PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 22.01.2024 r.

DPNT.401.18.2025

Pan
Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji
Ministerstwo Cyfryzacji

ePUAP**:** /MAiC/SkrytkaESP

Szanowny Panie Premierze,

w odpowiedzi na pismo z 8 stycznia 2025 r. (znak: DC.WAC.5555.32.2024), w związku z przedłożeniem projektu **Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025-2029,** (dalej: „projekt strategii"), działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] oraz art. 51 ustawy o ochronie danych osobowych[2], Prezes UODO (organ nadzorczy) uprzejmie przedstawia następujące uwagi.

Cyberbezpieczeństwo państwa powinno mieć bez wątpienia priorytetowe znaczenie dla wszystkich organów państwa zaangażowanych w procesy przetwarzania informacji i jest niezwykle istotnym zagadnieniem także dla Prezesa Urzędu Ochrony Danych Osobowych jako organu nadzorczego do spraw ochrony danych osobowych, czego wyrazem jest jego aktywny udział w opiniowaniu dotychczasowych projektów strategicznych planów cyfryzacji Polski[3]. Obowiązki administratorów wynikające z przepisów dotyczących przetwarzania informacji w różnych dziedzinach funkcjonowania państwa, w tym wynikające z prawa ochrony danych osobowych, często wiążą się z tymi dotyczącymi cyberbezpieczeństwa.

[1] Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietna 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.).
[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019, poz. 1781).
[3] Zob. np. stanowisko Prezesa UODO w sprawie Strategii Cyfryzacji przedstawione 12.12.2024 r., DOL.401.502.2024.

Jednocześnie **realizacja obowiązków z zakresu cyberbezpieczeństwa z poszanowaniem tych dotyczących przetwarzania danych osobowych właściwie wpisuje się nie tylko w ochronę danych osobowych, ale także przyczynia się do zapewniania bezpieczeństwa państwa i osób, których dane są przetwarzane**. W tym kontekście projekt strategii cyberbezpieczeństwa obejmuje szereg bardzo istotnych kwestii dla zapewnienia szeroko rozumianego bezpieczeństwa danych oraz informacji przetwarzanych w sektorze publicznym oraz prywatnym w obliczu trwających nieustannie i rozwijających się wrogich działań w cyberprzestrzeni. Z tego względu przedstawiony projekt strategii ma szczególne znaczenie dla Prezesa UODO.

Przedstawienie projektu strategii i podjęcie prac nad przygotowaniem takiego dokumentu należy zatem ocenić bardzo pozytywnie. Tak też należy odnieść się do proponowanego wzmocnienia odporności cyberprzestrzeni poprzez zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym i prywatnym oraz promowanie wiedzy i dobrych praktyk w zakresie ochrony ich własnych danych i informacji.

Jednocześnie jednak niektóre zagadnienia przedstawione w projekcie strategii mogą budzić wątpliwości czy też wymagają wyjaśnienia. W celu wzmocnienia projektu strategii w kontekście ochrony danych osobowych i bezpieczeństwa informacji, Prezes Urzędu Ochrony Danych Osobowych przedstawia poniższe uwagi.

1. **Podstawa prawna**

Jak słusznie wskazano w projekcie strategii, ryzyko wystąpienia cyberzagrożeń wpływających na bezpieczeństwo państwa nieustannie wzrasta. Rolą państwa jest więc zapewnienie możliwie najwyższego stopnia bezpieczeństwa cyfrowego kraju, które zrealizowane może zostać poprzez podjęcie konkretnych działań w tym zakresie. Organ nadzorczy rozumie wagę przedstawionego projektu strategii dla bezpieczeństwa obywateli i popiera rozwiązania mające zapewnić im większą ochronę w świecie cyfrowym. Organ nadzorczy uważa tym samym za konieczne zwrócenie uwagi na aspekt **konieczności dokonania zmian w przepisach prawa** w zakresie wskazanym w projekcie strategii. Prawodawca powinien wziąć pod uwagę, że rozwiązania mające zapewnić cyberbezpieczeństwo mogą być wprowadzane **jedynie w oparciu o wyraźną podstawę prawną**. Dokonanie kompleksowych i wyczerpujących zmian w prawie, przede wszystkim na poziomie ustawowym, poprzedzać powinno wprowadzenie konkretnych rozwiązań mających zapewnić cyberbezpieczeństwo. Często bowiem rozwiązania te wpływać będą na sposób przetwarzania danych osobowych, ich jawność lub dostępność. Przepisy prawa powinny być dostosowane do szybko zmieniających się rozwiązań technologicznych, a docelowo, na ile to możliwe, powinny rozwiązania te wyprzedzać. Projektowane przepisy powinny być przy tym neutralne technologicznie, co zapewniałoby odporność tych rozwiązań na zmiany technologii.

Jednocześnie Prezes UODO zauważa **potrzebę szerszej analizy oraz zmiany przepisów już obowiązujących**, wprowadzających wadliwe z punktu

widzenia ochrony danych rozwiązania, które w ocenie organu nadzorczego negatywnie wpływać mogą na zachowanie cyberbezpieczeństwa państwa.

W szczególności wskazać w tym miejscu należy **rejestry publiczne**[4], w których jawne i ogólnodostępne są dane osobowe, m.in. numer PESEL (np. rejestr ksiąg wieczystych), a także podpisy elektroniczne, w których numer PESEL wykorzystywany jest w formie identyfikatora. Poprzez wykorzystanie numeru PESEL można zidentyfikować konkretną osobę. Jego użycie wymagane jest także jako element weryfikacji tożsamości przy wielu czynnościach niosących za sobą daleko idące konsekwencje dla obywatela (np. udzielenie kredytu). Jego nieuprawnione użycie stanowi więc istotne zagrożenie dla osób fizycznych. W związku z tym możliwość jego nieuprawnionego użycia powinna zostać uznana za cyberzagrożenie dla praw i wolności obywateli. Kwestia ta ma znaczenie także w związku z przewidywanym w rozporządzeniu eIDAS2 europejskim portfelem tożsamości cyfrowej oraz pojęciem certyfikatu podpisu elektronicznego – prawodawca rozważyć powinien zmianę prawa w celu dostosowania polskich przepisów do wymogów wynikających z tego rozporządzenia.

Z powyżej przytoczonych przykładów wynika więc, że istnieje **potrzeba dokonania przeglądu dotychczasowego modelu funkcjonowania rejestrów i wypracowania jednolitych standardów ich tworzenia** w oparciu m.in. o ogólne zasady przetwarzania danych wskazane w art. 5, z zachowaniem warunków określonych w art. 6 ust. 3 oraz art. 9 rozporządzenia 2016/679. Zwrócić należy uwagę, że odpowiednio zaprojektowany rejestr publiczny gwarantować powinien prawidłowość, integralność i poufność przetwarzanych w nim danych zgodnie z zasadą poufności i integralności.

W projekcie strategii (pkt 2) wskazano, że „istotne jest, aby prawo do prywatności nie utrudniało identyfikacji cyberprzestępców oraz ich ścigania i nie zapewniało im bezkarności". Choć walka z cyberprzestępczością jest bardzo istotnym i społecznie oczekiwanym działaniem, to jednak ograniczenie stosowania przepisów rozporządzenia 2016/679 oraz przepisów wdrażających dyrektywę 2016/680[5] i inne akty prawne z zakresu ochrony praw podstawowych może zostać dokonane jedynie na zasadach określonych w przepisach tych aktów (w tym w art. 23 rozporządzenia 2016/679), ale także z uwzględnieniem art. 52 ust. 2 Karty Praw Podstawowych UE, a także art. 47 i 51 Konstytucji RP w zw. z jej art. 31 ust. 3.

W projekcie strategii uwzględnione powinno być zatem zarówno wprowadzenie nowych przepisów prawa odpowiadających na ryzyka związane z

---

[4] Zgodnie z art. 3 pkt 5 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307), dalej: ustawa o informatyzacji, rejestr publiczny oznacza rejestr, ewidencję, wykaz, listę, spis albo inną formę ewidencji, służące do realizacji zadań publicznych, prowadzone przez podmiot publiczny na podstawie odrębnych przepisów ustawowych.

[5] 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 (Dz. U. UE. L. z 27.04.2016, Nr 119, str. 89 ze zm.).

pojawiającymi się technologiami, jak i przegląd oraz zmiana już istniejących regulacji i rozwiązań.

2. Analiza ryzyka

Przy wprowadzaniu zmian w przepisach prawa prawodawca powinien wykonać **analizę ryzyka przetwarzania danych**, która wykazywałyby m.in. niezbędność wykorzystania danych do projektowanych rozwiązań. W szczególności dotyczy to rozwiązań związanych z cyberbezpieczeństwem, które wielokrotnie wiążą się z użyciem nowych technologii, i które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 35 ust. 1 rozporządzenia 2016/679). Przeprowadzenie testu prywatności powinno następować już na etapie tworzenia przepisów prawa (*privacy by design* – art. 25 rozporządzenia 2016/679), przed przyjęciem założeń do konkretnych projektów informatycznych, a prawodawca przy tworzeniu przepisów kierować powinien się podejściem opartym na ryzyku (art. 24 rozporządzenia 2016/679). W szczególności powinno mieć to miejsce w przypadkach dotyczących rejestrów publicznych oraz integracji danych, jak chociażby wskazany w pkt 5.3 projektu strategii system łączności mobilnej umożliwiającej przetwarzanie informacji niejawnych do klauzuli „zastrzeżone" w oparciu o system CATEL, Centrum Wymiany i Analizy Informacji, czy platforma elektronicznego zarządzania dokumentami niejawnymi.

3. Rozwiązania technologiczne

W projekcie strategii nie wskazano na **zagadnienie przetwarzania danych biometrycznych** (art. 4 pkt 14 rozporządzenia 2016/679), których użycie dla celów identyfikacyjnych jest coraz powszechniej wykorzystywane. Organ nadzorczy widzi jednak potrzebę zwrócenia uwagi na ryzyka związane z przetwarzaniem danych biometrycznych, które pod rozwagę powinien wziąć prawodawca. Dane biometryczne należą do danych szczególnych kategorii określonych w art. 9 ust. 1 rozporządzenia 2016/679. Ich przetwarzanie jest co do zasady zabronione, chyba że spełniony jest jeden z warunków wskazanych w art. 9 ust. 2 rozporządzenia 2016/679. Należy zwrócić uwagę również na konsekwencje posłużenia się danymi biometrycznymi i możliwość wyinterpretowania z nich dalszych danych o osobie. Kwestia danych biometrycznych powinna być uregulowana w taki sposób, aby zapewnione zostało ograniczenie przetwarzania danych biometrycznych do niezbędnego minimum, przy zachowaniu właściwych rygorów ochrony i poufności danych osobowych, tj. ze wskazaniem mechanizmów przewidujących odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą oraz stworzeniem możliwych rozwiązań alternatywnych.

Prezes UODO chciałby także zwrócić uwagę na **ryzyka związane z użyciem sztucznej inteligencji** w kontekście cyberbezpieczeństwa. Prawodawca zwrócić powinien uwagę na ryzyka związane z kradzieżą tożsamości, technologiami

śledzącymi czy podszywaniem się pod osoby przy użyciu narzędzi sztucznej inteligencji. Moduły wykorzystujące sztuczną inteligencję oraz inne nowe technologie, w tym zaawansowane technologie biometryczne mogą być źródłem istotnych zagrożeń takich jak ukryta dyskryminacja, czy identyfikacja. Zagadnienia te mają szczególne znaczenie w przypadku przetwarzania danych osobowych, w tym wizerunku osób, gdzie stosując metody sztucznej inteligencji możliwa jest nie tylko identyfikacja lub weryfikacja osób, ale również określenie ich stanu zdrowia czy stanów emocjonalnych. Wraz z rosnącym znaczeniem i większym powszechnym dostępem do tych narzędzi projekt strategii uwzględniać powinien sposoby zacieśnienia współpracy pomiędzy organami publicznymi, których zadaniem byłby nadzór nad prawidłowym korzystaniem z narzędzi sztucznej inteligencji. Prawodawca powinien każdorazowo przy dopuszczaniu do użycia narzędzi sztucznej inteligencji zadbać o przeprowadzenie odpowiedniej analizy ryzyka w zakresie bezpieczeństwa danych, zwracając szczególną uwagę czy przy ich wykorzystaniu nie dochodzi do zautomatyzowanego podejmowania decyzji wywołującego wobec jednostki skutki prawne lub w sposób podobny istotnie na nią wpływającego. Prawodawca przy tworzeniu rozwiązań dopuszczających użycie narzędzi sztucznej inteligencji powinien zadbać o odpowiednią podstawę prawną dla tego rodzaju operacji przetwarzania, a także o spełnienie obowiązku informacyjnego, realizowanie prawa do interwencji ludzkiej, czy wdrażanie właściwych środków ochrony interesów osób, których dane dotyczą. Szczególna uwaga powinna zostać poświęcona operacjom przetwarzania danych szczególnych kategorii. Uwaga ta odpowiada także motywowi 66 czekającego na wdrożenie unijnego rozporządzenia 2024/1689 (tzw. AI Act)[6], w którym podkreślono, że „do systemów AI wysokiego ryzyka należy stosować wymogi dotyczące zarządzania ryzykiem, jakości i istotności wykorzystywanych zbiorów danych, dokumentacji technicznej i rejestrowania zdarzeń, przejrzystości i przekazywania informacji podmiotom stosującym, nadzoru ze strony człowieka oraz solidności, dokładności i cyberbezpieczeństwa”.

4. Uwagi szczegółowe

Uwagi szczegółowe należy zacząć od wskazania, że w projekcie **strategii nie wyjaśniono dokładnego zakresu tej strategii**. Niejasne jest przede wszystkim czy projekt strategii ogranicza się jedynie do sfery wykonawczej NIS2 oraz ustawy o krajowym systemie cyberbezpieczeństwa (na co wskazuje fragment pkt. 3: „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025-2029 nie obejmuje jednak tych kwestii, jako wykraczających poza ramy ustawowe określające KSC”), czy też ma charakter szerszy, obejmujący m.in. kwestię ochrony danych oraz bezpieczeństwa określonych w rozporządzeniu 2016/679 oraz dyrektywie 2016/680

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 13.06.2024, poz. 1689).

(na szerszy zakres strategii wskazuje chociażby „Cel szczegółowy 4. Budowanie świadomości, wiedzy i kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa oraz obywateli”).

W pkt. 1 strategii cyberbezpieczeństwa, w miejscu w którym mowa o spójności przyjmowanej strategii z innymi dokumentami, wskazane powinno zostać, że projektowana strategia **musi być zgodna także z przepisami unijnymi**, w tym ze wspomnianym rozporządzeniem 2016/679.

Odnośnie do punktu 4.2, w którym określono cel główny strategii, w zakresie promowania wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę informacji, wskazać należy, że cel ten dotyczy także zakresu zastosowania rozporządzenia 2016/679 i kompetencji organu nadzorczego, o których mowa m.in. w art. 57 i 58 rozporządzenia 2016/679. Także wskazany w pkt. 4.3 „Cele szczegółowe” cel szczegółowy 4 dotyczy m.in. zwiększenia świadomości co do ochrony danych w społeczeństwie. Strategia zawierać powinna uwzględniać więc, we wskazanym zakresie, także odpowiednie przepisy rozporządzenia 2016/679 oraz rolę organu nadzorczego.

W pkt. 5.2 wskazano, że system teleinformatyczny S46 wspiera dokonywanie zgłoszenia naruszeń ochrony danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych. Zasadnym wydaje się, aby prawodawca uwzględnił także zgłoszenia dokonywane na podstawie dyrektywy 2016/680.

W pkt. 5.3 projektu strategii, w kontekście zapewnienia dostępu do wiedzy eksperckiej dotyczącej cyberzagrożeń, wskazano Centra Wymiany i Analizy Informacji (ISAC). Nie jest jednak jasne, na jakiej podstawie prawnej funkcjonować mają ww. Centra, gdyż w ostatnim przedstawionym organowi projekcie ustawy o krajowym systemie cyberbezpieczeństwa (projekt z 3 października 2024 r.) nie przewidziano powstania ISAC.

Zwiększenie cyberbezpieczeństwa podmiotów kluczowych i podmiotów ważnych, o którym mowa w pkt. 5.4 projektu strategii, w ocenie organu nadzorczego, uzupełnione powinno zostać o uwzględnienie podmiotów znajdujących się w łańcuchu dostaw, które jednak nie znajdują się w treści regulacji ustawy o krajowym systemie cyberbezpieczeństwa ani NIS2. Naruszenie bezpieczeństwa u jednego z mniejszych podmiotów w łańcuchu dostaw może powodować bowiem późniejsze negatywne skutki dla bezpieczeństwa podmiotów kluczowych i ważnych. Dalej w pkt. 5.4 projektu strategii omówiono działania strategiczne, które mają zostać podjęte w związku ze wzrostem liczby cyberataków. Wskazane w projekcie strategii pojęcie cyberataków odnosi się jednak tylko do tych cyberataków, które określone zostały w ustawie o krajowym systemie cyberbezpieczeństwa. Dla zapewnienia pełniejszej i szczelniejszej ochrony przed cyberatakami właściwym wydaje się **przyjęcie szerszej definicji cyberataków**, wykraczającej poza ramy ustawy o krajowym systemie cyberbezpieczeństwa. Ta sama uwaga odnosi się także do pkt. 7.1, w którym wskazano, że „certyfikowane produkty, usługi i procesy ICT będą objęte nadzorem krajowego organu do spraw certyfikacji cyberbezpieczeństwa” – wydaje się, że objęci nadzorem powinni zostać także dostawcy niewskazani w treści regulacji ustawy o krajowym systemie cyberbezpieczeństwa.

Pozytywnie należy ocenić przewidziany w punkcie 5.7 projektu strategii przegląd i dalszy rozwój narzędzi wprowadzonych ustawą o zwalczaniu nadużyć w komunikacji elektronicznej[7] służących **ograniczaniu podszywania się przestępców pod adresy elektroniczne osób prywatnych, banków i innych instytucji**. Zamierzone cele będą jednak trudne do osiągnięcia, jeśli środki ograniczające podszywanie się pod inne osoby nie zostaną wprowadzone również w odniesieniu do elektronicznej komunikacji głosowej, poprzez ograniczenie lub całkowite wyeliminowanie tzw. CallerID Spoofingu. W związku z powyższym w punkcie 5.7 projektu strategii celowym byłoby rozszerzenie działań ministra właściwego do spraw informatyzacji w zakresie przeglądu stosowanych środków bezpieczeństwa w komunikacji elektronicznej oraz sporządzenie planu działań naprawczych, poprzez dostosowanie przepisów oraz inicjowanie działań mających na celu modyfikację lub opracowywanie i wprowadzanie nowych środków bezpieczeństwa, w tym bezpieczeństwa komunikacji głosowej.

W pkt 6.1 projektu strategii wskazano na wprowadzenie rozwiązań umożliwiających wyłączenie stosowania Prawa zamówień publicznych[8]. Projektodawca rozważyć powinien wprowadzenie rozwiązań zapewniających ograniczenie dostępu do informacji o szczegółach towarów i usług zakupionych na potrzeby cyberbezpieczeństwa. Ponadto, jak wskazano w projekcie strategii, podjęte zostaną działania na rzecz zwiększenia cyberbezpieczeństwa systemów i rejestrów państwowych oraz cyfrowych usług publicznych. Rozwiązania te uwzględniać powinny odpowiednią retencję danych oraz wynikającą z art. 51 Konstytucji RP oraz art. 8 EKPC[9] ochronę przed gromadzeniem i wykorzystywaniem danych osobowych, stanowiącą część prawa do poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji. W ostatnim zdaniu pkt. 6.1 projektu strategii słusznie zwrócono uwagę na rozwój narzędzi technicznych i organizacyjnych mających na celu wzmocnienie poziomu cyberodporności i higieny cyfrowej małych i średnich przedsiębiorstw. **Nieuzasadnione jednak wydaje się wskazywanie, że cel ten zostanie osiągnięty poprzez certyfikację cyberbezpieczeństwa procesów ICT** u tych przedsiębiorców, gdyż rolą certyfikacji nie jest rozwój narzędzi technicznych czy organizacyjnych, lecz potwierdzenie właściwego, czyli zgodnego z przyjętymi standardami ich stosowania. Podkreślić należy, że podniesienie poziomu odporności systemów informacyjnych odbywać powinno się z uwzględnieniem kryteriów wskazanych w art. 32 rozporządzenia 2016/679.

Pogłębienia analizy i szerszej dyskusji wymaga przewidziany w pkt 6.2 projektu strategii **rozwój krajowej kryptografii, w tym migracji do kryptografii postkwantowej oraz rozwój technologii kwantowych**. Zgodnie z założeniami strategii technologie kwantowe wykorzystywane mają być m.in. do ochrony danych.

---

[7] Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2024, poz. 1803).
[8] Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320).
[9] Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r., Nr 61, poz. 284).

Choć rozwój krajowej kryptografii należy ocenić jako słuszny i ważny kierunek rozwojowy, to w projekcie strategii nie wskazano w jakim zakresie mają być wykorzystywane oraz jakie podmioty zobowiązane będą do ich używania. Wybór odpowiedniej metody zabezpieczeń danych przy użyciu technologii kwantowych powinien być natomiast przedmiotem szerszej debaty, gdyż przedstawiony projekt strategii nie wyjaśnia jakie narzędzia technologii kwantowej mają zostać wykorzystane. Ponadto, ze względu na koszty zastosowania technologii kwantowych prawodawca rozważyć powinien wsparcie w tym zakresie zarówno dla podmiotów sektora publicznego, jak i prywatnego. Określony powinien zostać także konkretny harmonogram wprowadzania nowych rozwiązań technologicznych – prawodawca musi bowiem pamiętać, że zastosowanie kryptografii postkwantowej oraz technologii kwantowej może być niemożliwe w przypadku posługiwania się starszymi systemami operacyjnymi. Potencjalni użytkownicy rozwiązań postkwantowych oraz kwantowych muszą być przygotowani na wdrożenie takich rozwiązań. Należy również zwrócić uwagę, że w odniesieniu do fragmentu, w którym mowa, że standardy będą uwzględniać obszary, gdzie będzie można w dalszym ciągu korzystać z dotychczasowych rozwiązań kryptograficznych, w tym technologii zwiększających prywatność, warto poddać rozwadze uwzględnienie PETs i dotychczasowych rozwiązań tam, gdzie to będzie możliwe.

W pkt. 6.3 projektu strategii zaproponowano **rozwój usług przetwarzania w chmurze obliczeniowej.** Docelowo jak najwięcej podmiotów ma mieć możliwość korzystania z usług przetwarzania w Publicznej Chmurze Obliczeniowej. W projekcie strategii nie przedstawiono jednak konkretnych warunków dotyczących przechowywania danych, ani mechanizmów weryfikacji bezpieczeństwa usług. Nie wskazano także na konieczność przeprowadzenia **analizy ryzyka oraz oceny skutków dla ochrony danych** w tym zakresie, ani nie określono ryzyka naruszenia praw i wolności osób wynikającego z przetwarzania dużej ilości danych osobowych i wpływu na liczbę osób, których dane dotyczą. Projekt strategii zakłada także budowę systemów informatycznych państwa w sposób umożliwiający migrację danych poza granice Rzeczypospolitej Polskiej. Należy zwrócić uwagę, że w przypadku przekazywania danych osobowych do państw trzecich spełnione muszą być warunki określone w rozdziale V rozporządzenia 2016/679. Dla zachowania bezpieczeństwa oraz suwerenności technologicznej istotną kwestią jest jaki podmiot obsługiwać będzie Publiczną Chmurę Obliczeniową – krajowy czy spoza EOG. Powierzenie prowadzenia platformy podmiotowi prywatnemu spoza EOG powodowałoby natomiast dodatkowe ryzyka dla danych w niej przetwarzanych. Ponadto, projektodawca szczególną uwagę powinien zwrócić na zasady dotyczące przetwarzania danych osobowych określone w art. 5 rozporządzenia 2016/679 i art. 4 dyrektywy 2016/680 oraz zasady uwzględniania ochrony danych już w fazie projektowania i domyślnej ochrony danych określone w art. 25 rozporządzenia 2016/679 i art. 20 dyrektywy 2016/680. Przyjęte rozwiązania powinny umożliwiać identyfikację administratora (lub administratorów) danych osobowych (w rozumieniu art. 4 pkt 7 rozporządzenia 2016/679), a w przypadku przetwarzania danych przez

wiele podmiotów (w szczególności przez organy publiczne) uwzględnione powinny zostać role współadministratorów lub podmiotów przetwarzających (w rozumieniu art. 4 pkt 8 rozporządzenia 2016/679).

Dla usprawnienia mechanizmów skutecznego zapobiegania i reagowania na incydenty cyberbezpieczeństwa, o czym mowa w pkt. 6.4 projektu strategii, projektodawca rozważyć powinien **utworzenie jednego i zaufanego źródła informacji o incydentach cyberbezpieczeństwa i naruszeniach** wynikających z rozporządzenia 2016/679, w przypadku gdy zachodziłyby przesłanki wskazane w art. 34 rozporządzenia 2016/679. Ponadto, w punkcie 6.4 słusznie podkreślono potrzebę zwiększania zdolności operacyjnych poprzez działania obejmujące m.in. „środki do rozpoznawania zagrożeń w cyberprzestrzeni, rozwój ochrony przed atakami typu DDoS, oprogramowanie i rozwiązania sprzętowe zwiększające cyberbezpieczeństwo". Działania te poprzez dostarczanie narzędzi i usług oraz stosowanie odpowiednich taktyk mają mieć na celu utrudnienie lub uniemożliwienie przeprowadzenia cyberataku. **W projekcie oraz przygotowywanym planie działań nie wskazano jednak konkretnych narzędzi ani usług jakie miałyby być w tym zakresie realizowane.**

W pkt. 6.5 projektu strategii określono rozwój standaryzacji w cyberbezpieczeństwie. W ocenie organu nadzorczego **standaryzacja ta uwzględniać powinna zasady *privacy by design* oraz *privacy by default*** (art. 25 rozporządzenia 2016/679).

Odnośnie do punktu 7.2 wskazać należy, że kwestie działania w obszarze innowacji, rozmaite parki naukowo-techniologiczne, hackatony, wyzwania technologiczne czy konkursy również wiążą się z koniecznością uwzględnienia przepisów rozporządzenia 2016/679.

Kwestia wzmocnienia kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa, omówiona w pkt. 8.1 projektu strategii, dotyczy także przepisów rozporządzenia 2016/679, a zatem wskazany w nim organ nadzoru również objęty powinien być uzupełnieniem kadr o pracowników wyspecjalizowanych w cyberbezpieczeństwie.

W punkcie 8.2 dotyczącym rozwoju świadomości i wiedzy obywateli z zakresu cyberbezpieczeństwa należałoby uwzględnić również problematykę ochronę danych jako jeden z obowiązkowych elementów edukacji.

Podsumowanie

W czasach bardzo szybko zmieniającej się technologii, w których wiele aspektów życia przeniesionych zostało do cyfrowej rzeczywistości, zapewnienie odpowiedniego rozwoju cyberbezpieczeństwa państwa odczytywać należy jako jeden z najważniejszych czynników jego funkcjonowania oraz bezpieczeństwa.

Przedstawiony projekt strategii stanowi istotny dokument, który będzie wywierał wpływ także na sferę praw i wolności obywateli. Dlatego ważne jest, aby rozwiązania prawne z zakresu cyberbezpieczeństwa były w najwyższym stopniu

dopracowane i odpowiadały na wyzwania teraźniejszości i były dostosowywane do pojawiających się nowych zagrożeń.

Przedstawione w piśmie uwagi mają na celu zwrócenie uwagi Pana Premiera i Ministerstwa Cyfryzacji na kilka – istotnych z perspektywy organu nadzorczego – kwestii mających istotny wpływ na zachowanie cyberbezpieczeństwa państwa. Liczę, że będą one przydatne w dalszych pracach nad strategią.

Jednocześnie niezmiennie deklaruję wsparcie eksperckie Urzędu Ochrony Danych Osobowych i liczę na zaangażowanie nad wdrażaniem strategii oraz konkretnych rozwiązań prawnych z niej wynikających.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym/