Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.25.2025
Warszawa, 12 maja 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 20 października br. (sygn. DSP.INT.4510.40.2025) interpelacji Posła na Sejm RP Pana Jarosława Zielińskiego w sprawie działań rządu dla zapewnienia bezpieczeństwa państwa i obywateli wobec ataku hakerskiego na firmę EuroCert sp. z o.o. świadczącą komercyjne usługi na rzecz administracji publicznej w zakresie elektronicznej warstwy dowodu osobistego (interpelacja nr 7605)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Jaka jest skala wycieku danych osobowych urzędników oraz pracowników administracji państwowej?

Ad 2) Jaka jest skala wycieku danych funkcjonariuszy służb państwowych oraz żołnierzy Wojska Polskiego?

Ad 3) Jaka jest skala wycieku danych osobowych obywateli zajmujących kluczowe funkcje w gospodarce oraz spółkach strategicznych?

Uprzejmie informuję, że powyższe pytania są poza właściwością Ministra Cyfryzacji.

Ad 4) Czy podjęto działania mające na celu rezygnację (zawieszenie) z wszelkich usług świadczonych przez firmę EuroCert Sp. z o.o. na rzecz instytucji publicznych? Miałoby to znaczenie prewencyjne przy braku wiedzy co do skali ataku oraz faktycznej ilości wykradzionych danych.

Sprawa jest na bieżąco monitorowana i nadzorowana w ramach spotkań koordynacyjnych Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), w którym uczestniczą przedstawiciele najważniejszych dla bezpieczeństwa państwa instytucji oraz reprezentanci zespołów analiz i analiz technicznych kluczowych instytucji dla ww. zdarzenia.
W omawianej sprawie odbyło się również posiedzenie Zespołu do spraw Incydentów Krytycznych, podczas którego omówione zostały niezbędne do realizowania czynności celem niwelowania potencjalnych szkodliwych skutków incydentu.

Ponadto ww. sprawie został na stronie internetowej gov.pl upubliczniony Komunikat Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa zawierający m.in. zalecenia niezbędne do podjęcia z zamiarem minimalizacji zagrożeń i negatywnych skutków dla użytkowników produktów firmy EuroCert Sp. z o.o. których dotyczy wyciek.

Należy także podkreślić, że Minister Cyfryzacji wszczął z urzędu postępowanie administracyjne w sprawie możliwości prowadzenia przez EuroCert sp. z o. o. - kwalifikowanego dostawcę usług zaufania – w zakresie działalności niezgodnymi z przepisami ustawy o usługach zaufania i identyfikacji elektronicznej[1].

Ad 5) Jakie koszty w skali roku ponosi administracja publiczna z tytułu zakupu usług podpisu elektronicznego dla urzędników?

W oparciu o stanowisko Centrum Personalizacji Dokumentów Ministerstwa Spraw Wewnętrznych i Administracji informuję, że koszt serwisu i utrzymania informatycznego

[1] Ustawa z dnia 5 września 2016 r. o usługach zaufania i identyfikacji elektronicznej (Dz.U. z 2024 r., poz. 1725).

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

ul. Królewska 27
00-060 Warszawa

systemu do personalizacji dowodów osobistych, za pomocą którego są generowane i nagrywane certyfikaty w warstwie elektronicznej dowodu osobistego w 2025 r. wynosi miesięcznie 871 500 zł netto.

Ad 6) Jaka jest aktualna liczba wydanych dowodów osobistych z warstwą elektroniczną?

Statystyki dot. e-dowodów są generowane w określonych cyklach. Zgodnie z ostatnią aktualną informacją ponad 14 mln Polaków odebrało dowód z warstwą elektroniczną, z czego prawie 11 mln to osoby dorosłe.

Ad 7) Jakie są aktualne koszty utrzymania systemu wydanych nieodpłatnie obywatelom kluczy elektronicznych umieszczonych w warstwie elektronicznej dowodu osobistego?

Ministerstwo Cyfryzacji odpowiada wyłącznie za utrzymanie Rejestru Dowodów Osobistych. Nie jest również możliwe wskazanie konkretnych kosztów utrzymania pojedynczych komponentów, które wchodzą w skład SRP – miesięczne koszty utrzymania obejmują cały SRP.

Ad 8) Jakie są podejmowane działania uświadamiające obywateli o możliwościach wykorzystania udostępnionych kluczy elektronicznych umieszczonych w warstwie elektronicznej dowodu osobistego?

Minister Cyfryzacji podpisał w 2023 r. umowę na wytworzenie Systemu SDK (biblioteki), która po integracji z oprogramowaniem zamawiającego znacząco zwiększy potencjał użycia dowodu osobistego w usługach administracji publicznej. Będzie to możliwe dzięki wykorzystaniu każdego z certyfikatów umieszczonych w warstwie elektronicznej e-dowodu. Po przekazaniu SDK trwały prace zmierzające do implementacji biblioteki na platformach mobilnych (na urządzenia z systemem operacyjnym iOS i Android). Podjęto te prace, aby przygotować i umożliwić powszechnie dostępne i nieodpłatne wykorzystanie certyfikatów z e-dowodu w aplikacji mobilnej mObywatel. W lutym tego roku planowane jest wydanie wersji aplikacji mObywatel oferującej podpisywanie dokumentów podpisem osobistym (certyfikat z e-dowodu).

W wyniku wieloletnich starań Ministerstwo Cyfryzacji doprowadziło do przekazania przez CPD MSWiA licencji do oprogramowania SDK (Software Development Kit). Ma ono umożliwić samodzielne tworzenie aplikacji zintegrowanych z oprogramowaniem zawartym w warstwie elektronicznej e-dowodu do Centralnego Ośrodka Informatyki, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, Centrum e-Zdrowia i Ministerstwa Cyfryzacji. Przekazanie COI licencji na używanie tej biblioteki na COI rozpocząć jej implementację w ekosystemie Systemu Rejestrów Państwowych. Dzięki temu urzędnicy obsługujący tzw. sprawy obywatelskie przy użyciu aplikacji Źródło będą mogli korzystać zarówno z certyfikatu identyfikacji i uwierzytelniania (do logowania w aplikacji), jak i certyfikatu podpisu osobistego – do podpisywania różnego rodzaju zaświadczeń, potwierdzeń, przekazywanych obywatelowi drogą elektroniczną.

Ponadto trwają obecnie ustalenia dotyczące potencjalnego szerszego udostępnienia SDK dla rozwiązań desktopowych innym podmiotom, zainteresowanym integracją swoich rozwiązań dziedzinowych z e-dowodem.

Ponadto informuję, że informacje dotyczące dowodów osobistych z warstwą elektroniczną (tzw. e-dowód) zostały zamieszczone na portalu gov.pl, na stronie poświęconej dowodom osobistym[2] oraz na stronie dedykowanej dla e-dowodu[3]. Na przedmiotowej stronie zostały zawarte szczegółowe informacje dotyczące funkcji e-dowodu, możliwości korzystania z certyfikatów zawartych w warstwie elektronicznej dowodu, jak również stosowanych zabezpieczeń.

[2] https://www.gov.pl/web/gov/dowod-osobisty-informacje
[3] https://www.gov.pl/web/e-dowod

Informacje dotyczące funkcjonalności warstwy elektronicznej dowodu osobistego były zamieszczone w ulotkach przygotowanych dla obywateli, które MSWiA dystrybuowało do organów gmin w 2019 r. w związku z wdrożeniem dowodu osobistego z warstwą elektroniczną.

Od grudnia 2023 r. na urządzeniu do składania podpisu na wniosku o wydanie dowodu osobistego są wyświetlane informacje dotyczące funkcjonalności dowodu osobistego z warstwą elektroniczną, które mają zachęcić obywateli do korzystania z tych możliwości.

Zagadnienia związane z upowszechnianiem wykorzystywania warstwy elektronicznej dowodu osobistego zostały ujęte również w przygotowanym przez Ministerstwo Cyfryzacji projekcie dokumentu Strategia Cyfryzacji Polski do 2035 r.

Ad 9) Czy w związku z faktem, że każdy urzędnik państwowy otrzymał bezpłatne narzędzia autoryzacyjne umieszczone w warstwie elektronicznej dowodu osobistego, planowane jest zastąpienie odpłatnych usług komercyjnych produktami wydawanymi przez Ministra Spraw Wewnętrznych i Administracji? Działania takie zredukowałyby koszty budżetowe oraz przyczyniłyby się do poprawy bezpieczeństwa, uniezależniłyby administrację państwową od usług zewnętrznych, co do których, jak dowodzi aktualna sytuacja, nie ma ona wpływu na ich bezpieczeństwo.

Takie działania są realizowane w ramach projektu SRP 3.0 – Optymalizacja i Rozwój, których zakończenie planowane jest na koniec 2028 r. Niemniej udostępnienie możliwości podpisywania dokumentów certyfikatem z e-dowodu, obok innych opcji podpisu (jak podpis kwalifikowany i podpis zaufany), jest planowane na koniec 2026 r., wraz z dostarczeniem zmodernizowanego Rejestru Dowodów Osobistych.

Z informacji uzyskanych z Ministerstwa Spraw Wewnętrznych i Administracji, należy wskazać, że zgodnie z przepisami ustawy o dowodach osobistych[4] korzystanie z podpisu osobistego ma charakter opcjonalny (zależny od woli posiadacza dowodu osobistego). Osoby, które chcą korzystać ze wskazanej funkcjonalności, powinny wyrazić taką wolę we wniosku o wydanie dowodu osobistego. Certyfikat podpisu osobistego zamieszcza się bowiem w warstwie elektronicznej dowodu osobistego osoby, która posiada pełną zdolność do czynności prawnych i przy składaniu wniosku o wydanie dowodu osobistego wyraziła zgodę na zamieszczenie tego certyfikatu. Możliwe jest również zamieszczenie certyfikatu w dowodzie osobistym osoby, która:

1) ukończyła 13. rok życia i przy składaniu wniosku o wydanie dowodu osobistego zgodę na zamieszczenie tego certyfikatu wyrazili jedno z rodziców, opiekun lub kurator tej osoby; w przypadku osoby, o której mowa w art. 25 ust. 3 ustawy *o dowodach osobistych*, zgodę na zamieszczenie certyfikatu podpisu osobistego wyraża ta osoba;
2) ukończyła 13. rok życia, jeżeli osoba ta przed upływem ważności dowodu osobistego wydawanego na okres 12 miesięcy osiągnie pełną zdolność do czynności prawnych, i przy składaniu wniosku o wydanie dowodu osobistego zgodę na zamieszczenie tego certyfikatu wyrazili jedno z rodziców, opiekun lub kurator tej osoby; w przypadku osoby, o której mowa w art. 25 ust. 3 ustawy o dowodach osobistych, zgodę na zamieszczenie certyfikatu podpisu osobistego wyraża ta osoba.

Natomiast opatrzenie danych podpisem osobistym wywołuje w stosunku do podmiotu publicznego skutek prawny równoważny podpisowi własnoręcznemu, natomiast w stosunku do podmiotu innego niż podmiot publiczny, jeżeli obie strony wyrażą na to zgodę.

Określone przepisy prawa stanowią o możliwości opatrzenia pisma konkretnym podpisem elektronicznym w zależności od rodzaju sprawy, przy czym należy mieć na uwadze, że –

[4] ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz.U. z 2022 r., poz. 671)

zgodnie z ustawą - Kodeks postępowania administracyjnego[5] – sprawy należy prowadzić i załatwiać na piśmie utrwalonym w postaci papierowej lub elektronicznej, a pisma utrwalone w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym lub kwalifikowaną pieczęcią elektroniczną organu administracji publicznej ze wskazaniem w treści pisma osoby opatrującej pismo pieczęcią. W związku z powyższym, kwestia wyboru stosowania podpisu osobistego do załatwiania określonych spraw pozostaje w gestii danego organu.

Jednocześnie informuję, że incydent, o którym mowa w niniejszej interpelacji dotyczył podmiotu prywatnego, z którym MSWiA nie współpracuje. Usługi podpisu elektronicznego dla MSWiA realizuje Polska Wytwórnia Papierów Wartościowych S.A. W 2024 r. koszt powyższej usługi, w przypadku MSWiA, wyniósł 12 686,87 zł.

Ad 10) Kiedy planowane jest przystosowanie systemów instytucji państwowych do obligatoryjnej weryfikacji warstwy elektronicznej e-dowodu, co miałoby na celu wyeliminowanie prób posługiwania się skradzionymi oraz sfałszowanymi dowodami osobistymi?

Ministerstwo Cyfryzacji, we współpracy z Centralnym Ośrodkiem Informatyki (COI), prowadzi obecnie prace analityczne dotyczące możliwości udostępnienia podmiotom zewnętrznym narzędzi (biblioteki SDK dla e-dowodu). Analiza obejmuje zarówno aspekty prawne, jak i techniczne.

Głównym celem tych działań jest zwiększenie bezpieczeństwa oraz eliminacja przypadków posługiwania się skradzionymi lub sfałszowanymi dowodami osobistymi. Dalsze decyzje w tej sprawie będą podejmowane we współpracy z właściwymi organami administracji publicznej.

Ad 11) Kiedy planowane jest obligatoryjne przystosowanie systemów medycznych do weryfikacji warstwy elektronicznej e-dowodu, co miałoby na celu uniemożliwienie kradzieży danych medycznych polskich obywateli oraz finansowe uszczelnienie systemu świadczeń zdrowotnych?

Z informacji uzyskanych z Ministerstwa Zdrowia wynika, że systemy medyczne typu HIS bądź systemy gabinetowe są zamawiane, utrzymywane i rozwijane przez podmioty i ich dostawców. Obecnie obowiązujące przepisy nie nakładają obowiązku korzystania z e-dowodu w celu dostępu do danych medycznych w placówce.

W ramach projektu pn. „Wprowadzenie nowoczesnych e-usług w podmiotach leczniczych", realizowanego ze środków POPC w latach 2018-2022, systemy szpitalne HIS zostały dostosowane do korzystania z warstwy elektronicznej e-dowodu (eDO) przez kadrę medyczną przy podpisywaniu dokumentów stanowiących elektroniczną dokumentację medyczną (EDM).

W 2019 r. rozważana była nieobligatoryjna zmiana wskazująca na wykorzystanie środka identyfikacji elektronicznej, w postaci e-dowodu, aplikacji mObywatel oraz mojeIKP, kart płatniczych wydawanych przez banki itp., w celu łatwiejszej i pewniejszej identyfikacji pacjenta. Zmiana nie doszła do skutku, ze względu na niską liczbę e-dowodów. Należy jednak zauważyć, że wspomniane rozwiązanie jest jedynie identyfikacją użytkownika, która nie jest w stanie skutecznie zabezpieczyć przed kradzieżą danych w rozumieniu ataku hakerskiego.

W 2023 r. Centrum e-Zdrowia (CeZ) podpisało z Centrum Personalizacji Dokumentów (CPD) umowę licencyjną na wykorzystanie biblioteki SDK (software development kit), dającej dostęp do warstwy elektronicznej dowodu osobistego. Jednakże, umowa

[5] art. 14 § 1a ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (Dz.U. z 2024 r., poz. 572)

licencyjna nie umożliwia przekazywania tej licencji do innych podmiotów, w tym komercyjnych, tworzących oprogramowanie dla podmiotów leczniczych.

Departament Innowacji (obecnie Departament e-Zdrowia) w Ministerstwie Zdrowia przy udziale przedstawicieli CPD i Polskiej Wytwórni Papierów Wartościowych (PWPW) zorganizował spotkanie z przedstawicielami producentów oprogramowania, zainteresowanymi wykorzystaniem uwierzytelnienia za pośrednictwem eDO w swoich aplikacjach. Przedstawiciele producentów oprogramowania, zgłosili szereg uwag, w tym:

- brak wsparcia PWPW w procesie wdrożenia i serwisu biblioteki SDK,
- scedowanie całej odpowiedzialności za błędy i awarie z wykorzystania biblioteki na producentów oprogramowania,
- niemożność przetestowania rozwiązania, z powodu braku środowiska testowego i testowych dowodów osobistych.

Z powodu braku stosownych uregulowań prawnych umożliwiających wdrożenie i wykorzystanie uwierzytelnienia za pośrednictwem eDO proces wdrażania nie mógł zostać rozpoczęty.

W związku z powyższym Ministerstwo Zdrowia zgłosiło następujące uwagi do projektu rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie warstwy elektronicznej dowodu osobistego:

- udostępnienie biblioteki dostępowej do warstwy elektronicznej Dowodu Osobistego umożliwiającej komunikację aplikacji z warstwa elektroniczną wszystkim podmiotom i w konsekwencji:
- określenie podmiotu udzielającego wsparcia technicznego integratorom wdrażającym wykorzystanie warstwy elektronicznej e-DO w swoich aplikacjach (np. Polskiej Wytwórni Papierów Wartościowych –producenta biblioteki SDK dostępowej do warstwy elektronicznej dowodu osobistego),
- określenie wymagań technicznych i sposobu pozyskania testowych dowodów osobistych z warstwa elektroniczną, niezbędnych do testowania w aplikacjach uwierzytelnienia za pomocą dowodu osobistego.

Warto podkreślić, że wdrożenie uwierzytelnienia za pośrednictwem eDO w aplikacjach podmiotów leczniczych przyśpieszyłoby proces informatyzacji podmiotów medycznych.

Ad 12) Kiedy planowane jest obligatoryjne przystosowanie systemów bankowych do weryfikacji warstwy elektronicznej e-dowodu, co miałoby na celu uniemożliwienie tworzenia fałszywych kont bankowych, prania pieniędzy, finansowania terroryzmu oraz powszechnego procederu wyłudzania środków finansowych na dane obywatela, którym została skradziona tożsamość?

Ministerstwa Finansów informuje, że nie brało udziału w tworzeniu przepisów dotyczących dowodów osobistych z warstwą elektroniczną. Od czasu wprowadzenia tego rodzaju dowodów, tj. od 4 marca 2019 r. do Ministerstwa Finansów nie wpłynęła żadna korespondencja od klientów banków świadcząca o występowaniu problemów ze stosowaniem e-dowodów przy zawieraniu umów bankowych. Ponadto Urząd Komisji Nadzoru Finansowego ani banki nie zgłaszały potrzeby zmiany przepisów w tym zakresie. Należy podkreślić, że banki świadczą szeroki wachlarz usług, podczas gdy pytanie dotyczy wyłącznie kwestii prowadzenia rachunków bankowych.

Warto także zauważyć, że na skutek ustawy o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości[6] w ustawie o usługach płatniczych[7]

[6] ustawa z dnia 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości (Dz. U. 2023 poz. 1394) (dalej: ustawa o zastrzeżeniu numeru PESEL)
[7] ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. 2024 poz. 30) (dalej: ustawa o usługach płatniczych)

został wprowadzony art. 4b, który zobowiązuje dostawców usług płatniczych do weryfikacji, czy numer PESEL konsumenta jest zastrzeżony przed: zawarciem umowy rachunku płatniczego, zawarciem umowy kredytu w rachunku płatniczym oraz zmianą umowy kredytu w rachunku płatniczym, w wyniku której następuje zwiększenie zadłużenia.

Ponadto wspomniany art. 4b ustawy o usługach płatniczych reguluje takie kwestie jak: zaspokojenia roszczenia ze strony dostawcy w stosunku do konsumenta i jego następców prawnych, weryfikacji zastrzeżenia oraz sytuację niedostępności systemu teleinformatycznego, w którym prowadzony jest rejestr zastrzeżeń numerów PESEL.

Zgodnie z uzasadnieniem ustawy o zastrzeżeniu numeru PESEL, ustawa miała za zadanie wprowadzenie rozwiązań zapobiegających zaciągnięciu na skradzione dane identyfikujące osobę różnego rodzaju zobowiązań w postaci np. kredytów i pożyczek oraz otwierania rachunków rozliczeniowych przeznaczonych do wykorzystania w działalności przestępczej. W przypadku zaciągnięcia powyższych zobowiązań lub podjęcia czynności pomimo zastrzeżonego numeru PESEL nastąpi zdjęcie odpowiedzialności za zobowiązania z osób, na rzecz których zostały zaciągnięte lub odmowa dokonania określonej czynności. Przyjęte rozwiązanie ma charakter prewencyjny oraz następczy. Dzięki ustawie możliwe będzie zapobieganie negatywnym skutkom kradzieży tożsamości (jeśli zaistnieją w przyszłości) lub zmniejszy ich uciążliwość (jeśli takie zdarzenie już nastąpiło). Zastrzeżenie będzie mogło być weryfikowane także przy okazji innych czynności prawnych - również przez osoby fizyczne przy użyciu dedykowanej e-usługi, natomiast brak możliwości domagania się zaspokojenia roszczenia znajdzie zastosowanie tylko w przypadkach wskazanych w przepisach szczególnych.

Zgodnie z art. 26 ustawy o zastrzeżeniu PESEL, dostawcy usług płatniczych (w tym również banki) mieli okres przejściowy na dostosowanie się do przedmiotowych przepisów do dnia 1 czerwca 2024 r.

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