowego oraz kluczowych instytucji państwowych. W przypadku potwierdzenia chęci uczestnictwa pracowników Urzędu Ochrony Danych Osobowych w planowanych warsztatach – wszelkie szczegóły zostaną ustalone odrębnie.

Z poważaniem

PRZEWODNICZĄCY
KOMISJI NADZORU FINANSOWEGO

Jacek Jastrzębski