Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.60.2025
Warszawa, 19 czerwca 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 2 kwietnia br. Posłanki na Sejm RP Pani Małgorzaty Pępek w sprawie ochrony danych osobowych obywateli w sektorze finansowym oraz środków kompensacyjnych w przypadku naruszenia ich poufności (interpelacja nr 8827)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania będące we właściwości Ministra Cyfryzacji.

Ad 1) Czy osobie, której dane osobowe zostały ujawnione w wyniku zaniedbania instytucji finansowej bądź jej podmiotu przetwarzającego, przysługuje jakiekolwiek odszkodowanie lub rekompensata?

Osoba, której dane zostały ujawnione w wyniku zaniedbania administratora lub podmiotu przetwarzającego dane, może uzyskać odszkodowanie za poniesioną szkodę materialną lub niematerialną. Podstawą dochodzenia odszkodowania jest art. 82 ust. 1 RODO[1], w myśl którego każda osoba, która poniosła szkodę materialną lub niematerialną ma prawo uzyskać odszkodowanie od administratora lub podmiotu przetwarzającego dane. Jako szkody majątkowe zalicza się m.in. straty finansowe, a szkody niemajątkowe to np. stres czy utrata poczucia bezpieczeństwa.

Zatem kwestia ewentualnego odszkodowania uzależniona będzie od sposobu jej rozstrzygnięcia przez daną instytucję finansową.

Jeżeli rozwiązanie zaproponowane przez administratora danych (w omawianym przypadku instytucję finansową) nie jest satysfakcjonujące, to na podstawie ustawy o ochronie danych osobowych[2] może zostać wniesiony pozew do właściwego sądu okręgowego.

Ponadto, na podstawie art. 77 ust. 1 RODO, może zostać wniesiona skarga na tę instytucję finansową do Prezesa Urzędu Ochrony Danych Osobowych.

Ad 2) Czy obecnie obowiązujące przepisy prawne są wystarczające, aby zapewnić realną ochronę obywatelom przed skutkami naruszeń danych osobowych, takich jak możliwość wyłudzeń kredytowych czy kradzieży tożsamości?

Obowiązujące obecnie przepisy stanowią solidną podstawę prawną służącą ochronie obywateli przed skutkami naruszeń danych osobowych, w tym wyłudzeniami kredytowymi i kradzieżą tożsamości.

[1] Rozporządzenie 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] art. 93 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781)

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

Należy jednak podkreślić, że w związku z dynamicznym rozwojem technologii, jak również coraz bardziej zaawansowanymi technikami stosowanymi przez cyberprzestępców, istnieje konieczność ciągłego dostosowywania regulacji prawnych.

Podstawową regulacją w zakresie ochrony danych osobowych jest RODO, a także ustawa o ochronie danych osobowych, która służy stosowaniu RODO.

Istotna jest również ustawa o ewidencji ludności[3] regulująca możliwość zastrzeżenia numeru PESEL, która szerzej została opisana w odp. na pyt. 3.

Regulacją niezwykle ważną w zakresie ochrony przed wyłudzaniem danych osobowych jest ustawa o zwalczaniu nadużyć w komunikacji elektronicznej[4].

Na mocy tej ustawy przedsiębiorcy telekomunikacyjni mają obowiązek m.in.

1) blokować krótkie wiadomości tekstowe zawierające treści wyczerpujące znamiona smishingu zgodne ze wzorcem wiadomości przekazanym przez CSIRT NASK - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego poziomu krajowego prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy. Jeden z 3 zespołów CSIRT poziomu krajowego odpowiedzialnych za reagowanie na incydenty cyberbezpieczeństwa (Zespół CSIRT NASK monitoruje występowanie smishingu i przekazuje przedsiębiorcom telekomunikacyjnym wzorce wiadomości wyczerpującej znamiona smishingu);
2) blokować wiadomości, przez które oszuści podszywają się pod podmioty publiczne, np. urząd skarbowy czy urząd miasta (w tym celu tworzony jest wykaz nadpisów – identyfikatorów wiadomości SMS, używanych zamiast numeru telefonu - zastrzeżonych dla podmiotów publicznych);
3) blokować połączenia głosowe, które mają na celu podszywanie się pod inną osobę lub instytucję – w tym celu tworzony jest wykaz numerów służących wyłącznie do odbierania połączeń głosowych (tzw. lista DNO), co ma na celu ograniczenie możliwości podszywania się pod numery infolinii banków, urzędów, czy innych podmiotów.

Ponadto, na mocy wspomnianej ustawy funkcjonuje lista ostrzeżeń dotycząca domen internetowych, które służą do wyłudzeń danych i niekorzystnego rozporządzania mieniem użytkowników internetu. Lista ostrzeżeń prowadzona jest przez CSIRT NASK na podstawie m.in. zgłoszeń dokonywanych przez osoby, które otrzymały wiadomość SMS bądź e-mail zawierający link do strony wyłudzającej dane osobowe. Przedsiębiorcy telekomunikacyjni blokują strony internetowe wpisane na listę ostrzeżeń poprzez usunięcie nazw domenowych z systemów teleinformatycznych przedsiębiorców telekomunikacyjnych. Obecnie na liście ostrzeżeń wpisanych jest ponad 200 000 niebezpiecznych domen.

Ad 3) Czy rozważają Państwo wprowadzenie zmian legislacyjnych w celu zwiększenia ochrony danych osobowych, zwłaszcza w sektorze finansowym, w tym np. wprowadzenie automatycznej ochrony numeru PESEL przed wykorzystaniem przez osoby trzecie bez zgody właściciela?

W kwestii cyberbezpieczeństwa podmiotów finansowych właściwe jest Ministerstwo Finansów, które obecnie proceduje projekt ustawy o zmianie ustawy o nadzorze nad

[3] ustawa z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2025 r. poz. 274)
[4] ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1803)

rynkiem finansowym oraz niektórych innych ustaw (UC11) służący stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011[5]. Celem tej regulacji jest zwiększenie odporności cyfrowej i bezpieczeństwa ICT (ang. *Information and Communications Technology* - technologie informacyjne i komunikacyjne) w obszarze usług finansowych.

Jednocześnie należy podkreślić, że w celu ograniczenia skutków kradzieży tożsamości i wzmocnienia bezpieczeństwa obywateli, ustawodawca już wprowadził nowe mechanizmy ochrony danych osobowych. Na mocy wspomnianej już w odp. na pyt. 2 ustawy o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości[6], każda osoba pełnoletnia może bezpłatnie zastrzec swój numer PESEL.

Bardzo istotnym elementem tej regulacji jest obowiązek weryfikacji statusu numeru PESEL, który obowiązuje od 1 czerwca 2024 r. Oznacza to, że podmioty takie jak banki, instytucje kredytowe, notariusze, operatorzy telekomunikacyjni czy podmioty notarialne mają prawny obowiązek sprawdzenia, czy numer PESEL nie został zastrzeżony — przed dokonaniem czynności prawnej, np. udzieleniem kredytu, pożyczki, ustanowieniem pełnomocnictwa czy zawarciem umowy sprzedaży nieruchomości.

W przypadku nieuwzględnienia zastrzeżenia i zawarcia umowy, osoba poszkodowana nie będzie ponosiła skutków prawnych wynikających z takich działań — co w praktyce stanowi istotną tarczę ochronną przed oszustwami.

Zastrzeżenia numeru PESEL można dokonać elektronicznie (za pomocą aplikacji mObywatel oraz na stronie internetowej gov.pl) lub osobiście w urzędzie gminy.

Dodatkowo użytkownik może:

- cofnąć zastrzeżenie numeru PESEL;
- ustawić automatyczne czasowe zastrzeżenie numeru PESEL;
- sprawdzać historię operacji i prób weryfikacji numeru PESEL.

Ad 4) Jakie działania podejmuje rząd w celu minimalizacji ryzyka przyszłych wycieków danych obywateli oraz podniesienia poziomu cyberbezpieczeństwa w instytucjach publicznych i prywatnych podmiotach finansowych?

Rząd prowadzi intensywne działania w celu minimalizacji ryzyka przyszłych wycieków danych obywateli oraz podniesienia poziomu cyberbezpieczeństwa w podmiotach odpowiedzialnych za funkcjonowania państwa, w szczególności administracji publicznej, zarówno rządowej, jak i samorządowej.

W pierwszej kolejności należy wskazać, że organem odpowiedzialnym za cyberbezpieczeństwo podmiotów rynku finansowego jest Zespół CSIRT KNF realizujący zadania Sektorowego Zespołu Cyberbezpieczeństwa, we współpracy z podmiotami krajowego systemu cyberbezpieczeństwa (KSC).

Ministerstwo Cyfryzacji oraz Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa działający w ramach resortu cyfryzacji realizują szereg działań mających na celu podnoszenie poziomu bezpieczeństwa systemów państwowych. Najważniejsze przedsięwzięcie realizowane przez Ministerstwo to:

[5] Dz. Urz. UE L 333 z 27.12.2022, str. 1
[6] ustawa z dnia 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości (Dz.U. z 2023 r. poz. 1394)

- Projekt AntyDDoS: zapewnia centralnie osłonę przed atakami DDoS instytucji, w tym dla Sił Zbrojnych RP i służb specjalnych – obecnie osłona wdrożona została w 76 instytucjach;
- Bezpieczna łączność dla administracji publicznej: bezpieczny komunikator[7] na urządzenia służbowe dla administracji publicznej i podmiotów KSC, jak również mobilny system łączności niejawnej SKR-Z.
- Platforma CTI: platforma do rozpoznawania zagrożeń w cyberprzestrzeni (CTI) na potrzeby Ministra Cyfryzacji i Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz innych instytucji odpowiedzialnych za bezpieczeństwo teleinformatyczne na poziomie krajowym.
- System S46 – system IT do wymiany informacji i zgłaszania incydentów w ramach krajowego systemu cyberbezpieczeństwa. Na koniec 2024 r. z S46 korzystało 248 podmiotów, w tym operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne.

Jednym z przedsięwzięć, za pomocą których realizowane jest wzmacnianie ochrony kluczowych instytucji państwowych w obliczu rosnącej liczby cyberataków jest współfinansowany ze środków KPO (Inwestycja C3.1.1), konkurs grantowy pn. „Cyberbezpieczny Rząd". Jest to przedsięwzięcie, którego celem jest wsparcie administracji rządowej w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT. Wsparcie skierowane jest do podmiotów krajowego systemu cyberbezpieczeństwa, o których mowa w ustawie o krajowym systemie cyberbezpieczeństwa[8], takich jak naczelne lub centralne organy administracji rządowej oraz wojewodowie. Urzędy obsługujące te organy wraz z jednostkami im podległymi, są uprawnione do otrzymania grantów na poprawę odporności na cyberzagrożenia, w tym sfinansowanie modernizacji systemu zarządzania bezpieczeństwem informacji oraz rozbudowy infrastruktury cyberbezpieczeństwa. Celem projektu „Cyberbezpieczny Rząd" jest zwiększenie poziomu bezpieczeństwa informacji poprzez wzmacnianie odporności na incydenty w naczelnych i centralnych instytucjach państwowych. Wsparcie to obejmuje trzy kluczowe obszary cyberbezpieczeństwa, tj.: obszar organizacji, technologii i kompetencji. Stopień intensywności wsparcia w każdym z tych obszarów jest zależny od konkretnych potrzeb każdej organizacji. Nabór wniosków o granty w ramach projektu „Cyberbezpieczny Rząd" został zakończony w dniu 31 marca 2025 r., zgodnie z komunikatem dostępnym na stronie gov.pl. Szczegóły projektu dostępnie są stronie: Centrum Projektów Polska Cyfrowa. Do konkursu przystąpiło 53 Wnioskodawców, w tym: 13 ministerstw, 21 urzędów centralnych oraz 16 urzędów wojewódzkich. Wartość zgłoszonych projektów wyniosła ponad 276,6 mln zł, co oznacza realizację alokacji środków przeznaczonych na ten projekt na poziomie ponad 79%.

Kolejną inicjatywą jest, współfinansowany ze środków UE w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), projekt pn. „Cyberbezpieczny Samorząd". Celem tego projektu jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego (JST) poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych. Również w tym przypadku zakres wsparcia obejmuje trzy kluczowe obszary cyberbezpieczeństwa, tj.: obszar organizacji, technologii i kompetencji. Projekt ten jest już w trakcie realizacji. Do końca 2024 r. zostały podpisane wszystkie (2 495) umowy z JST, które złożyły wniosek o wsparcie grantowe i sukcesywnie wypłacane są im środki na realizację grantów, których łączna wartość wynosi 1 474 312 573,61 zł. Projekty

[7] https://www.gov.pl/web/baza-wiedzy/komunikator
[8] art. 4 pkt 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024 poz. 1077)

grantowe mogą być realizowane do 30 czerwca 2026 r. Dokumentacja naboru oraz dodatkowe materiały o projekcie dostępne są na stronie Centrum Projektów Polska Cyfrowa.

W przygotowaniu są również kolejne inicjatywy, których celem będzie podniesienie poziomu cyberbezpieczeństwa kolejnych grup podmiotów objętych krajowym systemem cyberbezpieczeństwa. Przykładem takiej inicjatywy jest np. planowany do uruchomienia w połowie tego roku, również współfinansowany ze środków KPO konkurs grantowy dla przedsiębiorstw realizujących zadania polegające na zbiorowym zaopatrzeniu w wodę i wykorzystujących w realizacji tych zadań technologie operacyjne (OT) w przemysłowych systemach sterowania (ICS).

Należy również podkreślić, że Ministerstwo Cyfryzacji proceduje projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) wprowadzający wymóg wdrożenia systemu zarządzania bezpieczeństwem informacji przez podmioty kluczowe i podmioty ważne w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)[9]. Istotą tych rozwiązań jest zwiększenie cyberbezpieczeństwa podmiotów publicznych oraz prywatnych, a przez to poziom cyberbezpieczeństwa całego kraju.

Mając na uwadze krytyczne znaczenie kompetencji z zakresu cyberbezpieczeństwa wśród osób pełniących najważniejsze funkcje w państwie, Minister Cyfryzacji we współpracy z NASK-PIB[10] prowadzi projekty prewencyjno-edukacyjne (tzw. projekty SecureV). W ramach projektów realizowane są specjalne, indywidualne szkolenia z zakresu cyberbezpieczeństwa dla kluczowych osób w państwie. Są to szkolenia realizowane indywidualnie lub w małych grupach, a terminy i zakres merytoryczny szkoleń dostosowywane są do konkretnych potrzeb szkolonych osób. Każda indywidualnie przeszkolona osoba zostaje wyposażona w uniwersalne narzędzia służące do silnego uwierzytelnienia. W latach 2025-2026 w ramach projektu przeszkoleni zostaną: obejmuje przedstawiciele władzy ustawodawczej i wykonawczej, przedstawiciele jednostek samorządu terytorialnego, przedstawiciele sądów i prokuratur, przedstawiciele Krajowego Biura Wyborczego oraz organów wyborczych.

NASK-PIB realizuje również wiele działań edukacyjnych z zakresu cyberbezpieczeństwa, które są kierowane do różnych grup użytkowników internetu. W ramach takich działań NASK-PIB prowadzi kampanie informacyjne w zakresie bezpiecznego korzystania z internetu a także opracowuje i publikuje materiały edukacyjne dot. różnego rodzaju oszustw internetowych, w tym m.in. oszustw na fałszywe inwestycje, (Uważaj na fałszywe inwestycje w sieci, fałszywych sklepów online (Jak kupować bezpiecznie online.).

Ponadto, na portalu gov.pl rozwijana jest baza wiedzy o cyberbezpieczeństwie[11], gdzie publikowane są poradniki, artykuły, rekomendacje oraz inne materiały edukacyjne, które

[9] Dz. Urz. UE L 333 z 27.12.2022, str. 80
[10] Naukowa i Akademicka Sieć Komputerowa - to państwowy instytut badawczy nadzorowany przez Minister Cyfryzacji. Kluczowym polem aktywności NASK-PIB są działania związane z zapewnianiem bezpieczeństwa internetu, reagowaniem na zdarzenia naruszające bezpieczeństwo sieci w Polsce oraz działania edukacyjne.
[11] https://www.gov.pl/web/baza-wiedzy/aktualnosci

pozwalają społeczności internetowej zdobyć wiedzę na temat bezpiecznego korzystania z technologii cyfrowych oraz jak chronić swoje dane w internecie.

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa