Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.221.2026
Warszawa, 18 listopada 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 3 listopada br. Posła na Sejm RP Pana Bartłomieja Pejo w sprawie pilnego wdrożenia obligatoryjnego uwierzytelniania wieloskładnikowego (2FA/MFA) na państwowych platformach cyfrowych przetwarzających wrażliwe dane obywateli w związku z rosnącymi zagrożeniami cyberbezpieczeństwa (interpelacja nr 20668)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Czy Ministerstwo Cyfryzacji, wyciągając wnioski z niedawnego masowego wycieku danych z systemu MyDr, zamierza wprowadzić bezwzględny, odgórny zakaz stosowania logowania jednoetapowego na wszystkich państwowych platformach cyfrowych przetwarzających wrażliwe dane obywateli?

Obowiązek wieloskładnikowego uwierzytelniania przez podmioty kluczowe i podmioty ważne w ramach krajowego systemu cyberbezpieczeństwa wynika z obowiązków określonych w art. 8 ust. 1 pkt 2 lit. l oraz pkt 5 lit. a ustawy o krajowym systemie cyberbezpieczeństwa[1]. Stosowanie tych wymogów obowiązywać będzie od 3 kwietnia 2027 r. Niezależnie od tego Ministerstwo Cyfryzacji wielokrotnie zalecało stosowanie wieloskładnikowego uwierzytelniania, np. w rekomendacjach i komunikatach Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Ad 2) W jakim horyzoncie czasowym Ministerstwo Cyfryzacji, we współpracy z Ministerstwem Sprawiedliwości, wprowadzi obowiązkowe uwierzytelnianie dwuskładnikowe (2FA) w Portalu Informacyjnym Sądów Powszechnych, aby uniemożliwić przestępcom dostęp do akt sądowych po prostym przejęciu hasła użytkownika?

Obowiązek wieloskładnikowego uwierzytelniania przez podmioty kluczowe i podmioty ważne w ramach KSC wynika z obowiązków określonych w art. 8 ust. 1 pkt 2 lit. l oraz pkt 5 lit. a ustawy o KSC. Stosowanie tych wymogów obowiązywać będzie od 3 kwietnia 2027 r. Niezależnie od tego Ministerstwo Cyfryzacji wielokrotnie zalecało stosowanie wieloskładnikowego uwierzytelniania, np. w rekomendacjach i komunikatach Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Jednocześnie należy wskazać, że funkcjonowanie portalu reguluje ustawa Prawo o ustroju sądów powszechnych[2] oraz rozporządzenie Ministra Sprawiedliwości z dnia 20 lutego 2026 r. w sprawie portalu informacyjnego[3], jako organu właściwego w kwestii zarządzania tym systemem.

Ad 3) Jakie konkretne systemy zabezpieczeń są obecnie rekomendowane lub wdrażane przez resort w ramach zapowiadanego pakietu „CyberPiątka", aby państwowe platformy

[1] Art. 8 ust. 1 pkt 2 lit. l oraz pkt 5 lit. a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20 z późn. zm.), dalej: (ustawa o KSC)
[2] Art. 53e ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (Dz.U. z 2024 r. poz. 334 z późn. zm.)
[3] Dz.U. z 2026 r. poz. 216

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

ul. Królewska 27
00-060 Warszawa

posiadały spójne, zintegrowane mechanizmy ochronne oparte na biometrii lub powiadomieniach push w aplikacji mObywatel?

Planowane wykorzystanie aplikacji mObywatel i mojeIKP dotyczy powiadamiania pacjentów o zarejestrowanych zdarzeniach medycznych, a nie uwierzytelniania użytkowników tych platform.

W ramach przygotowywanego projektu przewidujemy natomiast rozwiązania służące wzmocnieniu ochrony danych osobowych i cyberbezpieczeństwa, w szczególności poprzez nałożenie dodatkowych obowiązków informacyjnych na podmioty przetwarzające dane osobowe na dużą skalę. Rozwiązania te mają zapewnić administratorom lepszy dostęp do informacji o stosowanych zabezpieczeniach, wynikach ich weryfikacji oraz zmianach mogących wpływać na bezpieczeństwo powierzonych danych. Projekt zakłada również wprowadzenie wymogu certyfikacji procesów zarządzania cyberbezpieczeństwem związanych z powierzonym przetwarzaniem dokumentacji medycznej.

Ponadto projekt przewiduje usprawnienie przekazywania do CSIRT NASK danych identyfikujących osoby, których dane osobowe zostały pozyskane lub ujawnione w sposób nieuprawniony w związku z incydentem lub cyberzagrożeniem. Rozwiązanie to ma umożliwić szybsze udostępnianie informacji w ramach usługi Bezpieczne Dane, tak aby osoby dotknięte naruszeniem mogły sprawdzić, czy dotyczyło ono ich danych, i odpowiednio wcześnie podjąć działania ograniczające jego skutki. W obszarze ochrony zdrowia przewiduje się również zwiększenie przejrzystości powierzania przetwarzania dokumentacji medycznej poprzez wprowadzenie dodatkowych obowiązków informacyjnych wobec pacjentów.

Ad 4) Czy Ministerstwo Cyfryzacji prowadzi obecnie audyt bezpieczeństwa wszystkich rządowych i resortowych portali pod kątem podatności na przejęcie kont z powodu braku zabezpieczeń 2FA /MFA, a jeśli tak – jakie są wnioski z tego audytu?

Obowiązek wieloskładnikowego uwierzytelniania przez podmioty kluczowe i podmioty ważne w ramach KSC wynika z obowiązków określonych w art. 8 ust. 1 pkt 2 lit. l oraz pkt 5 lit. a ustawy o KSC. Stosowanie tych wymogów obowiązywać będzie od 3 kwietnia 2027 r. Niezależnie od tego Ministerstwo Cyfryzacji wielokrotnie zalecało stosowanie wieloskładnikowego uwierzytelniania, np. w rekomendacjach i komunikatach Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Jednocześnie należy wskazać, że audyty bezpieczeństwa systemów informacyjnych są realizowane przez podmioty objęte ustawą o KSC, zgodnie z ciążącymi na nich obowiązkami (art. 15). Minister Cyfryzacji jako organ właściwy do spraw cyberbezpieczeństwa dla określonych w ustawie sektorów, nie zastępuje podmiotu w realizacji tych obowiązków, przy czym podmioty publiczne zostały włączone do KSC jako sektor objęty obowiązkami określonymi w art. 8 i 15 od czasu nowelizacji ustawy o KSC, która weszła w życie 3 kwietnia 2026 r., przy czym (zgodnie z powyższą informacją) podmioty te mają czas na wdrożenie wymogów ustawowych przez rok od wejścia w życie nowelizacji, czyli do 3 kwietnia 2027 r., a więc możliwość kontrolowania ich w zakresie realizacji obowiązków ustawowych będzie możliwa po 3 kwietnia 2027 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