WICEPREZES
NAJWYŻSZEJ IZBY KONTROLI
MAŁGORZATA MOTYLOW

LOL.410.017.01.2021

Michał Dworczyk
Minister – członek Rady Ministrów
Kancelaria Prezesa Rady Ministrów
Aleje Ujazdowskie 1/3
00-583 Warszawa

WYSTĄPIENIE POKONTROLNE

P/21/081 – Bezpieczeństwo informacji w pracy na odległość i mobilnym przetwarzaniu danych

NAJWYŻSZA IZBA KONTROLI
ul. Filtrowa 57, 02-056 Warszawa
T +48 22 444 50 00, F +48 22 444 57 93
nik@nik.gov.pl
Adres korespondencyjny: Skr. poczt. P-14, 00-950 Warszawa

I. Dane identyfikacyjne

Jednostka kontrolowana	Kancelaria Prezesa Rady Ministrów (dalej: KPRM lub Kancelaria)
Kierownik jednostki kontrolowanej	Michał Dworczyk, Minister – członek Rady Ministrów, wykonujący zadania Szefa KPRM od 19 grudnia 2017 r.
Zakres przedmiotowy kontroli	Monitorowanie przetwarzania przez jednostki administracji publicznej danych w pracy na odległość w celu zachowania bezpieczeństwa informacji.
Okres objęty kontrolą	Lata 2020-2021 (do 16 listopada 2021 r.) z uwzględnieniem zdarzeń wcześniejszych, jeżeli miały one wpływ na kontrolowane obszary działalności.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Olsztynie
Kontrolerzy	1. Zbigniew Wołodko, doradca techniczny, upoważnienie do kontroli nr LOL/106/2021 z 7 września 2021 r. 2. Waldemar Żarnoch, specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/105/2021 z 7 września 2021 r. (akta kontroli str.1-2)

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W opracowanej i przyjętej przez Radę Ministrów w 2019 r. Strategii Cyberbezpieczeństwa RP na lata 2019-2024 określono cele i priorytety służące podniesieniu poziomu bezpieczeństwa teleinformatycznego kraju. Wyznaczono również Plan Działań w aspekcie m.in. podniesienia poziomu odporności systemów informacyjnych administracji publicznej. W Kancelarii Prezesa Rady Ministrów[3] w ograniczonym zakresie monitorowano natomiast zapewnienie przez jednostki administracji publicznej bezpieczeństwa informacji w pracy na odległości i mobilnym przetwarzaniu danych.

[1] Dz. U. z 2020 r. poz. 1200 ze zm., dalej: ustawa o NIK.

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[3] Do 6 października 2020 r. w Ministerstwie Cyfryzacji.

III. Opis ustalonego stanu faktycznego

Opis stanu faktycznego

1. W Strategii Cyberbezpieczeństwa RP na lata 2019-2024[4], uchwalonej 22 października 2019 r. przez Radę Ministrów na podstawie art. 68 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[5], określono (zgodnie z art. 69 ust. 1 tej ustawy) cele strategiczne oraz odpowiednie środki regulacyjne, mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa, w tym maksymalny limit wydatków z budżetu państwa dla określonej części budżetowej. Jako cel główny założono podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym, a także promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. W Strategii wyodrębniono pięć celów szczegółowych, tj.:

- rozwój krajowego systemu cyberbezpieczeństwa (cel szczegółowy nr 1),
- podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty (cel nr 2),
- zwiększanie potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni (3),
- budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa (4),
- zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa (5).

W KPRM określono Plan Działań, o którym mowa w Strategii Cyberbezpieczeństwa (pkt 10 – zarządzanie Strategią Cyberbezpieczeństwa RP). Ujęto w nim zagadnienia dotyczące m.in. podniesienia poziomu bezpieczeństwa teleinformatycznego, w tym poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcia zdolności do skutecznego zapobiegania i reagowania na incydenty. W ramach trzech celów szczegółowych wskazanych w Strategii[6] wyodrębniono 15 zadań do realizacji z określonym harmonogramem (terminem rozpoczęcia i zakończenia podejmowanej inicjatywy), oczekiwanymi efektami wynikającymi z ich realizacji oraz szacunkowym kosztem wykonania. Wskazane w tym Planie działania związane z zapewnieniem bezpieczeństwa przetwarzania informacji przez jednostki administracji publicznej dotyczyły m.in.:

- Opracowania standardów cyberbezpieczeństwa i rekomendacji oraz zestawów dobrych praktyk na potrzeby jednostek samorządu terytorialnego. Datą rozpoczęcia realizacji był pierwszy kwartał 2020 r., a zakończenie zaplanowano na czwarty kwartał 2024 r. Efektem ich przygotowania, w ramach działań statutowych Kancelarii, ma być zbiór standardów cyberbezpieczeństwa dla jednostek samorządu terytorialnego, w tym m.in. bezpieczeństwo pracy zdalnej, stacji roboczych, urządzeń oraz aplikacji mobilnych. Wskazano również, że jednostki te regularnie będą otrzymywać zestawy poradników oraz dobrych praktyk.
- Utworzenia siedmiu Regionalnych Centrów Cyberbezpieczeństwa (tzw. RegioSOC), działających na poziomie regionalnym wg podziału NUTS 1[7],

[4] Zastąpiła ona Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022.
[5] Dz. U z 2020, poz. 1369.
[6] Cel szczegółowy 1 - Rozwój krajowego systemu cyberbezpieczeństwa; cel szczegółowy 2 - Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydent; cel szczegółowy 4 – Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa.
[7] NUTS 1 – makroregiony (grupujące województwa) – 7 jednostek.

odpowiedzialnych za wsparcie dla gmin, powiatów, urzędów marszałkowskich oraz szpitali, czy szkół. Datą rozpoczęcia realizacji będzie pierwszy kwartał 2022 r., a zakończenia czwarty kwartał 2024 r. Szacunkowy koszt wykonania działania przewidziano w kwocie 140,0 mln zł (ujęty w Krajowym Planie Odbudowy).

W ww. dokumentacji nie określono zasad monitorowania przetwarzania przez jednostki administracji publicznej danych w pracy na odległość w celu zachowania bezpieczeństwa informacji.

(akta kontroli str. 3-48)

2. Zgodnie z punktem 10 Strategii Cyberbezpieczeństwa po dwóch latach od przyjęcia oraz w czwartym roku obowiązywania, dokument ten podlega przeglądowi i ocenie efektów jego oddziaływania, a wyniki tego przeglądu przedstawiane są Radzie Ministrów.

W poszczególnych latach objętych kontrolą w KPRM nie dokonywano przeglądu i oceny efektów oddziaływania Strategii. Dyrektor Generalna Kancelarii wyjaśniła, że z uwagi na to, że jest to dokument ramowy i horyzontalny, w ocenie Departamentu Cyberbezpieczeństwa KPRM nie zaistniały dotychczas okoliczności wskazujące na konieczność jego aktualizacji. Będzie ona poddana przeglądowi w określonym terminie, tj. po dwóch latach od jej przyjęcia, a w przypadku wystąpienia uzasadnionych okoliczności może to nastąpić w innych terminach niż te, o których mowa w dokumentacji.

(akta kontroli str. 26-27, 41-42, 191-192)

3. Departament Cyberbezpieczeństwa KPRM opracował i udostępnił Narodowe Standardy Cyberbezpieczeństwa (dalej: NSC), tj. zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informatycznych wykorzystywanych przez podmioty mające zamiar efektywnie zarządzać systemami bezpieczeństwa informacji. Zaprezentowane publikacje[8] stanowiły przewodniki metodyczne, posiadające strukturę odpowiadającą Polskim Normom, stosowanym w zarządzaniu bezpieczeństwem informacji przez podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty realizujące zadania publiczne, operatorów usług kluczowych i dostawców usług cyfrowych. Na zestaw publikacji specjalnych składały się:

- Standardy kategoryzacji bezpieczeństwa,
- Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych,
- Poradnik Planowania Awaryjnego,
- Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu,
- Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji,
- Zabezpieczenia bazowe systemów informatycznych oraz organizacji,
- Mapowanie środków bezpieczeństwa,
- Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego (część I i II),
- Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego,
- Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania”,

[8] Dostępne na portalu: https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber

– Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.

W Kancelarii opracowano również propozycje i zalecenia dotyczące bezpieczeństwa pracy zdalnej, w tym rozwiązań organizacyjnych i technicznych w czasie epidemii Covid-19 oraz rekomendacje działań. Dotyczyły one tzw. cyberhigieny w czasie pracy zdalnej, tj. m.in. korzystania z domowej sieci Wi-Fi, wdrożenia VPN[9], dwuskładnikowego uwierzytelniania, tworzenia kopii zapasowych, niekorzystania z publicznych otwartych sieci Wi-Fi oraz nieużywania prywatnych skrzynek pocztowych, czy grup na portalach społecznościowych do komunikacji firmowej, a także stosowania się do wytycznych pracodawcy oraz wykorzystywania do pracy tylko komputera i telefonu firmowego. Wskazano na zadbanie o *bezpieczeństwo* urządzeń w sieci domowej, w tym silne hasło do sieci Wi-Fi oraz aktualizacje oprogramowania urządzeń, pracy przy użyciu e-mail oraz komunikatorów, chmury i narzędzi do pracy zdalnej (Microsoft, Cisco, Google). Opisane zostały podstawowe funkcjonalności systemów do prowadzenia wideokonferencji: Cisco Webex, czy MS Teams. Możliwość nagrywania rozmów oraz spotkań uwzględniono także w rekomendacjach skierowanych dla nauczycieli prowadzących lekcje online. Jako narzędzie pracy zdalnej wskazano ww. narzędzie MS Teams z informacją, że lekcje mogą być nagrywane i odtworzone w trybie offline w dowolnym momencie[10]. Informacje te udostępniono od marca 2020 r. poprzez ich publikację w Internecie[11].

(akta kontroli str. 49-53, 56-79, 184-190)

4. W okresie objętym kontrolą w KPRM nie gromadzono danych dotyczących skali wdrożenia pracy zdalnej w jednostkach administracji publicznej. Nie monitorowano również sposobu wdrożenia przez te jednostki zaleceń i rekomendacji działań dotyczących podniesienia poziomu bezpieczeństwa teleinformatycznego, w tym m.in. narodowych standardów cyberbezpieczeństwa.

Dyrektor Generalna w Kancelarii poinformowała m.in., że jednostka nie prowadziła zadań koncentrujących się w szczególności na bezpieczeństwie przetwarzania przez jednostki administracji publicznej danych w pracy na odległość.

Podsekretarz Stanu w KPRM wyjaśnił również m.in., że przepisy prawa nie nakładają na ministra właściwego do spraw informatyzacji, ani na Pełnomocnika Rządu do spraw Cyberbezpieczeństwa obowiązku gromadzenia informacji w przedmiotowym zakresie. Minister właściwy do spraw informatyzacji ma uprawnienia do przeprowadzania kontroli nie we wszystkich podmiotach realizujących zadania publiczne, ale tylko w tych, co do których nie są właściwe inne organy administracji rządowej. Pełnomocnik ds. Cyberbezpieczeństwa realizuje swoje zadania z wykorzystaniem zagregowanych danych i wskaźników opracowanych z udziałem organów administracji publicznej, organów właściwych do spraw cyberbezpieczeństwa, CSIRT MON – Ministra Obrony Narodowej, CSIRT GOV – Szefa Agencji Bezpieczeństwa Wewnętrznego oraz CSIRT NASK – Naukowej i Akademickiej Sieci Komputerowej Państwowego Instytutu Badawczego[12]. Dodał także, że dane o zakresie i skali wdrożenia pracy zdalnej

[9] VPN - bezpieczny kanał komunikacji. Określany jest mianem „bezpiecznego tunelu w sieci", który umożliwia organizacji prowadzić zaszyfrowaną komunikację podczas użytkowania usług sieciowych. Zastosowanie VPN w ramach infrastruktury sieciowej firmy oznacza: prowadzenie szyfrowanej komunikacji w sieci, uzyskanie bezpiecznego połączenia w trakcie użytkowania Internetu i prowadzenia komunikacji między użytkownikami, zapewnienie silnej ochrony przed wyciekami lub kradzieżą danych oraz monitorowanie w czasie rzeczywistym potencjalnych zagrożeń. Wdrożenie VPN w sieci firmowej pozwala pracownikom wykonywać poszczególne czynności zdalnie dzięki połączeniu się wirtualnie z siecią. Okazuje się przydatna zwłaszcza podczas podróży służbowych oraz pracy pomiędzy zespołami z różnych oddziałów firmy.

[10] Np. do użytku ucznia, np. w celu powtórzenia omawianego przez nauczyciela materiału.

[11] Cyfryzacja KPRM Portal Gov.pl - https://www.gov.pl/web/cyfryzacja/razem-ale-osobno--to-powinniscie-wiedziec-o-pracy-zdalnej.

[12] CSIRT – Computer Security Incident Response Team, tj. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego. Ustanowione zostały trzy takie zespoły: CSIRT NASK, CSIRT GOV oraz CSIRT MON. Każdy

można jedynie postrzegać w kategorii czynników ryzyka, które winny być brane pod uwagę przez właściwe podmioty przy zarządzaniu ryzykiem. Zapewnienie bezpieczeństwa informacji i przetwarzania danych w jednostkach administracji publicznej jest obowiązkiem tych jednostek.

Według uzyskanych w toku kontroli wyjaśnień, wszelkie rekomendacje w zakresie podniesienia poziomu bezpieczeństwa teleinformatycznego są jedynie zaleceniami i dobrymi praktykami, które mają ułatwić podmiotom realizującym zadania publiczne wypełnienie leżących w ich zakresie obowiązków wynikających z przepisów prawa. Z tego powodu KPRM nie monitoruje stopnia wdrożenia ww. zaleceń.

Najwyższa Izba Kontroli przyjmuje ww. wyjaśnienia, że przepisy nie nakładają obowiązku gromadzenia informacji w przedmiotowym zakresie, a zapewnienie bezpieczeństwa informacji i przetwarzania danych w jednostkach administracji publicznej należy do tych jednostek. Należy jednak zauważyć, że to minister właściwy do spraw informatyzacji i Pełnomocnik Rządu do spraw Cyberbezpieczeństwa odpowiadają za projektowanie rozwiązań w tym zakresie, przedkładanych następnie organom stanowiącym przepisy prawa. Zdaniem Izby, w celu prowadzenia skutecznego nadzoru nad wykonywaniem zadań publicznych pożądane byłoby więc pozyskiwanie danych dotyczących zakresu wdrożenia pracy zdalnej w poszczególnych jednostkach administracji publicznej, w tym sposobu wykorzystywania systemów i urządzeń teleinformatycznych do przetwarzania informacji w pracy na odległość. Posiadanie takich danych umożliwiałoby bowiem określenie skali wykorzystywania tych urządzeń, w tym prawidłowego użytkowania prywatnego sprzętu teleinformatycznego do celów służbowych w aspekcie bezpieczeństwa informacji. Istotne jest również monitorowanie stosowania określonych rozwiązań teleinformatycznych, w tym wytycznych i rekomendacji działań w czasie pandemii Covid-19. Mogłyby one także pozwolić na wcześniejsze rozpoznanie zagrożeń i sformułowanie dodatkowych wskazówek zapobiegających ewentualnym incydentom i tym samym wpływać na podniesienie poziomu cyberbezpieczeństwa.

Podkreślenia wymaga również, że dane o zakresie i skali wdrożenia pracy zdalnej w jednostkach administracji publicznej powinny być wykorzystywane m.in. do analizy ryzyka dotyczącego zapewnienia bezpieczeństwa informacji, nie tylko w odniesieniu do poszczególnych podmiotów, ale również w aspekcie strategicznym, tj. w odniesieniu do zadań realizowanych ministra właściwego do spraw informatyzacji.

(akta kontroli str. 41-42, 80-88)

Z danych posiadanych przez Departament Cyberbezpieczeństwa KPRM, przekazanych przez CSIRT NASK wynikało, że w 2020 r. wystąpiło 388 incydentów dotyczących bezpieczeństwa danych w administracji publicznej, a w 2021 r. (do 31 sierpnia) odnotowano 287 takich incydentów.

Dyrektor Departamentu Cyberbezpieczeństwa KPRM poinformował m.in., że Departament nie ma wiedzy dotyczącej incydentów zgłoszonych w latach 2020 – 2021 do CSIRT-ów poziomu krajowego, które mogły mieć wpływ na bezpieczeństwo informacji oraz które związane były z wykonywaniem pracy zdalnej lub mobilnym przetwarzaniem danych w jednostkach administracji publicznej. Do Ministra Cyfryzacji jako organu właściwego do spraw cyberbezpieczeństwa dla sektora infrastruktura cyfrowa CSIRT-y poziomu krajowego przekazują informacje dotyczące jedynie liczby zgłoszonych incydentów w podziale na sektory gospodarki, w tym

z nich odpowiedzialny jest za różne incydenty zgłaszane przez podmioty przyporządkowane według ustawy o krajowym systemie cyberbezpieczeństwa. Zespoły te współpracują ze sobą oraz z podobnymi zespołami na świecie w celu zapewnienia bezpieczeństwa sieci wewnętrznych oraz wykrywaniu zagrożeń w sieci publicznej. Podmiot publiczny zgłasza do właściwego CSIRT-u incydenty w podmiocie publicznym.

administrację publiczną, bez informacji czego incydent cyberbezpieczeństwa dotyczył. Podał również, że CSIRT-y poziomu krajowego nie są zobligowane do przekazywania szczegółowych informacji o incydentach do organów właściwych.

(akta kontroli str. 89-91)

5. W okresie objętym kontrolą KPRM przeprowadziła jedną kontrolę[13] dotyczącą wykorzystania systemów teleinformatycznych do realizacji zadań publicznych. Objęto nią Ministerstwo Rodziny i Polityki Społecznej (dalej: MRiPS lub Ministerstwo). W wyniku tej kontroli, obejmującej okres od 6 października 2020 r. do 30 lipca 2021 r., pozytywnie oceniono działania Ministerstwa mające na celu zapewnienie bezpieczeństwa informacji w aspekcie zarządzania infrastrukturą informatyczną. Dotyczyły one m.in. bezpieczeństwa pracy zdalnej, zabezpieczenia dostępu do systemów i nadania uprawnień, wdrożenia rozwiązań monitorujących ruch osobowy w obiektach MRiPS, monitorowania systemów teleinformatycznych i środowiska ich pracy, a także działań użytkowników w tych systemach oraz zapewnienia przejrzystego procesu wdrażania zmian w systemach i tworzenia kopii zapasowych. Ustalono również, że dla pełnego wdrożenia kompleksowego i spójnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI) niezbędne jest opracowanie całościowej analizy ryzyka w stosunku do wszystkich aktywów Ministerstwa, kompleksowej dokumentacji SZBI oraz wdrożenia narzędzi nadzorczych dostarczających całościowych informacji na temat poszczególnych etapów jego ustanowienia.

(akta kontroli str. 54, 92-120)

6. W I półroczu 2020 r. Ministerstwo Cyfryzacji[14] przedstawiło informacje zawierające szczegółowe opisy funkcjonalne oraz scenariusze implementacyjne w odpowiedzi na dwa wnioski złożone w sprawie rekomendowanych rozwiązań teleinformatycznych w czasie pandemii Covid-19[15]. W wyniku ich rozpatrzenia wskazano na możliwości wykorzystania oprogramowania i licencji do telepracy grupowej oraz wspomagania teleinformatycznego obszaru back-office[16], które umożliwiają m.in. testy, weryfikację rozwiązań i usług przed podjęciem decyzji o ich zastosowaniu w docelowym środowisku urzędu. Określono, że zakres modelowych działań podjętych w celu organizacji bezpiecznego środowiska i utrzymania ciągłości działania jednostek administracji rządowej dla efektywnej pracy komórek merytorycznych podczas epidemii Covid-19 powinien obejmować pięć podstawowych obszarów:

- zabezpieczenie urządzeń mobilnych i zdalnego dostępu do środowiska urzędu,
- elektroniczne zarządzanie dokumentacją,
- usługi wideokonferencyjne,
- komunikację administracji rządowej z obywatelami,
- dostęp do zapasowej infrastruktury teleinformatycznej – usługi chmurowe.

[13] Kontrolę przeprowadzili pracownicy Departamentu Nadzoru i Kontroli KPRM. Czynności kontrolne realizowano od 27 maja do 16 lipca 2021 r.

[14] Jednostka została zniesiona 7 października 2020 r. z mocą obowiązującą od dnia poprzedniego, na mocy rozporządzenia Rady Ministrów z dnia 7 października 2020 r. w sprawie zniesienia Ministerstwa Cyfryzacji, zgodnie z którym dotychczasowi pracownicy ministerstwa z działu informatyzacja zostali włączeni do KPRM i na podstawie rozporządzenia Prezesa Rady Ministrów z dnia 6 października 2020 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji - Kancelaria Prezesa Rady Ministrów zapewnia obsługę ministra.

[15] Pismo z 6 kwietnia 2020 r. w sprawie problemów w funkcjonowaniu samorządów lokalnych w związku z epidemią Covid-19 i rozwiązań dla jednostek samorządu terytorialnego Stowarzyszenie Gmin i Powiatów Wielkopolski oraz pismo nr IK 471365 z 8 kwietnia 2020 r. w sprawie rekomendowanych rozwiązań teleinformatycznych w stanie pandemii Covid-19.

[16] Back-office to wydzielona część korporacji, gdzie przeprowadzane są procesy dotyczące wsparcia w prawidłowym i sprawnym funkcjonowaniu współczesnej organizacji.

Przygotowując rekomendację do prowadzenia pracy zdalnej w środowisku cyfrowym Ministerstwo Cyfryzacji uwzględniło również następujące aspekty:

- wyposażenie pracowników w mobilne urządzenia służbowe – komputery i smartfony oraz wykorzystanie urządzeń prywatnych do komunikacji służbowej,
- zapewnienie bezpiecznego szyfrowania dostępu (VPN) do zasobów informacyjnych organizacji,
- uzgodnienie kanałów komunikacyjnych – e-mail, telefon, komunikatory w aplikacjach wideokonferencyjnych,
- wykorzystanie bezpłatnych, ale zweryfikowanych pod kątem bezpieczeństwa (w szczególności w zakresie europejskich wymagań ochrony danych osobowych) narzędzi do pracy grupowej, umożliwiających: szyfrowaną rozmowę pomiędzy pracownikami, zorganizowanie wideokonferencji wewnętrznej i publicznej oraz jednoczesną pracę nad dokumentami.

(akta kontroli str. 55-121-183)

IV. Uwagi

Uwaga

Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następującą uwagę:

Zdaniem Najwyższej Izby Kontroli wskazane byłoby gromadzenie w KPRM danych o skali wdrożenia pracy na odległość w jednostkach administracji publicznej, a także monitorowanie sposobu wykorzystania opracowanych przez KPRM rekomendacji i wytycznych w czasie pandemii Covid-19 w celu skutecznego nadzoru oraz podniesienia poziomu bezpieczeństwa informacji.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do Prezesa NIK. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykorzystania uwagi

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwagi oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Warszawa, 6 grudnia 2021 r.

Wiceprezes
Najwyższej Izby Kontroli
Małgorzata Motylow

.....
podpis