

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

- **KOMISJI SAMORZĄDU TERYTORIALNEGO
I POLITYKI REGIONALNEJ
(NR 116)
z dnia 27 maja 2026 r.**

Pełny zapis przebiegu posiedzenia Komisji Samorządu Terytorialnego i Polityki Regionalnej (nr 116)

27 maja 2026 r.

Komisja Samorządu Terytorialnego i Polityki Regionalnej, obradująca pod przewodnictwem posła **Michała Krawczyka (KO)**, przewodniczącego Komisji, zrealizowała następujący porządek dzienny:

- informacja ministra cyfryzacji na temat stanu cyberbezpieczeństwa w jednostkach samorządu terytorialnego;
- informacja ministra cyfryzacji na temat obecnych i planowanych usług udostępnionych w cyfrowym portfelu mObywatel usprawniających współpracę jednostek samorządu terytorialnego z ich mieszkańcami.

W posiedzeniu udział wzięli: **Rafał Rosiński** podsekretarz stanu w Ministerstwie Cyfryzacji, **Sylwester Szczepaniak** koordynator do spraw społeczeństwa informacyjnego i smart city w Biurze Unii Metropolii Polskich im. Pawła Adamowicza, **Marek Wójcik** pełnomocnik zarządu Związku Miast Polskich.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Mateusz Daszewski** i **Sławomir Jakubczak** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł **Michał Krawczyk (KO)**:

Dzień dobry, witam państwa bardzo serdecznie.

Otwieram 116. posiedzenie Komisji Samorządu Terytorialnego i Polityki Regionalnej.

Witam panie posłanki, panów posłów, witam zaproszonych gości, witam pana ministra Rafała Rosińskiego, podsekretarza stanu w MC. Witam przedstawicieli samorządu terytorialnego – jest z nami pan Marek Wójcik, sekretarz Komisji Wspólnej Rządu i Samorządu Terytorialnego. Szanowni państwo, witam także pana Sylwestra Szczepaniaka, koordynatora do spraw społeczeństwa informacyjnego i smart city Unii Metropolii Polskich im. Pawła Adamowicza.

Stwierdzam kworum.

Przedmiotem dzisiejszego posiedzenia, zgodnie z przedstawionym porządkiem, będzie w punkcie pierwszym rozpatrzenie informacji ministra cyfryzacji na temat stanu cyberbezpieczeństwa w jednostkach samorządu terytorialnego i w punkcie drugim – rozpatrzenie informacji ministra cyfryzacji na temat obecnych i planowanych usług udostępnianych w cyfrowym portfelu mObywatel usprawniających współpracę jednostek samorządu terytorialnego z ich mieszkańcami. Czy są uwagi do porządku dziennego? Nie widzę. Stwierdzam jego przyjęcie.

Proponuję, abyśmy łącznie rozpatrzyli obydwa punkty. Bardzo proszę pana ministra o przedstawienie informacji.

A, przepraszam, jeszcze chciałem dwa słowa powiedzieć, bo dzisiaj szczególny dzień – Dzień Samorządu Terytorialnego. W związku z tym chciałem w imieniu całej Komisji – choć nie pytałem o to, ale czuję się upoważniony – podziękować wszystkim samorządowcom, pracownikom samorządowym tworzącym nasze wspólnoty samorządowe na wszystkich szczeblach samorządu. Chciałbym podziękować za ich codzienną pracę i za to, ile trudu wkładają w sprawne funkcjonowanie jednostek samorządu terytorialnego, i chciałbym życzyć dobrej współpracy z Komisją Samorządu Terytorialnego i Polityki Regionalnej i z rządem, w szczególności z MSWiA, bo wiemy, że to ministerstwo sprawuje główny nadzór nad jednostkami samorządu terytorialnego. Bardzo dziękujemy za waszą pracę, wszystkiego dobrego i również liczymy na dobrą współpracę.

Panie ministrze, oddaję głos. Bardzo proszę, jeszcze w sprawie Dnia Samorządu Terytorialnego.

Pełnomocnik zarządu Związku Miast Polskich Marek Wójcik:

Dziękuję serdecznie, panie przewodniczący.

Panie posłanki, panowie posłowie, panie ministrze, szanowni państwo, ja chciałem wnieść drobną poprawkę do życzeń pana przewodniczącego. Otóż chciałem, żebyście państwo czuli, że to jest także wasze święto, bo państwo jesteście Komisją, która gromadzi osoby życzliwe samorządom terytorialnym. Wielu spośród państwa w samorządach pracowało, ale nawet jeśli nie, to też tworzycie samorząd terytorialny i macie na to duży wpływ. Dlatego też proszę przyjąć życzenia w drugą stronę – ode mnie w imieniu Komisji Wspólnej Rządu i Samorządu Terytorialnego. Mamy nadzieję, że najbliższe miesiące przyniosą wiele dobrych rozwiązań w tym zakresie, czego państwu i sobie życzę. Dokładam do tych życzeń tradycyjne życzenia zdrowia i optymizmu. Dziękuję.

Przewodniczący poseł Michał Krawczyk (KO):

Bardzo dziękujemy.

I teraz oddajemy głos panu ministrowi. Bardzo proszę, panie ministrze.

Podsekretarz stanu w Ministerstwie Cyfryzacji Rafał Rosiński:

Panie przewodniczący, panie posłanki, panowie posłowie, szanowni państwo, oczywiście ja też się przyłączam do życzeń, skoro już tak sobie je składamy. Też byłem po tej stronie – po stronie samorządowej – i wiem, jak ona jest istotna. Myślę, że wszyscy patrzymy na to jako na cały ekosystem funkcjonowania struktur państwa.

Ale przechodząc już do meritum sprawy, czyli do informacji, która po pierwsze będzie mówiła o stanie cyberbezpieczeństwa z punktu widzenia JST, a po drugie – tak jak pan przewodniczący stwierdził – automatycznie omówię także drugi punkt, dotyczący pewnych funkcji dotyczących samorządów terytorialnych, jeżeli mówimy o aplikacji mObywatel. Najważniejsze rzeczy państwo otrzymali także w materiałach informacyjnych, spróbuję więc przedstawić to w sposób jak najbardziej zwięzły.

Przechodząc do punktu pierwszego, czyli do spraw związanych z cyberbezpieczeństwem – na początku, wprowadzając, mamy świadomość, że Polska jest krajem, który w największym stopniu doświadcza cyberataków, nawet w aspekcie międzynarodowym, w UE. Związane jest to także z naszym położeniem geopolitycznym. Biorąc pod uwagę statystyki, w 2025 r. było to ponad 270 tys. cyberincydentów, dla porównania – w 2024 r. ponad 111 tys., czyli wzrost o ponad 144%.

Obsługą tych cyberincydentów w Polsce zajmują się trzy zespoły CSIRT, czyli zespoły do spraw reagowania na cyberataki. Na poziomie krajowym mamy CSIRT w NASK, czyli w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym. On zajmuje się największą liczbą odnotowanych cyberincydentów – ponad 260 tys. Mamy także CSIRT GOV w ABW i CSIRT MON w MON.

Ale biorąc pod uwagę – bo myślę, że to jest także clou sprawy – jak to wyglądało w roku 2025 w ramach administracji samorządowej, w tym w jednostkach organizacyjnych, według CSIRT NASK, bo on zajmuje się rejestracją tychże incydentów, było w 2025 r. – 3249 takich incydentów cyberbezpieczeństwa, w 2024 r. ta ilość to było 2027, czyli jest wzrost ok. 60% rok do roku. Musimy mieć świadomość, że to są tylko te zgłoszone cyberincydenty. Oczywiście mogło być ich więcej, bo część samorządów terytorialnych mogła ich po prostu nie zgłaszać.

Co w związku z tym robimy? Jakie działania są podejmowane właśnie wobec samorządów terytorialnych i w zakresie współpracy JST w obszarze cyberbezpieczeństwa? Oczywiście nowelizowana jest ustawa o krajowym systemie cyberbezpieczeństwa, co jest pokłosiem wprowadzenia dyrektywy NIS2 i pewnych nowych obowiązków, które zostały także nałożone na samorządy terytorialne. Oczywiście w ramach współpracy – ja mam przyjemność także współprzewodniczyć Zespołowi ds. Społeczeństwa Informacyjnego – wypracowujemy wspólnie z samorządami terytorialnymi, z Komisją Wspólną Rządu i Samorządu Terytorialnego te rozmowy, dyskusje w ramach pewnych uregulowań, one jak najbardziej tutaj się odbywają. Nowe przepisy przewidywają możliwość zawierania porozumień i wspólnego wykonywania zadań z zakresu cyberbezpieczeństwa. Jeżeli mówimy o samorządach, samorządy mogą te zadania realizować wspólnie w formie prawnej, jaka będzie dla nich wygodna. Oznacza to, że możliwe będzie na przykład wyznaczenie jednostki odpowiedzialnej za realizację ustawowych obowiązków przez pozostałe jednostki samorządu terytorialnego, spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej. Czyli mogą być takie przypadki, że na przykład jedna jednostka

organizacyjna gminy będzie odpowiadała za obowiązki cyberbezpieczeństwa w pozostałych jednostkach organizacyjnych gminy.

I może przechodząc już konkretnie do określonych rozwiązań – planujemy już od czerwca tego roku powołać, a właściwie ogłaszamy konkurs na lokalne centra cyberbezpieczeństwa. I one właśnie są odpowiedzią m.in. na te przedstawione przeze mnie możliwości współpracy. Tę możliwość zapewnia nowe brzmienie art. 16e znowelizowanej tejże ustawy, który zapewnia podstawę do zawierania tychże porozumień w celu realizacji zadań związanych z cyberbezpieczeństwem.

Środki, które będą przeznaczone na ten projekt, na tworzenie tych lokalnych centrów cyberbezpieczeństwa, będą współfinansowane m.in. ze środków UE oraz z budżetu państwa w ramach programu „Fundusze Europejskie na Rozwój Cyfrowy” w latach 2021–2027. Zgodnie z aktualnymi założeniami programu FERC projekt utworzenia i rozwoju będzie mógł być realizowany do końca 2030 r. Do tego czasu centra, które powstaną w wyniku jego realizacji, powinny osiągnąć pełną zdolność operacyjną do skutecznej ochrony przed cyberatakami jednostek, które zostaną objęte tą działalnością.

Podstawowe informacje dotyczące naboru. Plan – koniec czerwca tego roku. Planowana łączna alokacja projektu to jest 270 mln zł. Zakładana liczba centrów, które powstaną w wyniku tego projektu, to jest 30. Tryb naboru – konkurencyjny konkurs wniosków o wsparcie dotacyjne. Okres projektu – lata 2026–2030. Trwałość projektu – pięć lat. Konkurs będzie prowadzony przez Centrum Projektów Polska Cyfrowa. Łączna wysokość dofinansowania – od 1 mln do 15 mln zł, uzależniona od liczby jednostek samorządowych objętych tymże projektem. W przypadku współpracy samorządów maksymalna wartość dofinansowania będzie wynosiła od 6 mln do 15 mln zł, w zależności od liczby samorządów wspólnie realizujących projekt.

Może teraz przejdę do obecnego wsparcia, bo to są oczywiście plany, które będą realizowane jeszcze w tym roku. Obecny projekt, który już funkcjonuje, to projekt grantowy „Cyberbezpieczny Samorząd”, współfinansowany ze środków UE i budżetu państwa także w ramach programu FERC. Łączna kwota grantów to ok. 1,5 mld zł. Z tego na dzień 22 maja bieżącego roku do JST trafiło już ponad 1,433 mld zł, czyli ponad 97% całości wsparcia, jakie mają otrzymać JST. Czyli można powiedzieć, że już w większości przypadków ten projekt został zrealizowany. Wnioski o granty można było składać od 19 lipca 2023 r. do 14 grudnia 2023 r. Obecnie w związku z licznymi wnioskami grantobiorców trwa proces zmiany dokumentacji naboru, którego celem jest wydłużenie okresu realizacji projektów grantowych do 30 września 2026 r. Dotychczas był to termin 30 czerwca 2026 r. Operatorem projektu jest Centrum Projektów Polska Cyfrowa, w partnerstwie z NASK-PIB.

Ministerstwo uruchomiło projekt „Cyberbezpieczny Samorząd”, aby samorządy wzmocniły swoją odporność m.in. na cyberzagrożenia. Jednostki samorządu otrzymują dofinansowanie w formie grantów w przedziale od 200 tys. zł do 850 tys. zł dla gmin oraz do 850 tys. zł dla powiatów i samorządów województw. Środki oczywiście związane były z poprawą ich cyberbezpieczeństwa. Są to m.in. audyty, wdrożenie lub aktualizacja polityki bezpieczeństwa informacji, mechanizmów, środków, które zwiększają odporność na ataki w cyberprzestrzeni.

Kolejnym projektem, który cieszył się także bardzo dużym zainteresowaniem, był projekt grantowy „Cyberbezpieczne Wodociągi”, współfinansowany ze środków KPO. W dniu 1 września 2025 r. uruchomiony został nabór wniosków do tego programu. Celem było wzmocnienie cyberodporności infrastruktury krytycznej właśnie w sektorze zbiorowego zaopatrzenia w wodę, który objęty jest krajowym systemem cyberbezpieczeństwa, w szczególności modernizacja systemów IT i OT, audyty bezpieczeństwa, szkolenia pracowników w tymże zakresie. Nabór wniosków w tym konkursie zakończył się 2 października 2025 r. W jego wyniku zostało złożonych 896 wniosków o dofinansowanie o łącznej wartości ponad 730 mln zł. Minimalna wartość grantu wynosiła 130 tys. zł, maksymalna była zależna od pomocy de minimis. Wnioski o granty składały zarówno gminy i jednostki organizacyjne, jak i spółki samorządowe. Zgłoszenia napłynęły ze wszystkich województw. Najwięcej wniosków w relacji do liczby gmin złożono w województwach: pomorskim – 54%, lubuskim – 51%, warmińsko-mazurskim – 50%, najmniej w podlaskim – 24% oraz łódzkim – 23%. W lutym tego roku zostały ogłoszone wyniki konkursu, opublikowano listę rankingową projektów wybranych do dofinansowania. W ramach konkursu pozytywnie oceniono 759 wniosków o łącznej wartości ponad 624 mln zł. Z podmiotami, których wnioski uzyskały pozytywną ocenę, zostaną podpisane umowy o powierzenie grantu. Na dzień 22 maja 2026 r. podpisano już 657 umów oraz zrealizowano 567 przelewów do grantobiorców na łączną kwotę 487 mln zł.

Projekty mogą być realizowane do 31 grudnia 2026 r., a alokacja projektu pozwoli objąć wsparciem wszystkie podmioty, które uzyskały pozytywną ocenę w naborze.

Biorąc pod uwagę sprawy dotyczące cyberbezpieczeństwa, niezmiennie istotną rzeczą są szkolenia organizowane dla samorządów terytorialnych. Ministerstwo Cyfryzacji prowadzi ogólnopolski program bezpłatnych szkoleń online z cyberbezpieczeństwa dla pracowników podmiotów KSC. Szkolenia realizowane są we współpracy z NASK i partnerami firm technologicznych w ramach tzw. programu „PWCyber”. Podnoszą świadomość, kompetencje, gotowość do reagowania na incydenty. Program będzie miał trzy poziomy szkoleń. Dla wszystkich – cyberhigiena, podstawy bezpieczeństwa. Dla kadry IT – obowiązki wynikające z ustawy, zgłaszanie incydentów, typowe zagrożenia i specjalistyczne warsztaty IT dotyczące podatności, reagowania, testów bezpieczeństwa.

No i program „SECURE” – program edukacyjny realizowany przez ministerstwo we współpracy z NASK. Są to szkolenia adresowane do włodarzy i osób odpowiedzialnych za cyberbezpieczeństwo w podmiotach administracji publicznej. W ramach realizacji projektu w 2026 r. przeprowadzony zostanie pilotaż budowy kompetencji trenerskich w zakresie cyberbezpieczeństwa. Celem pilotażu jest przygotowanie przedstawicieli do pełnienia roli lokalnych trenerów w zakresie podstaw cyberbezpieczeństwa. W ramach pilotażu zostaną przeszkoleni minimum dwaj przedstawiciele JST z każdego województwa. Szkolenia będą w małych, maksymalnie pięcioosobowych grupach.

Funkcjonuje także tzw. system zarządzania cyberbezpieczeństwem S46. Jego nazwa wynika z art. 46 znowelizowanej ustawy o Krajowym Systemie Cyberbezpieczeństwa. Jest to system teleinformatyczny, który wspiera zgłaszanie, obsługę incydentów, wymianę informacji, współpracę pomiędzy uczestnikami. System jest udostępniony JST wraz z integracją z moje.cert.pl. Nowelizacja ustawy wprowadziła obowiązkowe wykorzystanie przez większość podmiotów KSC, w tym JST, które są podmiotami KSC.

I ostatnia rzecz dotycząca tego punktu to platforma cyber.gov.pl – nowoczesna rządowa platforma stworzona z myślą o bezpieczeństwie cyfrowym obywateli, firm, instytucji publicznych. W jednym miejscu znajdują się wszystkie kluczowe usługi i narzędzia – od zgłaszania incydentów, przez monitorowanie zagrożeń, po dostęp do rozwiązań takich jak Artemis, czyli skanowanie podatności przez NASK, czy aplikacji moje.cert.pl. I oczywiście tę platformę jak najbardziej z powodzeniem mogą wykorzystywać JST.

Przejdę do punktu związanego z aplikacją mObywatel i funkcjami, które w związku z tym mogą wykorzystywać samorządy terytorialne. Jak wiemy, ponad 11 mln Polaków korzysta z tej aplikacji. Jesteśmy z niej jako MC, tu wspólnie oczywiście z COI, bardzo dumni. Mamy się czym pochwalić nie tylko na poziomie krajowym, ale i w skali międzynarodowej.

W ramach konsekwentnie realizowanej strategii cyfryzacji usług publicznych aplikacja obecnie, jeżeli mówimy o samorządach terytorialnych, oferuje rozwiązania dotyczące wdrażania m.in. własnych dokumentów elektronicznych, takich jak karty mieszkańca, lokalne karty rodzinne czy karty seniora, w sposób szybki, bezpieczny, maksymalnie uproszczony. Na ten moment skorzystały już m.in. duże samorządy, takie jak Wrocław, Bydgoszcz, czy takie miasta jak Zduńska Wola, Olecko czy Kobyłka. Proces przystąpienia do usługi został zaprojektowany tak, aby ograniczyć bariery formalne i technologiczne po stronie JST. Wniosek o uruchomienie usługi składany jest za pośrednictwem dedykowanego panelu współpracy, intuicyjnego także dla administracji samorządowej. Po zawarciu stosownego porozumienia, wdrożeniu niezbędnych zmian dokument może zostać udostępniony mieszkańcom bezpośrednio w aplikacji mObywatel z poziomu katalogu dostępnych usług i dokumentów, dzięki czemu obywatele otrzymują dostęp do odpowiednich funkcji. Szczególnie istotne jest to, że proponowane rozwiązanie nie wymaga od JST posiadania własnego, zaawansowanego zaplecza informatycznego ani budowy dedykowanych systemów teleinformatycznych. Udostępniamy bowiem kompletny interfejs administracyjny, umożliwiający zarówno ręczne wprowadzanie dokumentów dla poszczególnych użytkowników, jak i masowe zasilanie systemu danymi poprzez import zbiorczy. W praktyce oznacza to, że jest to rozwiązanie efektywne, skalowalne i niezwykle przystępne wdrożeniowo, zarówno z perspektywy mieszkańców korzystających z aplikacji, jak i administracji publicznej odpowiedzialnej za świadczenie usług.

Ponadto myślę, że także dość ważną i wygodną dla mieszkańców samorządów sprawą jest to, że w ponad 220 urzędach w całej Polsce dostępna jest usługa e-płatności w mObywatelu. Przez ostatnie lata ta usługa konsekwentnie się rozwijała, stając się jednym z ważniejszych narzędzi cyfrowych wspierających mieszkańców i administrację samorządową. Dzięki e-płatnościom

mieszkańcy ponad 200 samorządów mogą wygodnie i bez prowizji opłacać wybrane należności online – szybko, bez wizyty w urzędzie, bez ręcznego wpisywania danych. W e-płatnościach dostępne są najpopularniejsze metody płatności, zaczynając od Blika. Dziś można także płacić kartą oraz portfelami cyfrowymi, takimi jak Apple Pay czy Google Pay. W zależności od decyzji urzędu możliwe jest opłacanie podatku od nieruchomości, opłaty za gospodarowanie odpadami komunalnymi czy opłaty za posiadanie psa. Nasze rozwiązanie usprawnia pracę samych urzędów, ogranicza liczbę błędów, wspiera bezgotówkową obsługę mieszkańców. Oczywiście gorąco zachęcamy JST do korzystania z tego rozwiązania.

Kolejną funkcją w mObywatelu, którą niebawem chcemy już udostępnić w ramach tej aplikacji, jest dostęp do e-Doręczeń w mObywatelu. Usługa będzie wdrażana sukcesywnie, ze względu na technicznych na koniec czerwca planowane jest całkowite udostępnienie usługi e-Doręczeń w aplikacji.

Jednocześnie warto podkreślić, że aplikacja mObywatel obejmuje również funkcjonalność mDowodu, stanowiącego cyfrowy odpowiednik dokumentu tożsamości. W celu zapewnienia wygodnej i powszechnie dostępnej weryfikacji tożsamości udostępniony został także webowy mechanizm weryfikacyjny umożliwiający potwierdzenie autentyczności dokumentu bez konieczności instalowania aplikacji mObywatel przez podmiot lub osobę dokonującą weryfikacji. Rozwiązanie to znacząco zwiększa dostępność usług cyfrowych, wspiera budowę nowoczesnych standardów obsługi obywatela w administracji publicznej.

To, nad czym pracujemy, to są równolegle prowadzone intensywne prace związane z wdrożeniem europejskiego portfela tożsamości cyfrowej. Ostatnio m.in. odbywała się rozmowa w ramach zespołu społeczeństwa informacyjnego na ten temat, a dziś także zostały przyjęte przez Komisję Wspólną Rządu i Samorządu Terytorialnego pewne zapisy dotyczące tego rozwiązania. W najbliższych latach stanie się ono jednym z elementów europejskiego ekosystemu usług cyfrowych. Rozwiązanie to rozwijane jest w oparciu o unijne rozporządzenie eIDAS 2.0 i docelowo zostanie zintegrowane z aplikacją mObywatel, umożliwiając obywatelom korzystanie z jednolitego, uznanego w całej UE środka identyfikacji elektronicznej na poziomie wysokim, w tym z usług samorządów.

Europejski Portfel Tożsamości Cyfrowej ma stanowić znacznie więcej niż wyłącznie portfel cyfrowy. Jego celem jest stworzenie wspólnego, bezpiecznego środowiska umożliwiającego obywatelom potwierdzanie tożsamości, korzystanie z usług publicznych i komercyjnych, podpisywanie dokumentów elektronicznych oraz realizację usług transgranicznych w całej UE. Istotnym elementem będzie również możliwość wydawania i prezentowania poświadczeń atrybutów, czyli cyfrowych potwierdzeń określonych cech lub uprawnień użytkownika, przykładowo wieku, statusu studenta, prawa wykonywania zawodu czy posiadania określonych uprawnień, bez konieczności ujawniania pełnego zakresu danych osobowych. Projekt zakłada zastosowanie mechanizmu selektywnego przekazywania danych, dzięki któremu użytkownik będzie miał pełną kontrolę nad zakresem informacji udostępnianych poszczególnym usługom i podmiotom. Oznacza to odejście od modelu przekazywania całego dokumentu na rzecz nowoczesnego, atrybutowego podejścia, zgodnego z najwyższymi europejskimi standardami bezpieczeństwa, prywatności i interoperacyjności.

I na koniec warto podkreślić, że Polska już dziś aktywnie uczestniczy w europejskich projektach pilotażowych związanych z budową portfela tożsamości cyfrowej, a doświadczenia zdobyte przy rozwoju mObywatela stanowią istotny fundament dla dalszej integracji usług cyfrowych na poziomie europejskim. Docelowo rozwiązanie to ma stworzyć obywatelom możliwość wygodnego, bezpiecznego, powszechnie uznanego potwierdzania tożsamości zarówno w kontaktach z administracją publiczną, jak i sektorem prywatnym, nie tylko w Polsce, ale w całej UE.

Tak przedstawiają się informacje, jeżeli chodzi o te dwa punkty. Myślę, że niezwykle istotna jest przede wszystkim sprawa dotycząca cyberbezpieczeństwa i współpracy podsektora rządowego z podsektorem samorządowym, a także wszelkie udogodnienia, które przedstawiłem w punkcie drugim, i wyjście naprzeciw oczekiwaniom samorządów terytorialnych, jeżeli mówimy o aplikacji mObywatel, no i ten Europejski Portfel Tożsamości Cyfrowej, który ma być też pewną podstawą do realizacji pozostałych zadań czy swobodnego poruszania się i identyfikacji w całej UE. Dziękuję bardzo.

Przewodniczący poseł Michał Krawczyk (KO):

Bardzo dziękuję.

Otwieram dyskusję. Czy ktoś z państwa pragnie zabrać głos? Bardzo proszę, pan poseł Tomaszewski.

Posel Włodzimierz Tomaszewski (PiS):

Dziękuję bardzo.

Ja tutaj, w tym zestawie informacji, wyczytałem przykład, który bardzo mnie zaniepokoił, chociaż on może dotyczyć każdego obszaru, ale tu był wymieniony, więc w jakiejś większej skali występuje – że zarejestrowano w tej akcji podszywanie się i, że tak powiem, dochodzenie przez podmioty nieuprawnione do danych obywateli, jeśli chodzi także o dane związane z ich bardzo wrażliwymi informacjami. I jest podany taki przykład związany z łódzkim zoo, ponieważ w Łodzi jest taki stan, że podjęto taki proceder, tworząc Łódzką Organizację Turystyczną, która jest trochę odrębna od Polskiej Organizacji Turystycznej, że miasto w zasadzie tej Łódzkiej Organizacji Turystycznej oddaje wszystkie dane związane z kartą łódzianina, z wszystkimi danymi, które miasto gromadzi, związanymi z obywatelami. No i tamten podmiot zaczął tymi danymi handlować. No ale ten handel, jak widać, może mieć tak dalekie skutki, że nie tylko chodzi o to, że ktoś wysłał informację do obywateli, że oferuje jakąś usługę, ale będzie się podszywał – jak widzę tutaj – pod wyciąganie tych danych, które będą zmierzały do już takiej skrajnie patologicznej formy wyłudzenia informacji. Wymienione jest łódzkie zoo. Ja bym prosił o możliwość zapoznania się, jak dalece ten przykład jest szeroki, bo łączę to z tym faktem, że samo miasto, samorząd, oddaje swoje dane organizacji, niby zewnętrznej, chociaż miasto jest jednym z udziałowców tej Łódzkiej Organizacji Turystycznej, ale w zasadzie podaje na tacy materiał do oszustwa, do wyłudzeń – i to na wielką skalę.

Wiem, że ta sprawa jest badana przez prokuraturę, ona była już opisywana, ale opisywany był fakt, że ktoś wyłudza informacje, żeby handlować danymi, a tutaj może to prowadzić do gigantycznych strat tych ludzi, obywateli. No bo ktoś zgłasza się tam, podszywając się pod łódzkie zoo – czy tam to jest w ogóle w tej chwili taki holding zrobiony w Łodzi, więc to jest taka czapa. Te informacje są również łączone i agregowane. Dlatego prosiłbym o udostępnienie szerszych informacji, na czym ten przykład tutaj polegał. To zresztą jest przestroga dla innych samorządów, bo chęć zysku i handlowania danymi w tym wypadku może się skończyć właśnie takim – można powiedzieć – gigantycznym uderzeniem i stratami obywateli.

Przewodniczący poseł Michał Krawczyk (KO):

Bardzo dziękuję.

Bardzo proszę. Proszę o przedstawienie się.

Koordynator do spraw społeczeństwa informacyjnego i smart city w Biurze Unii Metropolii Polskich im. Pawła Adamowicza Sylwester Szczepaniak:

Sylwester Szczepaniak, Unia Metropolii Polskich.

Ja chciałbym się odnieść do wypowiedzi pana ministra. Z panem ministrem dość często się spotykamy i dyskutujemy. Proszę państwa, reprezentuję co prawda organizację zrzeszającą największe miasta – jest nas dwanaście – ale to, co będę mówił, będzie dotyczyło też mniejszych jednostek.

Jeżeli chodzi o tę informację, która została tutaj przedstawiona, to jest to mniej informacja o stanie cyberbezpieczeństwa w JST, ale bardziej o działaniach ministerstwa, żeby ten stan cyberbezpieczeństwa podnieść. Jeżeli interesują państwa informacje o stanie krajobrazu cyberbezpieczeństwa w Polsce, to mogę państwu powiedzieć to, co wiemy na poziomie naszych organizacji – dobrze nie jest. I nie jest dobrze, bo te działania, które robi ministerstwo, są nastawione na danie nam narzędzi, wspieranie nas, na przykład „Cyberbezpieczny Samorząd”, w oprzążowaniu, podniesieniu się z tego bardzo niskiego poziomu na poziom akceptowalny technicznie. My mamy największy problem z ekspertami. Jeżeli chodzi o duże miasta, ten problem jest podwójny, dlatego że w dużych miastach walczymy z jednej strony z sektorem przedsiębiorstw, a z drugiej strony – ja zawsze muszę to mówić, wiem, że MC jest na mnie źle – z administracją rządową. Administracja rządowa w poprzedniej kadencji stworzyła program wspierania cyberbezpieczeństwa w aspekcie osobowym, czyli Fundusz Cyberbezpieczeństwa, którym finansuje i zrównuje te stawki dla pracowników sektora rządowego, a my takiego funduszu nie mamy. I teraz osoba, która nawet ma jakieś poczucie misji publicznej, jeżeli ma do porównania pracę w administracji rządowej versus pracę w administracji samorządowej, gdzie różnica jest blisko 50% wynagrodzenia, zawsze wybierze administrację rządową – prawie zawsze – chociaż moi dyrektorzy IT cały czas dzielnie stoją na straży samorządu. I to jest największy problem obecnie, dlatego że niezależnie od tego, jakie my narzędzia kupimy i ile systemów zakupimy – czy będziemy

mieli SIEM, XDR, monitoring urządzeń końcowych – na końcu te wszystkie oprogramowania dają jakieś sygnały i te sygnały trzeba obsługiwać.

Jedyną drogą, którą widzimy – i tutaj bardzo duże znaczenie będzie miał ten program lokalnych centrów cyberbezpieczeństwa – jest konsolidowanie zasobów. I to się powoli dzieje. Mogę powiedzieć na przykładzie Unii Metropolii Polskich, że większość miast bardzo mocno dyskutuje nad powołaniem takiego lokalnego centrum cyberbezpieczeństwa, niezależnie od środków finansowych, bo po prostu to jest jedyna szansa, żeby skumulować środki techniczne, a w szczególności ludzkie, zabrać tych ludzi, którzy się tym zajmują, z jednostek organizacyjnych po to, żeby one w ramach CUW świadczyły usługi dla tych jednostek. Wtedy można – że się tak wyrażę – z budżetu samorządowego wyciągnąć więcej na wynagrodzenie.

Do tego też zmieniono ustawę samorządową w ramach ustawy o KSC, że teraz takim CUW może być też spółka komunalna, co do tej pory było niemożliwe. Dlaczego tak? Dlatego że w tych spółkach komunalnych mamy wodociągi, mamy infrastrukturę krytyczną, gdzie te podmioty, część z nich, już dzisiaj były do tej pory operatorami usług kluczowych w rozumieniu KSC. Tam już te kompetencje są, więc można tutaj znaleźć efekt synergii.

Jeżeli chodzi o mniejsze JST – tutaj trochę sobie będę uzurpował wypowiedzenie się za inne jednostki i organizacje – sprawa wygląda jeszcze gorzej, dlatego że te samorządy, które mają jednostki budżetowe, samorządowe zakłady budżetowe... Tam nawet nie ma co konsolidować i to jest bardzo duży problem. Dlatego jest taka inicjatywa w ramach działań samorządowców, trochę oddolna, nazywa się ISAC-JST, żeby przynajmniej się zrzeszyć i wymieniać informacjami, know-how, jak obsługiwać te incydenty. I tutaj ten ISAC się rozwija, to jest na zasadzie stowarzyszenia osobowego, być może się przekształci w jakieś bardziej twarde ciało.

Jeszcze tylko powiem, bo pan minister powiedział, że pracowaliśmy bardzo dużo nad tą ustawą, że myśmy w trakcie prac nad tą ustawą bardzo mocno podnosili ten problem, żeby można było zawierać porozumienia i dawać narzędzia w ramach tych porozumień, a z drugiej strony bardzo nie chcieliśmy, żeby wymogi dla tych najmniejszych jednostek organizacyjnych były zbyt duże. Dlatego te jednostki organizacyjne, które mają dzisiaj stosować KRI i tego nie robią – a mamy na to wymierny dowód w postaci kontroli NIK – nie robią tego, bo nie chcą albo nie wiedzą, że mają to robić. Dyrektor szkoły bardzo często nie wie, że ma KRI, bo ma komputery, salę gimnastyczną i pracowników. Albo nie są w stanie tego zrobić i dlatego będą stosować załącznik numer 4 do tej ustawy, który jest takim naprawdę minimum minimum. To jest – można powiedzieć – najniższy poziom bezpieczeństwa.

Jeżeli chodzi o kolejną rzecz z zakresu ustawy i cyberbezpieczeństwa, to proszę państwa, musimy pamiętać o tym, że tak naprawdę realnie możemy powiedzieć, czy ta ustawa coś zmieniła, za rok, bo do tej pory przepisy dotyczące obowiązków z zakresu cyberbezpieczeństwa były bardzo lakoniczne w tej ustawie i dla nas kluczowe było KRI, tylko że KRI nie było monitorowane, bo było monitorowane w ramach wewnętrznych audytów i te audyty nigdzie nie trafiały. Ta ustawa spowoduje, że te podmioty, które będą wchodziły w sektor ważny, czyli na przykład gospodarka odpadami, sektor kluczowy – czyli tutaj warto zaznaczyć: wszystkie starostwa, urzędy powyżej 50 pracowników oraz wybrane jednostki organizacyjne województwa – dopiero będą raportować. I dopiero zobaczymy, jaki ten stan cyberbezpieczeństwa jest, bo będą raportować nie tylko incydenty, ale też swoje audyty. Dzisiaj to jest strefa mroku. To, co pan minister przygotował, to jest to, co słusznie pan minister wskazał – trafia do CSIRT, a my wiemy, że większość organizacji, które obowiązywał dawny rozdział 5, nawet nie wiedziała, że coś takiego jak CSIRT istnieje i że mają tam cokolwiek zgłaszać. Więc my naprawdę podnosimy się z bardzo niskiego poziomu.

I teraz co zrobiła wojna w Ukrainie? To to, że wschodnia flanką jest dużo bardziej do tego przygotowana, bo już padała ofiarą ataków. JST, niezależnie od skali, te, które są bliżej rosyjskiego niedźwiedzia – że tak się wyrażę – już podejmowały te działania niezależnie, bo to ich po prostu bezpośrednio dotyczyło. Były ataki za pomocą sieci, ale były też ataki poprzez próby podłączania różnych urządzeń przez petentów, więc tam to poczucie potrzeby cyberbezpieczeństwa jest większe. W środku kraju, na zachodzie jeszcze aż tak mocno to nie wybrzmiewało. To jest moja część dotycząca cyberbezpieczeństwa.

Ja tylko chciałbym jeszcze się odnieść do jednej rzeczy, ostatniej z zakresu cyberbezpieczeństwa – skali, bo pan minister mówił o pieniądzach i środkach. To, czy pieniędzy jest wystarczająco, trzeba porównać do wydatków, które my ponosimy. O osobowych mówiłem, ale teraz przejdźmy sobie na wydatki czysto majątkowe dotyczące takiej prostej rzeczy jak antywirus.

Mówienie w kontekście cyberbezpieczeństwa o antywirusie jest trochę obrazą ludzi, którzy się zajmują cyberbezpieczeństwem, ale średni zakup antywirusa w samorządzie małym to jest 50 tys. zł, ale już jak wchodzimy na miasta średnie i większe, te, które już sobie skonsolidowały IT, to już idziemy w setki tysięcy złotych albo w przypadku moich miast – 3 mln zł. No i my dostajemy w naszych miastach 300 tys. z tych środków, więc tych środków zawsze będzie mało. I to, co ministerstwo wyciąga z systemu europejskiego, ja tak uważam, jest bardzo dobre, ale będzie potrzeba tego więcej. I my już dzisiaj mówimy, że mamy do 2030 r. Musimy zacząć myśleć, co zrobimy po 2030 r., kiedy te licencje, subskrypcje, sprzęt wygasną. Musimy już myśleć, planować, już szukać w tym nowym modelu finansowania europejskiego, jak nas zabezpieczyć po 2030 r. Doświadczenia ze wszystkimi systemami pokazują, że to jest bliżej, niż nam się wszystkim wydaje.

To, jeżeli chodzi o cyberbezpieczeństwo. Nie wiem, czy mam się teraz odnosić do mObywatela, czy po prostu w drugiej części. Jeżeli chodzi o mObywatela, to chciałbym państwu powiedzieć, że to, co mogę potwierdzić, to to, co powiedział pan minister. Dodałbym tylko dwie rzeczy.

Idzie bardzo wielka rewolucja. Ta rewolucja nazywa się Europejski Portfel Tożsamości Cyfrowej i ta rewolucja... Dlatego ostatnio bardzo długo dyskutowałem z przedstawicielami MC. MC dzisiaj nastawia się na wprowadzenie tego Europejskiego Portfela Tożsamości Cyfrowej. On ma być na grudzień i on musi być. To będzie klęska wizerunkowa Polski, jak my tego nie zrobimy na grudzień. I ja rozumiem tę filozofię. Wszystkie zastrzeżenia samorządów, że my nie wiemy jak, my nie wiemy z czym, trzeba dostosować systemy, są przedmiotem dalszej troski resortu. Jesteśmy umówieni i dlatego tutaj o tym mówię. Na Komisji Wspólnej Rządu i Samorządu Terytorialnego dzisiaj oficjalnie padło stanowisko, że my wydaliśmy opinię pozytywną do tego projektu Europejskiego Portfela Tożsamości Cyfrowej, który ma być tym mObywatelom 3.0, ale pod warunkiem, że przystąpimy niezwłocznie do prac nad przygotowaniem całego ekosystemu do uznawania tego portfela, bo tam wchodzi kwestie organizacyjne, dostosowania rejestrów centralnych i naszych, dostosowania przepisów prawa proceduralnego, bo te dokumenty naprawdę będą zrównane z dokumentami papierowymi. A wiecie państwo, jak wygląda dokumentacja wewnętrzna w samorządach – nadal dominuje papier. Dodatkowo musimy dostosować, musimy zrobić inwestycje, bo ten nowy europejski portfel wymaga od nas podjęcia inwestycji, czyli zaimplementowania tych protokołów, które tam wchodzi, uznawania tych standardów technicznych, które tam są. I to jest wyzwanie, które przed nami stoi w 2026 i 2027 r., bo do 2027 r. mamy być już gotowi. I to jest coś, co warto, żeby państwo tutaj... Nie mogę nic sugerować panom posłom i paniom posłankom, ale ten projekt będzie stał prawdopodobnie na Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii. Warto, żeby przedstawiciele Komisji Samorządu Terytorialnego i Polityki Regionalnej w tych pracach uczestniczyli, bo tam będą wychodziły kwestie czysto samorządowe, nie tylko systemowe. Dziękuję bardzo.

Przewodniczący poseł Michał Krawczyk (KO):

Bardzo dziękuję.

Bardzo proszę, pan Marek Wójcik.

Pełnomocnik zarządu Związku Miast Polskich Marek Wójcik:

Marek Wójcik, Związek Miast Polskich. Dziękuję, panie przewodniczący, za udzielenie głosu.

Ja chcę bardzo krótko powiedzieć o kilku kwestiach, które znalazły się w tym sprawozdaniu. Po pierwsze, dziękujemy za program „Cyberbezpieczny Samorząd”. Gorąco prosimy o to, żeby podczas prac nad programowaniem kolejnego okresu w UE – 2028-2034 – spróbować upomnieć się o pieniądze na tego typu przedsięwzięcia. Tam jest prawie 1,5 mld zł. Bardzo dziękujemy. To jest dobry program, bardzo nam pomaga.

Druga sprawa. Jeżeli chodzi o rozwiązania prawne, które są przed nami, te, które dotyczą różnych regulacji wprowadzających dokumenty cyfrowe – to jest kierunek oczywisty, ale prośba o rozważenie, czy przypadkiem niektóre dokumenty jednak nie powinny być także dublowane papierowo. Mówię to na przykładzie także doświadczeń z wojny na Ukrainie. Tak więc przed nami zmiany dotyczące prawa jazdy, dowodów rejestracyjnych, ale zwróćcie państwo uwagę, jak gigantyczne były problemy w sektorze medycznym w pozyskiwaniu chociażby dokumentów, które, jeżeli były tylko w rejestrze elektronicznym, to w momencie, kiedy te narzędzia były objęte atakami Rosjan, wówczas była pustka, opieraliśmy się na różnego rodzaju oświadczeniach. Tak samo tutaj – prośba o rozważenie, bo jeszcze raz powtórzę: oczywista jest kwestia, że zmierzamy w kierunku cyfryzacji, to jest jasne, ale być może niektórym dokumentom dotyczącym tożsamości, niektórych uprawnień warto się przyjrzeć.

Trzecia sprawa to kwestia infrastruktury krytycznej i pewnych rozwiązań prawnych, które wprost, na tacy, dają naszym przeciwnikom informacje, których moim zdaniem mieć nie powinni. Żeby nie być gołosłownym – pan minister w tym sprawozdaniu zawarł elementy dotyczące sieci wodno-kanalizacyjnych. Drodzy państwo, mamy projekty ustaw, które wprost zobowiązują nas do przedkładania pełnej informacji o wszystkich ujęciach wody i raportowania tego w BIP. Czyli dajemy gotową informację. To jest tylko jeden z przykładów. Tak więc prosba, żeby rozważyć taki monitoring ustawodawczy, który już obowiązuje w stosunku do infrastruktury krytycznej, ale także tej, która będzie się pojawiała, pod kątem ograniczenia tego typu informacji jako informacji ogólnodostępnej. Może dostępnej dla określonych podmiotów, przy pewnym utrudnieniu, ale tu dajemy to na tacy przeciwnikom. A z tą wodą to jest taki bardzo mocno przemawiający argument.

Czwarta rzecz – bardzo pozytywnie oceniam propozycję resortu dotyczącą lokalnych centrów cyberbezpieczeństwa, natomiast prosba o rozważenie, żeby te centra mogły wykraczać poza pojedynczą gminę. Dzisiaj mówimy o tym, że jednostki wewnątrz gminy itd. – to jest dobra propozycja, bardzo dobra propozycja. Musimy szukać różnych form poprawy efektywności działania także administracji i wydaje mi się, że mniejsze samorządy nie utworzą takich centrów. Będą miały duży problem, ale jeżeli będą to robiły wspólnie, to może będzie łatwiej. Tu rozumiem, że państwo przewidujecie jakieś wsparcie finansowe dla takich centrów. Jeżeli tak, to prosba o rozważenie, w różnych formach działania, także współpracy już istniejącej – wracam do tej wody – jeżeli są spółki, które obsługują czy w ramach różnych porozumień między samorządami realizują te zadania, to wydaje mi się, że powinny być, bez względu na zakres terytorialny, objęte tego typu wsparciem.

I wreszcie piąta, ostatnia sprawa, która dotyczy – pan minister o tym wspomniał przy okazji europejskiego portfela cyfrowego – tego, że tam, przynajmniej na razie, ja nie widzę takiej pełnej możliwości ujmowania w tych portfelach naszych danych lokalnych, tak nazwę to może w uproszczeniu. Tak więc jeżeli my mamy jakąś własną kartę mieszkańca – z tego co wiem, to chyba wypadają także legitymacje szkolne itd. – chodzi o to, żeby również tego typu dane mogły się w tych portfelach znaleźć. Korzystając z okazji, że pan minister wspomniał o tym portfelu, ośmielam się o tym powiedzieć. Bardzo dziękuję, że państwo podjęliście ten temat. I tu dziękuję też resortowi za zaangażowanie w to przedsięwzięcie. My czujemy to wsparcie i tę współpracę, o której mówił pan Sylwester, prowadzimy na bieżąco. Dziękuję bardzo.

Przewodniczący poseł Michał Krawczyk (KO):

Bardzo dziękuję.

Jeszcze o głos prosił pan Sylwester Szczepaniak. Bardzo proszę.

Koordynator do spraw społeczeństwa informacyjnego i smart city w Biurze Unii Metropolii Polskich im. Pawła Adamowicza Sylwester Szczepaniak:

Tak, tylko ad vocem. Te lokalne centra cyberbezpieczeństwa – tu było robocze spotkanie na ZSI. Właśnie tutaj mamy pewien konflikt interesów między jednostkami, dlatego że ministerstwo, z tego co wiem – i ten stan chyba nie uległ zmianie – kładzie nacisk na to, że te lokalne centra muszą być tylko i wyłącznie tworzone w ramach porozumień. No i tutaj właśnie my jako na przykład duże miasta trochę stoimy w opozycji do tego pomysłu jako jedynego kryterium. Bo jeżeli mamy powiat, który dogada się z mniejszymi samorządami – gminami lub innymi powiatami – albo grupa gmin się ze sobą skomunikuje i stworzą takie lokalne centrum cyberbezpieczeństwa, to oczywiście taka możliwość powinna być. Ale na przykład u nas, w naszych dużych miastach, naszymi takimi mniejszymi jednostkami jest 40, 80, 100 jednostek organizacyjnych i my chcielibyśmy wtedy też z tych pieniędzy trochę skorzystać, a dopiero w dalszej części myślimy o tym, żeby rozszerzyć się na gminy ościenne, na układy metropolitalne. Wiem, że ministerstwo w ramach dyskusji analizuje ten nasz pomysł. Tam jeszcze województwa podniosły ten temat, bo też województwa dostarczają pewne usługi dla JST, więc ta układanka jest dość skomplikowana, żeby tę małą kołderkę mimo wszystko jakoś sprawiedliwie rozdzielić. Te pomysły na ostatnim ZSI, chyba dwa miesiące temu były podniesione, i dlatego tak tylko chciałem ad vocem zaznaczyć, że ten temat jeszcze nie jest do końca zamknięty. Pierwotny pomysł resortu był chyba taki, żeby były tylko porozumienia.

Przewodniczący poseł Michał Krawczyk (KO):

Bardzo dziękuję.

Nie widzę więcej zgłoszeń. Ja sobie jeszcze pozwolę, panie ministrze, kilka krótkich kwestii poruszyć. Przedstawiciel Unii Metropolii Polskich mówił o tym, że – jeśli dobrze zrozumiałem – Polska Wschodnia jest lepiej przygotowana na ataki ze względu na bliskość granicy i doświadczenia. I w tym kontekście chciałem zapytać, czy jeśli mamy zidentyfikowanych w 2025 r. ponad 272 tys. incydentów, to czy jest różnica, jeśli chodzi o skalę tych incydentów, w stosunku do wielkości samorządów i też położenia geograficznego? Czy mamy taką wiedzę? Czy pan minister ma taką wiedzę? Czy wielkość samorządu też wpływa na tą skalę incydentów i czy to bardziej dotyczy właśnie dużych samorządów? Bo przypuszczam, że tak, ale chciałbym to wiedzieć. I czy to jest też związane z położeniem geograficznym? Chciałbym też zapytać o to słowo, że są „identyfikowane”, że „CSIRT identyfikuje”. „Identyfikuje” – to, rozumiem, że zostały zgłoszone przez samorządy. W ten sposób należy tę identyfikację rozumieć. A proszę powiedzieć, czy szacujecie państwo w jakikolwiek sposób pełną skalę incydentów, które mogły mieć miejsce w 2025 r.? Bo wiemy, ile jest tych zidentyfikowanych, a ile ich mogło być wszystkich? Czy to jest w ogóle do oszacowania? Bo ciekaw też jestem, jakie to mogą być liczby, bo przypuszczam, że są wielokrotnie większe.

I chciałbym jeszcze zapytać o kwestię europejskiego portfela i tego, jak on się będzie miał do mObywatela, bo my nie byliśmy zaznajamiani z tym rozwiązaniem informatycznym. Ja o nim słyszałem przy okazji wykorzystywania go do identyfikacji osób zakładających swoje konto na profilach społecznościowych i tej ustawy, nad którą pracujemy, z ograniczeniem wieku i możliwości sprawdzenia i weryfikacji tego wieku. Proszę powiedzieć, jak ten portfel cyfrowy będzie funkcjonował. Czy to będzie kolejna aplikacja, czy to będzie po prostu jakieś rozwiązanie informatyczne powiązane z mObywatelą? To mnie interesuje. I tyle, bardzo dziękuję.

Podsekretarz stanu w MC Rafał Rosiński:

Ja na początku oczywiście chciałbym serdecznie podziękować, bo nie powiedziałem tego na początku, ale oczywiście stronie samorządowej. Tu pan Sylwester mocno bierze udział w różnych formach współpracy samorządów i w Zespole ds. Społeczeństwa Informacyjnego. I tu wymieniamy się informacjami. Z punktu widzenia tej ustawy, która faktycznie została już docelowo uchwalona, ten wkład samorządów terytorialnych był tak naprawdę nieodzowny. To był bardzo duży wkład, te prace, to porozumienie, myśl, że cyberbezpieczeństwo jest ważne dla całego ekosystemu. Dlatego ten głos samorządów jak najbardziej bierzemy pod uwagę i zawsze konsultujemy, żeby każdy w jakiś sposób czuł się w tym dobrze i nie był pokrzywdzony.

Oczywiście wyzwania są duże. Ja jeszcze tak ad vocem ogólnie się odniosę. Te środki na cyberbezpieczeństwo, które są przeznaczone, ja mam takie całościowe kwoty, to dopowiem, bo tego nie mówiłem w sprawozdaniu. W 2025 r. było to ok. 4 mld zł, tylko w 2026 r. 5 mld zł, czyli ogromne środki, oczywiście z budżetu państwa i ze środków unijnych.

To prawda, co pan Sylwester tutaj wspominał odnośnie do Funduszu Cyberbezpieczeństwa i tego wynagrodzenia dla tych osób. Tego nie ma dla samorządów, ale tu, jeżeli mówimy o konkurencyjnym wynagradzaniu specjalistów, to była przeznaczona kwota w 2026 r. 365 mln zł, jeżeli chodzi o ponad 200 instytucji publicznych. Tu mówimy o tej konkurencyjności, jeżeli chodzi o wynagrodzenia, żeby te osoby, które dbają o bezpieczeństwo na tym szczeblu państwowym, także chciały oczywiście w tych instytucjach pracować.

Dobrze. I odnosząc się już do pytań pana przewodniczącego, jeżeli chodzi o położenie geograficzne, ilość cyberincydentów i zależność od tego, czy mamy do czynienia ze ścianą wschodnią czy zachodnią – ja na ten moment nie posiadam tych szczegółowych informacji, ale jeżeli one są, bo NASK takie statystyki prowadzi, to myślę, że jeżeli będzie taka wola, nie ma problemu, żeby taką statystykę także udostępnić.

Jeżeli chodzi o informację dotyczącą tych realnych, zgłoszonych cyberincydentów, zanotowanych głównie w dużej mierze przez CSIRT NASK – tam ponad 260 tys. – a te pozostałe przez CSIRT GOV i MON, to trudno nam tak naprawdę oszacować liczbę niezgłoszonych. Takich danych ja nie posiadam i nie wiem, czy NASK też ewentualnie to szacuje.

Ta nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa... Wcześniej także ustawa przed nowelizacją nakładała obowiązek zgłaszania tych cyberincydentów, ale nie było w związku z tym kar. Ta nowa ustawa wprowadza kary za niezgłaszanie tychże cyberincydentów.

Ta świadomość przede wszystkim samorządów terytorialnych w tym przypadku powinna być jak najbardziej – myślimy – większa.

Ta współpraca, jeśli chodzi o lokalne centra cyberbezpieczeństwa, jeszcze wracając do tego, faktycznie zakłada, że co najmniej dwie jednostki samorządu terytorialnego muszą być, żeby zostały utworzone. Tworzą się spotkania, zainteresowanie ze strony samorządów terytorialnych co do szczegółów i my także ze swojej strony udzielamy takich informacji. Te spotkania się odbywają, bo zainteresowanie jest. Jak na razie – tak jak powiedziałem – 30 takich lokalnych centrów cyberbezpieczeństwa ma powstać.

Odnosząc się do pytania dotyczącego Europejskiego Portfela Tożsamości Cyfrowej – jakie jest założenie, jakie jest podejście MC. Aplikacja mObywatel będzie funkcjonować nadal i będzie miała te wszystkie funkcje, które mamy. I jak na razie w 2027 r. założenie jest takie, że obok aplikacji mObywatel ma funkcjonować ta aplikacja EUDI, czyli w ramach Europejskiego Portfela Tożsamości Cyfrowej. I docelowo ma być ona włączona w funkcje, połączona z mObywatel, czyli na przykład z poziomu mObywatela będziemy mogli przejść do tej aplikacji EUDI. Czyli to jest, jeżeli chodzi o takie techniczne rozwiązanie, zakres podejścia do tego europejskiego portfela tożsamości. 24 grudnia tego roku jest planowane faktycznie wdrożenie. Pracujemy nad tym. Jest to dla nas także duże – i jak pan Sylwester wspomniał – priorytetowe i ważne wyzwanie, bo pokazujemy się jako taki lider w tym zakresie cyfrowych rozwiązań, także e-usług publicznych, i naprawdę nie mamy się czego wstydzić. Pracujemy nad tym i te wszystkie spotkania służą m.in. temu, aby tych błędów czy jakichś niedoskonałości było jak najmniej. Dziękuję.

Przewodniczący poseł Michał Krawczyk (KO):

Proszę mi powiedzieć, czyli europejski portfel tożsamości będzie służył tylko do potwierdzania tożsamości?

Podsekretarz stanu w MC Rafał Rosiński:

Nie, nie tylko do potwierdzania.

Przewodniczący poseł Michał Krawczyk (KO):

To co tam będzie?

Podsekretarz stanu w MC Rafał Rosiński:

Miedzy innymi dzięki temu europejskiemu portfelowi tożsamości będziemy mogli zidentyfikować się tak, jak identyfikujemy się mObywatel, w innych krajach UE. Czyli poruszać się – można powiedzieć – bez dokumentu plastikowego. W tym momencie, kiedy jesteśmy, nie wiem, w Niemczech, na Słowacji, no to mObywatel tam nie funkcjonuje, bo tu chodzi o wymianę tychże danych. Ale ponadto – to pan przewodniczący także wspomniał – ma służyć jako też taka platforma czy aplikacja, która ma udostępniać selektywne dane przy ochronie danych osobowych, na przykład przy dostępie do – to, co chcemy wprowadzić – określonych mediów społecznościowych. Bo na ten moment nie chcemy wykorzystywać do tego mObywatela, tylko właśnie tę aplikację EUDI.

Przewodniczący poseł Michał Krawczyk (KO):

I rozumiem, że rozwiązania europejskie i regulacje europejskie są i teraz jesteśmy na etapie wdrażania ich w poszczególnych krajach?

Podsekretarz stanu w MC Rafał Rosiński:

Tak, one będą wdrażane. To jest – można powiedzieć – na chwilę obecną tylko taki szkielet, a my po prostu to wszystko dostosowujemy. To znaczy nie wszystkie kraje jednocześnie w 2027 r. oczywiście to wdrożą. My chcemy być liderem i tutaj pokazać, że można.

Przewodniczący poseł Michał Krawczyk (KO):

Dziękuję.

Bardzo proszę.

Koordynator do spraw społeczeństwa informacyjnego i smart city w Biurze Unii Metropolii Polskich im. Pawła Adamowicza Sylwester Szczepaniak:

Ja, uzupełniając, jeśli chodzi o europejski portfel tożsamości z punktu widzenia samorządów. Tak jak pan minister wskazał, ma on funkcjonować od 24 grudnia i z czasem będzie przejmował z mObywatela potwierdzenie tożsamości. Ale z drugiej strony obywatele zyskają na przykład

możliwość składania podpisów kwalifikowanych, z ich punktu widzenia za darmo – mówię: obywatele, nie przedsiębiorcy, bo tam jest zastrzeżenie – do administracji.

Po drugie, w tym portfelu my też jako samorządy będziemy mogli wydawać nasze atrybuty. Atrybut to jest taka nowa instytucja prawna. Atrybut to jest moje prawo albo prawo do rzeczy, które będzie miało postać cyfrową, zestandaryzowaną na poziomie europejskim – to według tych samych protokołów ma działać – i te dokumenty będą uznawane tak samo jak papierowe, bo tego wymaga akt prawa europejskiego. W związku z tym troszkę się zmieni sposób świadczenia usług, bo my domyślnie, już tworząc usługi na poziomie lokalnym czy administracja rządowa na poziomie centralnym, będziemy te usługi robić już pod wykorzystanie tego europejskiego portfela tożsamości. Czyli na przykład nie będziemy pytać w przyszłości o pełen zestaw danych, jeżeli nie są nam potrzebne, tylko – czy jesteś mieszkańcem. Ja jako obywatel mam w swoim polskim portfelu tożsamości informację, że mam taki adres zamieszkania, ale dla usługi nie jest potrzebna ta dana. Wystarczy, że z portfela przyjdzie na podstawie tych danych informacja – tak, jestem mieszkańcem – i usługa już będzie ufała portfelowi. Zmienia się trochę sposób organizacji, dlatego – tak jak powiedziałem w tej pierwszej części – o ile nikt nie kwestionuje tego europejskiego portfela tożsamości na poziomie samorządowym, my temu kibicujemy, sami szukamy tam swoich szans na rozwój, o tyle wiemy, ile trzeba pracy wykonać po stronie naszej administracji, żeby to zadziałało w pełni. I dlaczego to tak podnosimy? Dlatego że jesteśmy trochę ofiarą własnego sukcesu. mObywatel okazał się sukcesem i tak jak państwo posłowie, tak jak inni ludzie wymagamy od tego, żeby to narzędzie dawało nam coraz więcej. Mieszkańcy się nauczyli, chcą z tego korzystać. No i w tym momencie my jako administracja samorządowa nie możemy powiedzieć – no fajnie, że macie taką funkcjonalność, ale my nie jesteśmy w stanie jej obsłużyć. Tak więc my musimy się dostosować wewnętrznie – nasze systemy, rejestry – do tego. To jest duża praca i mamy na to rok. To nie jest dużo czasu i tutaj MC musi nas wspierać także regulacyjnie, bo pewnie będą rzeczy, które musimy prawnie dostosować. To tak chciałem uzupełnić moją wypowiedź, żeby nie zabrzmiało, że jesteśmy przeciwnikami tego narzędzia.

Przewodniczący poseł Michał Krawczyk (KO):

Jasne.

A jeszcze chciałem jedną rzecz dopytać. Czyli rozumiem, że ten europejski portfel cyfrowy będzie dostępny też dla osób niepełnoletnich, po to, żeby mogły chociażby, zakładając konto na portalu społecznościowym, być zweryfikowane pod kątem wieku, tak?

Podsekretarz stanu w MC Rafał Rosiński:

Tak, tak samo jak mamy mObywatel Junior, czyli też aplikację. Czyli tu do weryfikacji jak najbardziej. Bo jak wiemy, jeżeli mówimy o weryfikacji wieku, to – bo to jest ta rozmowa, która musi także wybrzmieć, bo często może publicznie nie jest to do końca jasno powiedziane – w tym momencie każdy będzie musiał się weryfikować, czyli osoba dorosła także.

Przewodniczący poseł Michał Krawczyk (KO):

A gdzie się weryfikować? A, w social mediach.

Podsekretarz stanu w MC Rafał Rosiński:

Tak.

Przewodniczący poseł Michał Krawczyk (KO):

Nie widzę więcej pytań, zgłoszeń w dyskusji.

Bardzo dziękujemy, panie ministrze. Bardzo dziękujemy naszym gościom za bardzo interesującą dyskusję. Bardzo dziękuję.