Ministerstwo
Cyfryzacji

Podsekretarz Stanu
Paweł Lewandowski

BPC.WIOC.4613.4.2023
Warszawa, 26 czerwca 2023 r.

Pan
Tomasz Grodzki
Marszałek Senatu RP

Dot. pisma z 16 maja br. w sprawie oświadczenia złożonego przez Senatora RP Pana Stanisława Lamczyka, podczas 62. posiedzenia Senatu RP (BPS/043-62-2171/23).

Szanowny Panie Marszałku,

poniżej przekazuję odpowiedzi na Pana Senatora pytania.

Co z programem cyfryzacji dla Polski?

W Polsce, program cyfryzacji został wprowadzony w celu rozwijania i modernizacji sektora technologii informacyjno-komunikacyjnych oraz poprawy dostępu obywateli i firm do usług cyfrowych. W ramach tego programu, polski rząd podjął wiele inicjatyw mających na celu wspieranie rozwoju cyfryzacji w kraju. Oto kilka ważnych obszarów objętych programem cyfryzacji:

1. Infrastruktura szerokopasmowa: Rząd dążył do zapewnienia dostępu do szybkiego Internetu na terenach wiejskich i w mniejszych miejscowościach, poprzez inwestycje w rozwój infrastruktury szerokopasmowej.
2. E-usługi dla obywateli: Program cyfryzacji obejmował rozwój elektronicznych usług dla obywateli, takich jak e-zdrowie (elektroniczne akta medyczne, telemedycyna), e-szkolnictwo (platformy edukacyjne, cyfrowe materiały edukacyjne) oraz e-administracja (elektroniczne usługi publiczne, elektroniczne składanie dokumentów).
3. Cyfrowa gospodarka: Polska starała się rozwijać cyfrową gospodarkę poprzez wspieranie innowacji, start-upów i przedsiębiorczości w sektorze technologii informacyjno-komunikacyjnych. Program obejmował również szkolenia i wsparcie dla przedsiębiorców w zakresie wykorzystania technologii cyfrowych.
4. Bezpieczeństwo cybernetyczne: W ramach programu, Polska dążyła do wzmocnienia swoich zdolności w zakresie ochrony przed zagrożeniami cybernetycznymi i promowania świadomości w dziedzinie bezpieczeństwa wśród obywateli i przedsiębiorstw.

Warto dodać, że Ministerstwo Cyfryzacji realizuje program pn. Program Rozwoju Kompetencji Cyfrowych, którego głównym celem jest rozwój kompetencji cyfrowych obywateli. Kompetencje cyfrowe są kluczowe dla udanej transformacji cyfrowej, obecnej we wszystkich dziedzinach naszego życia - od gospodarki, nauki, administracji po satysfakcjonujące i bezpieczne życie obywateli. Kompetencje cyfrowe są nieodzowne przy korzystaniu m.in. z usług edukacyjnych czy usług w zakresie opieki zdrowotnej. Wraz z potrzebą zastosowania nauki zdalnej, szczególnie uwidoczniło się, że kompetencje cyfrowe

telefon: +48 22 245 54 42
adres email: sekretariat.bm@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres: ul. Królewska 27
00-060 Warszawa

nie tylko umożliwiają zdobywanie i rozwój innych kompetencji, ale wręcz są warunkiem koniecznym do ich nabywania.

Dlatego przygotowano Program Rozwoju Kompetencji Cyfrowych, który został przyjęty uchwałą Rady Ministrów 21 lutego 2023 r. Program Rozwoju Kompetencji Cyfrowych jest kompleksowym dokumentem diagnozującym stan kompetencji cyfrowych w Polsce oraz zawierającym planowane działania w tym obszarze, skierowane do konkretnych grup (dzieci w wieku przedszkolnym, uczniowie, studenci, nauczyciele i edukatorzy, użytkownicy technologii cyfrowych, osoby stawiające pierwsze kroki w świecie cyfrowym, pracownicy, osoby zarządzające, przedsiębiorcy, pracownicy sektora publicznego, specjaliści ICT).

Realizacja PRKC ma na celu m.in.

- podniesienie poziomu kompetencji cyfrowych w Rzeczpospolitej Polskiej;
- zwiększenie podaży specjalistów ICT na rynku pracy;
- rozwój edukacji cyfrowej;
- poprawę jakości zarządzania rozwojem kompetencji cyfrowych.

W efekcie realizacji PRKC, zakłada się, że w 2030 r.:

- 80% mieszkańców Polski będzie posiadać co najmniej podstawowe kompetencje cyfrowe;
- 40% mieszkańców Polski będzie posiadać ponadpodstawowe kompetencje cyfrowe;
- 6% pracujących będą stanowić specjaliści ICT;
- 29% specjalistów ICT będą stanowić kobiety;
- na szczeblu administracji rządowej funkcjonować będzie ugruntowany i sprawdzony mechanizm koordynacji i monitorowania działań wspierających rozwój kompetencji cyfrowych, który bazuje na cyklicznie aktualizowanej diagnozie potrzeb społeczeństwa, biorący pod uwagę najnowsze trendy technologiczne i gospodarcze.

W Programie Rozwoju Kompetencji Cyfrowych ujęto działanie, które zakłada stworzenie niemal w każdej gminie miejsca do nabywania kompetycji cyfrowych – Klubu Rozwoju Cyfrowego. W Klubach Rozwoju Cyfrowego pracować będą edukatorzy - animatorzy rozwoju kompetencji cyfrowych w społeczności lokalnej. Kluby zostaną utworzone w oparciu o istniejące już w poszczególnych gminach placówki, bowiem nie chcemy kierować wysiłku organizacyjnego i finansowego na tworzenie nowych instytucji. Kluby Rozwoju Cyfrowego wzbogacą działające obecnie podmioty, takie jak biblioteki, świetlice, domy kultury i inne, o nowe funkcje, czyniąc je jeszcze bardziej użytecznymi dla społeczności lokalnej, pomagając zainteresowanym osobom w zaznajamianiu się z nowymi technologiami oraz rozwijaniu kompetencji cyfrowych.

Usługi Klubów Rozwoju Cyfrowego będą dostępne dla wszystkich obywateli. W każdej zainteresowanej gminie pojawi się miejsce, w którym m.in. każdy będzie mógł uzyskać informacje o dostępnej na rynku ofercie szkoleniowej w zakresie specjalistycznych umiejętności cyfrowych i dostępna będzie informacja o wymaganiach rynku pracy w zakresie umiejętności cyfrowych.

Ponadto Ministerstwo Cyfryzacji wraz Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym realizuje zadanie publiczne pn.: *„Monitoring treści dezinformujących i fake newsów dostępnych w mediach społecznościowych oraz przeprowadzenie*

działań analitycznych, koncepcyjnych i wdrożeniowych w celu budowy i rozwoju narzędzia do monitoringu treści dezinformujących i fake newsów". Zadanie jest częścią długofalowego i wielowątkowego projektu polegającego na budowie i rozwoju narzędzia do monitoring treści dezinformujących oraz fake newsów w mediach. Jego nadrzędnym celem jest dostarczenie najnowszej wiedzy na temat zmian zachodzących w świecie (w ujęciu technologicznym, ekonomicznym, społecznym i prawnym) pod wpływem rozwoju technologii AI. Prezentowane realizowane zadanie bez wątpienia wpisuje się w rozwój polityki AI oraz działania rządu w walkę z dezinformacją.

Dodatkowo w zakresie podejmowanych przez Ministerstwo Cyfryzacji działań służących poszerzeniu ekspertów m.in. z dziedziny AI, sztucznej inteligencji jest realizowany projekt pt:. *„Akademia Innowacyjnych Zastosowań Technologii Cyfrowych – AI Tech"*. Współfinansowany z funduszy europejskich projekt „AI Tech" jest realizowany w partnerstwie 5 polskimi uczelniami. Celem projektu jest stworzenie modelu systemowego kształcenia wysokiej klasy ekspertów w zakresie sztucznej inteligencji, uczenia maszynowego i cyberbezpieczeństwa. Studenci biorący udział w projekcie aktywnie poszerzają swoją wiedzę, w wyniku czego są stworzone przez nich projekty informatyczne opierające się na prowadzonych przez nich badaniach naukowych. Natomiast dotychczasowi absolwenci uzyskali zatrudnienie w prestiżowych firmach.

Wymienione powyżej działania są nielicznymi w stosunku do nowo podejmowanych działań, nad którymi Ministerstwo Cyfryzacji nieustannie pracuje.

Dlaczego Ministerstwo Cyfryzacji nie zmaga się ze współczesnymi problemami, takimi jak sztuczna inteligencja i związane z nią zagrożenia? Co z rozwojem polskiej bazy w tym zakresie, z sensownymi regulacjami?

Ministerstwo Cyfryzacji dostrzega kwestie związane z rozwojem sztucznej inteligencji. W 2020 roku Rada Ministrów przyjęła kompleksową Politykę dla rozwoju sztucznej inteligencji w Polsce. Opisuje ona działania, które Polska powinna wdrożyć i cele, które powinna osiągnąć, mające służyć rozwojowi polskiego społeczeństwa, polskiej gospodarki i nauki w obszarze sztucznej inteligencji. Dokument uwzględnia nie tylko międzynarodowy, prawny, czy techniczno-organizacyjny wymiar wykorzystania sztucznej inteligencji, ale i wymiar etyczny.

Ministerstwo stale diagnozuje problemy związane z wdrażaniem nowych technologii. Obecnie trwa badanie „W drodze ku doskonałości cyfrowej" mające określić gotowości wdrożenia, poziomu wiedzy i wykorzystania nowych technologii (sztuczna inteligencja, Internet rzeczy, e-usługi) w jednostkach samorządu terytorialnego, administracji centralnej, spółkach skarbu państwa, małych i średnich przedsiębiorstwach.

Przedstawiciele Ministerstwa aktywnie działają również w zakresie współpracy międzynarodowej związanej z rozwojem sztucznej inteligencji. Przykładem jest projekt AI4SME realizowany wspólnie z Global Partnership on Artficial Intelligence. Ma on na celu ułatwić małym i średnim przedsiębiorcom wdrażanie rozwiązań z zakresu sztucznej inteligencji

Ministerstwo Cyfryzacji od wielu lat pracuje nad regulacjami stosowania sztucznej inteligencji. W związku z tym została utworzona Grupa Robocza ds. Sztucznej Inteligencji

(GRAI) realizująca zestaw działań służących zapewnieniu w Polsce odpowiednich warunków dla rozwoju zastosowań AI zarówno w sektorach prywatnym i publicznym, a także w prowadzeniu badań naukowych.

Formuła Grupy Roboczej ds. Sztucznej Inteligencji jest otwarta i skupia szeroką reprezentację rynku.

Do współpracy zaproszono:

- dostawców technologii;
- przedstawicieli kancelarii specjalizujących się w prawie nowych technologii;
- przedstawicieli licznych sektorów działających na rynku (finanse, energetyka, zdrowie, edukacja, etc.);
- przedstawicieli nauki (badania i rozwój);
- organizacje pozarządowe;
- przedstawiciele ministerstw oraz instytucji, które są lub powinny być zainteresowane tematyką sztucznej inteligencji, lub/oraz w ich właściwościach są kwestie związane z regulacjami, które mają wpływ na rozwój zastosowań technologii AI w Polsce.

Cele działań Grupy Roboczej:

- wypracowanie rekomendacji służących zapewnieniu w Polsce odpowiednich warunków dla rozwoju zastosowań AI w przedsiębiorstwach i w sektorze publicznym;
- wypracowanie propozycji projektów wykorzystujących zagadnienia AI oraz sposobów wsparcia rozwoju tych już wdrażanych;
- opracowywanie założeń kampanii edukacyjnych w zakresie nowych technologii.

W 2018 r. praca Grupy Roboczej ds. Sztucznej Inteligencji odbywała się w czterech podgrupach:

- Gospodarka oparta o dane;
- Finansowanie badań i rozwoju;
- Edukacja;
- Etyka i prawo.

Reaktywacja działań Grupy Roboczej, która odbyła się w marcu 2021 r., oparła swoją strukturę o Skoordynowany Plan dla Sztucznej Inteligencji Komisji Europejskiej. Doprowadziło to do powstania następujących podgrup merytorycznych:

- Podgrupa ds. badań, innowacyjności i wdrożeń (research, innovation and deployment)/obszarów badawczych i edukacji
- Podgrupa ds. umiejętności cyfrowych (talent and skills)
- Podgrupa ds. ram polityki (policy framework)
- Podgrupa ds. etyki i prawa
- Podgrupa ds. globalnego zasięgu (global outreach)
- Podgrupa ds. zdrowia (health)
- Podgrupa ds. środowiska (environment)
- Podgrupa ds. robotyki (robotics)

- Podgrupa ds. rolnictwa

Więcej szczegółów znajduje się na stronach internetowych portalu sztucznej inteligencji oraz gov.pl, zawierający szczegółowe informacje o poszczególnych grupach merytorycznych.

Ponadto, Ministerstwo Cyfryzacji dokłada wszelkich starań, aby podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty publiczne, zapewniały odpowiedni poziom bezpieczeństwa dla danych Polaków. W tym zakresie należy wskazać dwie ustawy, które regulują przejawy współczesnych zagrożeń - ustawę o krajowym systemie cyberbezpieczeństwa oraz ustawę o zwalczaniu nadużyć w komunikacji elektronicznej.

Zagadnienia związane ze sztuczną inteligencją są również często podnoszone w kontaktach między instytucjami na poziomie roboczym, chociażby w ramach funkcjonującego Projektu Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC).

Dla podmiotów nieobjętych ww. regulacjami Ministerstwo Cyfryzacji publikuje stosowne rekomendacje oraz poradniki m.ni. w powszechnie dostępnej bazie wiedzy o cyberbezpieczeństwie na portalu gov.pl.

Warto również przypomnieć, że Rada Ministrów 28 grudnia 2020 r. przyjęła dokument kierunkowy *Polityka rozwoju sztucznej inteligencji w Polsce*, który określa działania i cele dla Polski w perspektywie krótkoterminowej (do 2023 r.), średnioterminowej (do 2027 r.) i długoterminowej (po 2027 r.).

Co wreszcie z internetem szerokopasmowym i dostępem do usług typu e-obywatel?

Rząd Polski przyjął strategię "Polska Cyfrowa", która zakładała rozbudowę infrastruktury szerokopasmowej na terenach wiejskich i w mniejszych miejscowościach. Celem było zapewnienie szybkiego dostępu do Internetu dla jak największej liczby mieszkańców. W ramach tego planu przeprowadzano inwestycje w infrastrukturę, w tym rozwój sieci światłowodowych i radiowych.

1 czerwca br. zostały ogłoszone konkursy na budowę sieci szerokopasmowych w ramach Krajowego Planu Odbudowy i Zwiększania Odporności oraz Programu Fundusze Europejskie na Rozwój Cyfrowy. Celem konkursów jest, aby wszyscy mieszkańcy terenów, na których inwestycje w sieci szerokopasmowe są nieopłacalne na warunkach rynkowych, mieli dostęp do szybkiego internetu. Konkursy przeznaczone są dla przedsiębiorców telekomunikacyjnych. Polska została podzielona na 402 obszary konkursowe. Ze środków KPO dofinansowanych zostanie 250 projektów o łącznej wartości do 6,6 MLD PLN i obejmujących 1050 tys. gospodarstw domowych, natomiast z FERC dofinansowanych zostanie 152 projektów o łącznej wartości do 4,6 MLD PLN i obejmujących 675 tys. gospodarstw domowych.

Informujemy również, że za pomocą Systemu Informacyjnego o Dostępie do Usług Stacjonarnego Internetu Szerokopasmowego możliwe jest sprawdzenie - dla dowolnej lokalizacji w Polsce - jakie usługi dostępu do stacjonarnego internetu są obecnie oferowane, czy dany adres jest planowany do objęcia zasięgiem sieci na zasadach komercyjnych oraz czy zapewnienie dostępu do internetu pod danym adresem zostanie sfinansowane ze środków Programu Operacyjnego Polska Cyfrowa, Funduszy Europejskich na Rozwój Cyfrowy albo Krajowego Planu Odbudowy.

Wszelkie informacje dotyczące systemu SIDUSIS oraz składania wniosków o dofinansowanie w ogłoszonych konkursach dostępne są na poniższych stronach internetowych:

1) SIDUSIS: https://internet.gov.pl/
2) Krajowy Plan Odbudowy: Inwestycja C 1.1.1 Zapewnienie dostępu do bardzo szybkiego internetu na obszarach białych plam (1 nabór) - Centrum Projektów Polska Cyfrowa - Portal Gov.pl (www.gov.pl)
3) Fundusze Europejskie na Rozwój Cyfrowy: Zwiększenie dostępu do ultra-szybkiego internetu szerokopasmowego (1 nabór) - Centrum Projektów Polska Cyfrowa - Portal Gov.pl (www.gov.pl)

E-obywatel:

W Polsce istnieje platforma ePUAP (Elektroniczna Platforma Usług Administracji Publicznej), która umożliwia obywatelom korzystanie z elektronicznych usług administracji publicznej. Przez ePUAP można składać dokumenty, sprawdzać swoje dane, rejestrować pojazdy i wiele innych.

Elektroniczne składanie dokumentów: Program cyfryzacji wprowadził możliwość elektronicznego składania dokumentów, takich jak wnioski o dowód osobisty, rejestracja pojazdów, składanie deklaracji podatkowych itp. Obywatele mogą załatwiać wiele spraw bez konieczności osobistego stawiania się w urzędach.

Usługi zdrowotne online: W ramach programu cyfryzacji, rozwijane są usługi zdrowotne online, takie jak e-recepty, e-skierowania czy elektroniczne akta medyczne. Obywatele mają możliwość korzystania z tych usług przez platformy internetowe.

Mając na uwadze stale rosnące zainteresowanie aplikacją mObywatel, jej dynamiczny rozwój oraz oczekiwania społeczne w zakresie udostępniania w niej nowych usług i dokumentów oraz zapewnienia powszechnego uznawania tych dokumentów, Rada Ministrów podjęła decyzję o opracowaniu, a następnie przyjęciu niniejszego projektu ustawy.

Aktualnie kwestie dotyczące funkcjonowania aplikacji mObywatel uregulowane są w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Projekt ustawy o aplikacji mObywatel przewiduje uchylenie powyższych przepisów oraz wprowadzenie podstaw prawnych udostępniania szerokiego wachlarza usług w aplikacji mObywatel oraz wykorzystywania i uznawania dokumentów elektronicznych, obsługiwanych przy użyciu tej aplikacji, co najmniej tak powszechnie jak to ma dziś miejsce w przypadku tradycyjnych dokumentów.

Pierwsza w Polsce ustawa poświęcona aplikacji zyskała szerokie poparcie obywateli oraz parlamentarzystów. Wprowadza m.in. cyfrowy dokument tożsamości, czyli mDowód. Nie jest to dowód osobisty w postaci elektronicznej – to zupełnie nowy dokument (funkcjonujący niezależnie od dowodu osobistego), którym będziemy mogli posługiwać się w kraju.

Ten elektroniczny dokument będzie powszechnie respektowany – w urzędach i każdym innym miejscu, w którym załatwia się sprawy i należy okazać dokument tożsamości.

Dokument będzie pozwalał na stwierdzenie tożsamości i obywatelstwa polskiego użytkownika aplikacji mObywatel:

- na terytorium Rzeczypospolitej Polskiej,
- w relacjach wzajemnej fizycznej obecności stron (np. przy zawieraniu umowy kupna-sprzedaży),
- w każdym przypadku, gdy z przepisu prawa wynika obowiązek stwierdzenia tożsamości na podstawie dokumentu tożsamości, w szczególności na podstawie dowodu osobistego.

Projekt ustawy zakłada również umożliwienie prowadzenia w systemie mObywatel ewidencji dokumentów elektronicznych dostępnych w aplikacji mObywatel i wydawanych przez podmioty publiczne (np. jednostki samorządu terytorialnego) oraz inne podmioty (np. samorządy zawodowe, stowarzyszenia, związki sportowe, organizacje zrzeszające miłośników zwierząt). Podmioty te będą mogły prowadzić ewidencję, uruchamiać i zarządzać swoimi dokumentami elektronicznymi wydanymi dla obywateli.

Kolejnym udogodnieniem przewidzianym w projekcie ustawy jest zapewnienie możliwości dokonywania wygodnych płatności. Usługa będzie powiązana z innym projektem realizowanym przez Ministra Cyfryzacji obejmującym udostępnienie platformy płatności dla podmiotów publicznych.

Wśród nowych dokumentów elektronicznych, jakie będą dostępne w aplikacji warto wymienić w szczególności :

- legitymację osoby niepełnosprawnej, co jest realizacją oczekiwań społecznych kierowanych m. in. do Komisji ds. Petycji
- legitymację służbową nauczyciela,
- legitymację doktoranta,
- dokumenty potwierdzające prawo do wykonywania zawodów medycznych: lekarzy, lekarzy dentystów, pielęgniarek, położnych, fizjoterapeutów, diagnostów laboratoryjnych oraz farmaceutów.

Ponadto w drodze zgłoszonych poprawek w procesie legislacyjnym dostępne będą również takie dokumenty jak:

- legitymacja senatorska,
- karta rowerowa,
- karta nauczyciela,
- dokumenty potwierdzające prawo do wykonywania zawodów medycznych: lekarza i lekarza dentysty, pielęgniarki i położnej, ratownika medycznego dla obywateli Ukrainy będących użytkownikami aplikacji mObywatel, których pobyt na terytorium Rzeczypospolitej Polskiej uznaje się za legalny na podstawie ustawy z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa.

Przykładowe nowe funkcje, które pojawią się w mObywatelu to:

- e-płatności – dzięki tej usłudze wszystkie zobowiązania finansowe, jakie wystawił nam urząd będą pod kontrolą z poziomu aplikacji. Bez prowizji i w kilku kliknięciach zapłacimy np. za podatek od nieruchomości i wniesiemy inne samorządowe opłaty.

Na początku maja w Bydgoszczy miała miejsce pierwsza płatność BLIKIEM zrealizowana przez aplikację w partnerstwie z urzędem miasta i Asseco. To nie tylko szybka forma płatności – cyfryzujemy cały proces, nie czekamy na księgowanie – potwierdzenie wpłaty pojawia się w systemie od razu;

- „bezpieczny autobus" – wysyłamy dzieci na kolonie, obozy – wszyscy chcemy mieć pewność, że autokar, który je przewozi, jest sprawny technicznie. Będziemy mogli to łatwo sprawdzić, korzystając z mObywatela;
- e-pełnomocnictwa – każdy z nasz będzie mógł szybko i bezpłatnie upoważnić kogoś bliskiego do załatwiania za niego spraw urzędowych, bez konieczności chodzenia do notariusza i ponoszenia dodatkowych kosztów z tego tytułu;
- Karta Mieszkańca, czyli nowoczesna forma potwierdzająca możliwość korzystania z miejskich przywilejów dla płacących podatki w danej miejscowości.

Rozwiązania proponowane w projekcie ustawy są ważnym krokiem na drodze postępującej cyfryzacji administracji publicznej z uwzględnieniem dynamicznego rozwoju myśli technologicznej oraz kierunków wyznaczanych przez Unię Europejską oraz realizacji postulatów zgłaszanych przez społeczeństwo.

Czy w Polsce zostanie zbudowana suwerenność cyfrowa? Czy zbudujemy ją lokalnie, dla Polaków?

Ministerstwo Cyfryzacji od wielu lat realizuje Program Wspólnej Infrastruktury Informatycznej Państwa (Program WIIP) w oparciu o Uchwałę WIIP. W ramach WIIP zbudowana została Rządowa Chmura Obliczeniowa zapewniająca przetwarzanie danych systemów informatycznych administracji rządowej w infrastrukturze informatycznej Ministerstwa Cyfryzacji. Ponadto, w ramach Uchwały WIIP opracowano Standardy Cyberbezpieczeństwa Chmur Obliczeniowych, które regulują kwestie przetwarzania danych w chmurach obliczeniowych dla danych i systemów informatycznych administracji rządowej.

Co z zarządzaniem danymi Polaków np. danymi w systemie energetycznym czy danymi systemie zdrowotnym i media społecznościowych?

Należy zaznaczyć, że poruszane kwestie w ww. pytaniu znajdują się w gestii różnych administratorów danych osobowych. Każdy z tych systemów ma stosownego administratora danych, który odpowiada za zarządzanie danymi osobowymi tam zgromadzonymi. Minister Cyfryzacji nie jest ich administratorem lecz odpowiednie organy lub podmioty. W przypadku systemów energetycznych, administratorem danych jest Minister Klimatu i Środowiska lub Minister Aktywów Państwowych. Minister Cyfryzacji nie może zatem odpowiedzieć w zastępstwie tych organów. Odnośnie zaś systemów zdrowotnych administratorem danych jest Minister Zdrowia. Podstawy do przetwarzania danych osobowych przez organy administracji publicznej w prowadzonych przez nie systemach, powinny wynikać z odpowiednich, sektorowych przepisów powszechnie obowiązującego prawa. Minister Cyfryzacji nie nadzoruje w ramach swoich zadań tych administratorów ani nie odpowiada za zarządzanie tymi systemami.

W zakresie przetwarzania danych osobowych w mediach społecznościowych, należy wskazać, że są one co do zasady przetwarzane przez właściwych administratorów, na podstawie zgody osoby fizycznej, która korzysta z tego rodzaju usług/mediów. W tym przypadku każda osoba indywidualnie decyduje czy wyraża zgodę na przetwarzanie jej

danych osobowych przez dany podmiot będący administratorem jej danych, zgromadzonych w stosownych mediach społecznościowych. Minister Cyfryzacji nie ma uprawnień do nadzoru i kontroli w tym aspekcie wobec tych administratorów.

Takie uprawnienia, zgodnie z RODO oraz ustawą o ochronie danych osobowych, ma niezależny organ nadzoru, tj. Prezes Urzędu Ochrony Danych Osobowych (PUODO). Każdy obywatel, jeśli uważa, że dany administrator narusza RODO gdy przetwarza jego dane osobowe, może złożyć skargę do PUODO. PUODO zaś może w rezultacie takiej skargi przeprowadzić kontrolę i postępowanie administracyjne wobec takiego administratora.

Wobec powyższego Minister Cyfryzacji nie ma uprawnień do oceny zarzutów niezgodności z prawem międzynarodowych korporacji, podnoszonych w wystąpieniu Senatora. Należy jednak w tym miejscu wskazać, że wobec wskazanych przez Senatora podmiotów mediów społecznościowych toczą się stosowne postępowania, prowadzone przez irlandzki organ nadzorczy, EROD oraz TSUE, w zakresie niezgodnego z RODO przetwarzania danych osobowych. Do czasu prawomocnego zakończenia tych postępowań należy powstrzymać się od jednoznacznych ocen w tej kwestii.

Niezależnie od powyższego, Minister Cyfryzacji podejmuje działania na rzecz ochrony danych osobowych i zapewniania odpowiednich standardów bezpieczeństwa. Tworzone są przepisy i regulacje mające na celu ochronę prywatności i danych obywateli. Równocześnie, prowadzone są działania edukacyjne i kampanie informacyjne, aby podnieść świadomość społeczeństwa na temat zagrożeń i dobrych praktyk związanym z bezpieczeństwem danych (realizowane np. przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego - CSIRT NASK).

Ministerstwo Cyfryzacji pozostaje w dialogu z największymi podmiotami na rynku mediów społecznościowych, analizuje wszystkie sygnały spływające do resortu dot. zagrożeń związanych z korzystaniem z mediów społecznościowych, w szczególności przez osoby najmłodsze.

Prowadzony dialog oraz szeroka wymiana informacji z innymi podmiotami, w szczególności z właściwymi agencjami UE, takimi jak ENISA, stanowi podstawę budowania rekomendacji oraz wytycznych. W tym zakresie Ministerstwo Cyfryzacji uczestniczy w tworzeniu kampanii informacyjnych, które mają na celu budowanie świadomości użytkowników w zakresie zagrożeń, jakie pojawiają się w mediach społecznościowych.

W ramach działań edukacyjnych Ministerstwo Cyfryzacji prowadzi m.in. wspomnianą już powszechnie dostępną bazę wiedzy o cyberbezpieczeństwie na portalu gov.pl, gdzie publikowane są materiały o bezpieczeństwie online w tym artykuły i poradniki dot. bezpiecznego korzystania z mediów społecznościowych, w tym publikacje nt. mediów społecznościowych[1].

Dostępna jest także baza Sprawdź, czy Twoje dane są bezpieczne, w której można sprawdzić, czy dane konkretnego użytkownika internetu znalazły się wśród upublicznionych przez cyberprzestępców.

[1] https://www.gov.pl/web/baza-wiedzy/bezpieczni-w-mediach-spolecznosciowych--praktyczne-wskazowki oraz https://www.gov.pl/web/baza-wiedzy/media-spolecznosciowe-jak-bezpiecznie-z-nich-korzystac.

Działania podnoszące świadomość obejmują szeroką, zróżnicowaną grupę użytkowników Internetu, są one realizowane długofalowo oraz dostosowywane do zmieniających się realiów w cyberprzestrzeni.

Minister Cyfryzacji wspiera także działania podejmowane przez CSIRT NASK, udzielając prowadzącemu ten Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, dotacji podmiotowej.

Warto zauważyć, że od początku wydarzeń związanych z sytuacją na wschodniej granicy Polski, a następnie konfliktu zbrojnego w Ukrainie, CSIRT NASK odnotowuje próby ataków wykorzystujące ten kontekst. Najczęściej są za to odpowiedzialne grupy przestępcze, które wpisując się w aktualny trend wydarzeń, wytwarzają wiadomości lub strony zorientowane na wyłudzanie poufnych danych dostępowych lub środków finansowych. Stosowana przez przestępców socjotechnika niezmiennie ma za zadanie wymusić podejmowanie na atakowanych szybkich, a także nieprzemyślanych decyzji. CSIRT NASK działając w trybie 24/7 przyjmuje tego typu zgłoszenia dążąc do niezwłocznego usunięcia tych treści z przestrzeni internetu. Robi to min. poprzez prowadzoną publicznie listę ostrzeżeń.

Ataki ukierunkowane na poszczególnych użytkowników lub instytucje w ostatnim czasie znacząco zorientowały się na ukraińskich instytucjach państwowych, a także wojskowych. W przypadku próby pozyskania naszych danych dostępowych najlepszą obroną pozostaje cały czas właściwa ocena w zakresie autentyczności każdej próby dotyczącej zmiany hasła. Niemniej istotne jest jednak także odpowiednie podejście w zakresie zachowania zasad higieny, a także konfiguracji zabezpieczeń naszego konta[2].

Każdą podejrzaną próbę aktywności w sieci można zgłaszać poprzez dedykowany formularz dostępny na stronie CERT.PL

W obszarze dezinformacji obserwujemy wzmożoną liczbę treści dezinformacyjnych, które zwłaszcza po wojnie na Ukrainie zostały zintensyfikowane. Akcje dezinformacyjne mają na celu zmianę percepcji na wydarzenia związane z sytuacją na Ukrainie, a zwłaszcza zmianę poczucia bezpieczeństwa i wzbudzanie paniki oraz strachu w opinii publicznej. Ponadto odnotowywane są materiały w przestrzeni internetowej, które mają na celu antagonizowanie ukraińskich uchodźców wojennych wobec społeczeństwa polskiego. Zachęcamy do czujności i reakcji na pojawiające się treści, które wzbudzają nasze wątpliwości, co do przekazu i intencji autora.

Niebezpieczne wpisy warto zgłaszać do administracji portalu lub medium społecznościowego i do NASK na maila - informacje@nask.pl - który wspiera internautów w weryfikowaniu informacji w mediach społecznościowych. Profile #WłączWeryfikację prowadzą doświadczeni eksperci instytutu, którzy dementują nieprawdziwe informacje krążące w sieci oraz wskazują przejawy działań dezinformacyjnych.

Ponadto, Polski Rząd aktywnie uczestniczy w pracach nad stworzeniem europejskiego systemu zarządzania danymi – systemu rozwiązań prawnych i pozaprawnych, którego celem jest zwiększenie dostępności i możliwości wykorzystania danych w gospodarce i w społeczeństwie, przy jednoczesnym utrzymaniu nad nimi kontroli przez generujące je przedsiębiorstwa i osoby fizyczne. Tworzony system zarządzania danymi jest oparty o

[2] https://www.cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf

koncepcję suwerenności danych, która zakłada przestrzeganie w jego ramach europejskich zasad i wartości oraz unijnych i krajowych przepisów prawa dot. m.in. ochrony konsumentów, prywatności, prawa konkurencji. Fundamentem systemu jest niedyskryminacyjny, równy dla wszystkich, oparty o jasne i funkcjonalne zasady, dostęp do danych. W konsekwencji każdy obywatel będzie wiedział kto, na jakich zasadach i w jakim zakresie będzie miał dostęp do generowanych przez siebie danych oraz uzyska narzędzia sprawowania kontroli nad procesem ich udostępniania.

Aktualnie trwają intensywne prace legislacyjne na forum Unii Europejskiej nad kolejną fazą budowania systemu zarządzania danymi. Ministerstwo Cyfryzacji odpowiada za negocjacje projektu Aktu w sprawie danych (Data Act). Wprowadzi on rozwiązania umożliwiające każdemu z obywateli swobodne dysponowanie danymi, które generują posiadane przez nich urządzenia podłączone do Internetu. Obywatele zyskają swobodny dostęp do tych danych oraz prawo udostępniania ich podmiotom trzecim (przedsiębiorcom i osobom fizycznym) w dowolnych celach – komercyjnych i niekomercyjnych. Zwiększy się też kontrola obywateli nad tym, komu i do jakich celów ich dane z urządzeń Internetu rzeczy udostępniają ich producenci.

Jak wreszcie będzie chciał zapisać się w historii cyfryzacji Polski nowy minister cyfryzacji?

Minister Cyfryzacji jest organem odpowiedzialnym za opracowanie regulacji prawnych, których podstawowym celem jest zagwarantowanie cyberbezpieczeństwa państwa i obywateli. Do aktów prawnych o kluczowym w tym zakresie znaczeniu należy zaliczyć ustawę o krajowym systemie cyberbezpieczeństwa oraz ustawę o zwalczaniu nadużyć w komunikacji elektronicznej.

Wśród głównych założeń ustawy o krajowym systemie cyberbezpieczeństwa znalazło się ustanowienie uregulowań prawnych umożliwiających implementacje dyrektywy NIS oraz utworzenie efektywnego systemu bezpieczeństwa teleinformatycznego na poziomie krajowym. Ustawa określa organizację oraz sposób funkcjonowania krajowego systemu cyberbezpieczeństwa, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy oraz zakresu i trybu stanowienia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Ponadto ustawa ustanawia zasady wskazywania operatorów usług kluczowych i ich obowiązki dotyczące wdrożenia efektywnego systemu zarządzania bezpieczeństwem, który obejmuje m.in. zarządzanie ryzykiem, procedury i mechanizmy zgłaszania i postępowania z incydentami czy organizację struktur na poziomie operatora.

Regulacja ta określa również organy właściwe ds. cyberbezpieczeństwa odpowiedzialne za sprawowanie nadzoru wobec operatorów usług kluczowych. Organy te są elementem krajowego systemu cyberbezpieczeństwa odpowiedzialnymi również za opracowywanie we współpracy z Zespołami Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) poziomu krajowego wytycznych bezpieczeństwa teleinformatycznego w wymiarze sektorowym.

Zespoły CSIRT poziomu krajowego, tj. CSIRT GOV[3], CSIRT MON[4] i CSIRT NASK[5][6], współpracują ze sobą, zapewniając spójny i kompletny system zarządzania ryzykiem w zakresie cyberbezpieczeństwa państwa oraz obsługę zgłoszonych incydentów, w tym zwłaszcza incydentów poważnych i krytycznych, najpoważniejszych z punktu widzenia państwa.

W tym aspekcie warto wskazać na konkretne dane - w 2021 r. zespół CSIRT NASK obsłużył 29 483 unikalnych incydentów cyberbezpieczeństwa, w 2022 r. - 39 683, czyli o ok. 34,5 % więcej niż w roku poprzednim i niemal czterokrotnie więcej niż 2019 r., w którym zespół ten odnotował 10 420 incydentów. Szkody powstałe na skutek tych działań (m.in. zaszyfrowanie danych, wykradzenie ich czy uniemożliwienie bądź utrudnienie świadczenia usług publicznych) są bardzo poważne.

Z uwagi na znaczny wzrost incydentów oraz zaawansowaną działalność cyberprzestępców konieczna stała się nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa. Na mocy nowelizowanych przepisów ustanowiony zostanie CSIRT INT prowadzony przez Szefa Agencji Wywiadu, zapewniający wsparcie placówkom dyplomatycznym i konsularnym w zakresie cyberbezpieczeństwa. Ponadto, dla każdego z sektorów krajowego systemu cyberbezpieczeństwa powołany zostanie CSIRT sektorowy mający wspierać operatorów usług kluczowych z danego sektora. Powołanie nowych CSIRT na szczeblu sektorowym wpłynie na skrócenie czasu obsługi incydentów w sektorze, a dodatkowo będą one obsługiwane ze szczególnym uwzględnieniem uwarunkowań sektora w jakim dane podmioty funkcjonują.

Do krajowego systemu cyberbezpieczeństwa zostaną dodatkowo włączeni przedsiębiorcy telekomunikacyjni, na których zostaną nałożone obowiązki z zakresu cyberbezpieczeństwa. Zostanie również powołany CSIRT Telco, który będzie wspierał te podmioty w realizacji tych zadań.

Przewiduje się także przyjęcie przepisów w zakresie certyfikacji cyberbezpieczeństwa, co przyczyni się do zwiększenia świadomości znaczenia cyberbezpieczeństwa w sektorze przedsiębiorstw i skłoni przedsiębiorców do stosowania bezpieczniejszych, sprawdzonych rozwiązań.

Kolejnym, niezwykle istotnym, z perspektywy każdego obywatela RP aktem prawnym jest ustawa o zwalczaniu nadużyć w komunikacji elektronicznej. Ustawa została przygotowana z uwagi na coraz powszechniejsze używanie komunikacji elektronicznej w życiu codziennym, fakt ten niestety nie pozostał bez wpływu na działalność cyberprzestępców, którzy zaczęli masowo wykorzystywać typowe dla tych form kontaktu podatności, w tym także działania socjotechniczne.

---

[3] CSIRT GOV - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego.
[4] CSIRT MON - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej.
[5] CSIRT NASK - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy.
[6] Zadania CSIRT poziomu krajowego zostały określone w art. 26 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2023 r. poz. 913).

Nadużycia dokonywane przez cyberprzestępców, które zostały spenalizowane w ramach projektu stanowią poważny problem i z tego względu doszło do podjęcia działań na poziomie ustawowym. Od kwietnia 2021 r. do początku czerwca 2022 r. zespół CSIRT NASK zidentyfikował 31 054 krótkich wiadomości tekstowych o znamionach smishingu w których oszuści podszywając się pod zaufane instytucje próbują nakłonić ofiarę do ujawnienia danych osobowych, informacji o karcie kredytowej czy zainfekować urządzenie[7]. Problem ten występuje powszechnie także na szczeblu międzynarodowym.

Powyższy projekt zakłada stworzenie nowych narzędzi do zwalczania najczęściej występujących oszustw takich jak phishing za pomocą sms-ów. W projekcie wprowadzono przepisy karne przewidujące odpowiedzialność za działania takie jak generowanie sztucznego ruchu, smishing oraz CLI spoofing. Przepisy te znacząco ułatwią organom prowadzenie spraw przeciwko oszustom wykorzystującym najnowsze technologie. Ponadto, zaproponowane rozwiązania mają służyć stworzeniu ram prawnych do podejmowania działań nie tylko mających na celu zwalczanie nadużyć, ale również zapobieganie im przez przedsiębiorców telekomunikacyjnych. Aby zapewnić prawidłową realizację tych zadań będą oni zobowiązani do podejmowania proporcjonalnych środków organizacyjnych i technicznych, blokowania krótkich wiadomości tekstowych zawierających znamiona smishingu na podstawie wzorca wiadomości czy blokowania połączeń głosowych, które mają na celu podszywanie się pod inną osobę lub instytucję.

Przewiduje się także obowiązek stosowania w przypadku świadczenia poczty elektronicznej mechanizmu uwierzytelniania SPF/DKIM/DMARC przez dostawców poczty elektronicznej dla co najmniej 500 000 użytkowników lub podmiotów publicznych. Powstanie ponadto wykaz numerów służących wyłącznie do odbierania połączeń głosowych prowadzony przez Prezesa Urzędu Komunikacji Elektronicznej. Takie rozwiązanie znacząco zmniejszy liczbę oszustw bowiem wiadomości i połączenia wychodzące z tych numerów będą od razu blokowane co uniemożliwi przestępcom wykorzystywanie tych numerów.

Projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej aktualnie znajduje się na etapie prac parlamentarnych.

Jak wprowadzane mają być nowe regulacje, np. podatek cyfrowy?

Zgodnie z ustawą z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2022 r. poz. 2512), do katalogu zadań Ministra Finansów należy realizacja dochodów i wydatków budżetu państwa, m.in. dochodów z podatków, a także współpraca finansowa, kredytowa i płatnicza z zagranicą. Stąd też tematyka "podatku cyfrowego" należy do kompetencji Ministra Finansów.

Czy zwiększy się inwigilacja Polaków z powodu braku współpracy Ministerstwa z ekspertami i czynnikami społecznymi , która jest w innych krajach?

Od wejścia w życie Dyrektywy NIS oraz przyjęcia ustawy o krajowym systemie cyberebzpieczeństwa, Ministerstwo Cyfryzacji współpracuje zarówno z ekspertami z innych Państw Członkowskich w ramach Grupy Współpracy, jak i z ekspertami w kraju. Przy każdej okazji, związanej z wprowadzaniem regulacji na poziomie unijnym dokumenty te są konsultowane ze stroną społeczną i każdy może się wypowiedzieć w tym zakresie.

[7] https://cert.pl/posts/2022/04/smishing-pge / ; https://cert.pl/posts/2022/04/flubot-smishing/

Eksperci Ministerstwa Cyfryzacji są także aktywni na wszystkich formach. W ramach nowej Dyrektywy NIS2, została powołana do życia Europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe). Jej celem jest pomaganie w skoordynowanym zarządzaniu na szczeblu operacyjnym incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę oraz zapewnianie regularnej wymiany odpowiednich informacji między państwami członkowskimi a instytucjami, organami, urzędami i agencjami Unii.

Równocześnie od momentu wejścia w życie Dyrektywy NIS, funkcjonuje sieć CSIRT, która składa się z przedstawicieli CSIRT wyznaczonych przez Państwa Członkowskie oraz CERT-EU odpowiadający za instytucje unijne. Do zadań Sieci CSIRT należy m.in. współpraca między poszczególnymi zespołami, wymiana informacji dotyczących zagrożeń, współpraca operacyjna, czy koordynowanie działań mających na celu łagodzenie skutków incydentów, w tym incydentów transgranicznych. W ramach tej sieci funkcjonują wszystkie 3 CSIRTy poziomu krajowego w Polsce, przy czym wiodącą rolę pełni CSIRT NASK. Eksperci CSIRT NASK uczestniczą w spotkaniach i na bieżąco monitorują i współpracują z ekspertami z innych zespołów.

Jednym z przykładów współpracy międzynarodowej jest Inicjatywa Counter Ransomware Iniciative, która została uruchomiona w październiku 2021 r. przez amerykańską Radę Bezpieczeństwa Narodowego. Przyłączyło się do niej ponad 30 krajów, w tym Polska. Celem CRI jest przyspieszenie współpracy między krajami w celu zwalczania oprogramowania ransomware, a mianowicie poprawa odporności sieci, zajęcie się systemami finansowymi, które sprawiają, że oprogramowanie ransomware jest opłacalne, zakłócenie ekosystemu oprogramowania ransomware poprzez współpracę organów ścigania oraz wykorzystanie narzędzi dyplomacji i zwiększenie potencjału partnerów. Eksperci z Ministerstwa Cyfryzacji oraz NASK uczestniczą w projektach mających na celu wymianę doświadczeń dotyczących radzenia sobie z atakami typu ransomware. Jednocześnie przedstawiciele obu instytucji prowadzą projekt RACER – zbiorowa skuteczna odporność na ataki ransomware. Celem projektu jest budowanie zbiorowej, ustrukturyzowanej, międzysektorowej wiedzy opartej na najlepszych praktykach w celu zwiększenia naszej zbiorowej odporności na ataki ransomware oraz opracowanie wspólnych, uzgodnionych na szczeblu międzynarodowym przewodników dotyczących trzech tematów dotyczących ataków ransomware.

Jednocześnie, w styczniu 2023 r. Ministerstwo Cyfryzacji zorganizowało w Warszawie praktyczne warsztaty dla sektora energetycznego wraz z Ambasadą USA, Departamentem Energii i Idaho National Laboratory i planujemy kolejną edycję w tym roku. Celem warsztatów, w którym uczestniczyło prawie 50 ekspertów z kilku krajów w tym Ukrainy, miała na celu zwiększenie ich wiedzy w zakresie bezpieczeństwa systemów OT.

Ponadto, wpisując się w dążenie Unii Europejskiej do suwerenności cyfrowej w otwartym i wzajemnie połączonym świecie, wyrażonej w m.in. dokumencie Droga ku cyfrowej dekadzie, Minister Cyfryzacji włącza się w projekty i działania na poziomie europejskim, których celem jest wzmocnienie pozycji i znaczenia Polski w obszarze cyberbezpieczeństwa.

Jedną z najnowszych europejskich inicjatyw w zakresie cyberbezpieczeństwa jest utworzenie Europejskiego Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (dalej: ECCC), którego celem jest zwiększenie bezpieczeństwa sieci i systemów informatycznych, w tym Internetu i innych

rodzajów infrastruktury krytycznej dla funkcjonowania społeczeństwa w sektorach transportu, ochrony zdrowia, energii, infrastruktury cyfrowej, gospodarowania wodą, czy finansowym. Zgodnie z treścią rozporządzenia powołującego ECCC, powinno być ono głównym unijnym instrumentem służącym skupianiu inwestycji w badania naukowe, technologię i rozwój przemysłu w dziedzinie cyberbezpieczeństwa oraz wdrażaniu odpowiednich projektów i inicjatyw razem z tworzoną Siecią. Sieć zaś tworzą Krajowe ośrodki koordynacji w państwach członkowskich (NCC), tworzone i utrzymywane ze środków tych państw.

Minister Cyfryzacji niezwłocznie włączył się w niniejszą inicjatywę, tworząc w strukturze urzędu Krajowe Centrum Kompetencji Cyberbezpieczeństwa, któremu powierzono szereg zadań o kluczowym znaczeniu dla rozwoju i koordynacji współpracy z ECCC, Siecią i pozostałymi interesariuszami w obszarze cyberbezpieczeństwa, rozpoczynając tym samym budowę krajowej Społeczności kompetentnej w dziedzinie cyberbezpieczeństwa.

Społeczność kompetentna to interdyscyplinarna i zróżnicowana grupa europejskich interesariuszy, zaangażowanych w rozwój i wzmocnienie potencjału europejskiego w zakresie cyberbezpieczeństwa. Jej rolą będzie: wnoszenie wkładu w misję ECCC i Sieci oraz wzmacnianie i upowszechnianie w całej Unii fachowej wiedzy z zakresu cyberbezpieczeństwa i dzielenie się tą wiedzą, czynny udział w realizacji działań ECCC oraz współpraca z ECCC i NCC, promowanie wspólnych projektów, wspieranie Unii w utrzymywaniu i rozwijaniu zdolności technologicznych i przemysłowych w dziedzinie cyberbezpieczeństwa niezbędnych do zabezpieczenia jej jednolitego rynku cyfrowego, pomaganie w identyfikowaniu wyzwań technicznych, które należy uwzględnić w krajowych i europejskich planach działania.

Krajowe Centrum Kompetencji realizuje ponadto inne przedsięwzięcia mające wpływ na rozwój krajowej branży bezpieczeństwa, jak:

- organizowane przez Europejskie Centrum Kompetencji Cyberbezpieczeństwa, Krajowe Centrum Kompetencji Cyberbezpieczeństwa (NCC-PL), Instytut Kościuszki i klaster #CyberMadeInPoland przy wsparciu zespołu projektowego ECCO w Katowicach w dniu 22 czerwca 2023 r. podczas Cybersec Forum/Expo 2023, wydarzenie matchmakingowe *Access to Market*. Celem tego wydarzenia była prezentacja firm, które opracowały skuteczne rozwiązania w obszarze cyberbezpieczeństwa i chciałyby dotrzeć z nimi do potencjalnych klientów – dziesięć z nich będzie miało szanse zaprezentować swoje rozwiązania przed europejską publicznością;
- pomoc techniczna świadczona przez NCC-PL poprzez wsparcie podmiotów krajowych w ubieganiu się o środki z Programu Cyfrowa Europa, zwiększając tym samym liczbę zainteresowanych tym źródłem finasowania bezpośredniego.

Poczta polska 22 kwietnia 2020 r. otrzymała z Ministerstwa Cyfryzacji płytę DVD z danymi Polaków, wszystkich dorosłych Polaków – łącznie z numerami PESEL – które miały służyć do organizacji wyborów kopertowych. Co z tymi danymi?

W dniu 20 kwietnia 2020 r. Poczta Polska S.A. złożyła elektroniczny wniosek o udostępnienie danych z rejestru PESEL, w trybie art. 99 ustawy z dnia 16 kwietnia 2020 r. o szczególnych instrumentach wsparcia w związku z rozprzestrzenianiem się wirusa SARS-

CoV-2 (Dz. U. z 2020 r. poz. 695), w celu i zakresie niezbędnym do podjęcia i realizacji czynności zmierzających do przygotowania przeprowadzenia wyborów Prezydenta RP w 2020 r. w trybie korespondencyjnym.

Następnie Poczta Polska S.A. przy piśmie z dnia 26 maja 2020 r. oświadczyła, że nie dysponuje już danymi osobowymi w jakiejkolwiek formie, które zostały jej przekazane w dniu 22 kwietnia br. z rejestru PESEL, ponieważ w dniu 15 maja 2020 r. komisyjnie zniszczono wszelkie nośniki (bazy), na których znajdowały się te dane. Na potwierdzenie tego dołączono kopię protokołu potwierdzającego komisyjne usunięcie zapisów tych danych.

Z wyrazami szacunku,

Paweł Lewandowski
Podsekretarz 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
adres strony internetowej: www.gov.pl/cyfryzacja

adres: ul. Królewska 27
00-060 Warszawa