LOL.430.001.2022
Nr ewid. 7/2022/P/21/081/LOL

Informacja o wynikach kontroli

BEZPIECZEŃSTWO INFORMACJI W PRACY NA ODLEGŁOŚĆ I MOBILNYM PRZETWARZANIU DANYCH

DELEGATURA W OLSZTYNIE

MISJĄ
Najwyższej Izby Kontroli jest niezależna, profesjonalna kontrola zadań publicznych w interesie obywateli i państwa

Informacja o wynikach kontroli
Bezpieczeństwo informacji w pracy na odległość i mobilnym przetwarzaniu danych

Dyrektor Delegatury NIK w Olsztynie

Piotr Górny

Akceptuję:
Wiceprezes Najwyższej Izby Kontroli

Małgorzata Motylow

Zatwierdzam:
Prezes Najwyższej Izby Kontroli

Marian Banaś
Warszawa, dnia 05.04.2022

Najwyższa Izba Kontroli
ul. Filtrowa 57
02-056 Warszawa
T/F +48 22 444 50 00
www.nik.gov.pl

SPIS TREŚCI

Zdjęcie na okładce:
adobe.stock/oliver de la haye

Wykaz stosowanych skrótów, skrótowców i pojęć

COVID-19	Ostra choroba zakaźna układu oddechowego COVID-19, wywoływana przez wirusa SARS-CoV-2 (stan epidemii wprowadzono w Polsce 20 marca 2020 r., a wcześniej – 14 marca 2020 r. – stan zagrożenia epidemicznego)[1].
Polecenie pracy zdalnej	Polecenie pracodawcy, kierujące pracownika do wykonywania przez czas oznaczony, pracy określonej w umowie o pracę, poza miejscem jej stałego wykonywania, o którym mowa w art. 3 ust. 1 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych.
Praca zdalna lub praca w formie zdalnej lub praca na odległość	Praca określona w umowie o pracę, wykonywana przez czas oznaczony poza miejscem jej stałego wykonywania, na podstawie polecenia pracodawcy, stosownie do ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych.
Pulpit zdalny	Pulpit zdalny to usługa, która pozwala na uzyskanie dostępu do komputera za pomocą innego komputera. Pulpit zdalny może być wykorzystywany do pracy zdalnej. Usługa ta pozwala na podłączenie się do komputera znajdującego się w biurze ze sprzętu znajdującego się w domu pracownika.
Ustawa Covid-19	Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2021 r. poz. 2095 t.j.).
Rozporządzenie KRI	Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247).
Systemy dziedzinowe (informatyczne)	Systemy, programy i aplikacje wykorzystywane w jednostkach kontrolowanych do realizacji podstawowych zadań.
SZBI	System Zarządzania Bezpieczeństwem Informacji.
VPN	Wirtualna sieć prywatna, szyfrowane połączenie umożliwiające bezpieczną transmisję danych.

[1] § 1 rozporządzenia Ministra Zdrowia z dnia 20 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii (Dz. U. poz. 491, ze zm.) oraz § 1 rozporządzenia Ministra Zdrowia z dnia 13 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu zagrożenia epidemicznego (Dz. U. poz. 433).

1. WPROWADZENIE

Pytanie definiujące cel główny kontroli

Czy podmioty realizujące zadania publiczne zapewniły aktualność rozwiązań w Systemie Zarządzania Bezpieczeństwem Informacji, umożliwiających bezpieczne przetwarzanie informacji w przypadku wprowadzenia trybu pracy zdalnej?

Pytania definiujące cele szczegółowe kontroli

1. Czy monitorowano sposób przetwarzania przez jednostki administracji publicznej danych w pracy na odległość w celu zachowania bezpieczeństwa informacji?
2. Czy zapewniono należytą organizację bezpieczeństwa informacji?
3. Czy opracowane rozwiązania techniczne i organizacyjne wdrożono, stosowano i egzekwowano?

Jednostki kontrolowane

- Kancelaria Prezesa Rady Ministrów (jednostka monitorująca szczebla centralnego),
- Izba Administracji Skarbowej w Olsztynie,
- dwie jednostki wojewódzkiej administracji zespolonej,
- dwie jednostki samorządu terytorialnego szczebla powiatowego,
- pięć jednostek samorządu terytorialnego szczebla gminnego.

Okres objęty kontrolą

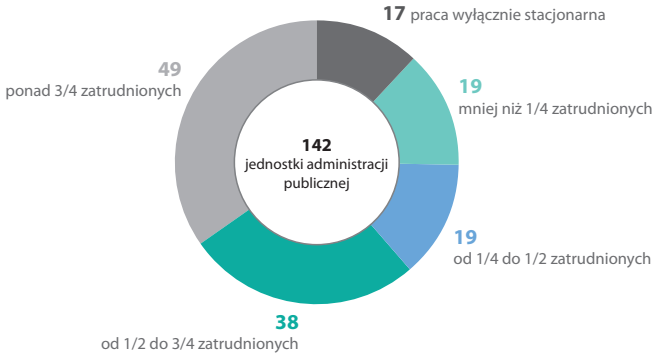
1 stycznia 2020 r.– –30 listopada 2021 r.[2]

Sprawne funkcjonowanie instytucji publicznych jest w dzisiejszym świecie niemożliwe bez zastosowania technologii informatycznych. Korzyści wynikające z ich stosowania to przede wszystkim ułatwienia w zakresie gromadzenia, wyszukiwania i przetwarzania informacji, możliwość łączenia i wykorzystywania informacji rozproszonych, gromadzonych przez różne instytucje. To również możliwość wykonywania zadań przez pracowników tych instytucji w systemie pracy na odległość, za pomocą odpowiednich urządzeń teleinformatycznych. Po drugiej stronie korzyści stoją zagrożenia, wśród których jednym z najistotniejszych jest bezpieczeństwo informacji. Informacja bezpieczna jest wówczas, gdy w procesach przetwarzania następuje gromadzenie informacji kompletnej, niesprzecznej, w sposób czytelny, we właściwym miejscu, formie i czasie. Również wtedy, gdy przekazywana jest właściwym adresatom, w terminie, odpowiednim kanałem oraz w tajemnicy przed niepożądanymi adresatami. Informacja powinna być zatem przetwarzana z zachowaniem zasady poufności oraz w taki sposób, aby ci którzy powinni mieli do niej dostęp.

Sytuacja związana z pandemią COVID-19 wymusiła na wielu podmiotach, również realizujących zadania publiczne, wprowadzenie pracy na odległość (zdalnej) jako rozwiązania zapewniającego przede wszystkim izolację i dystans społeczny, ale też ciągłość funkcjonowania i możliwość realizacji zadań. Ta nowa dla administracji publicznej forma pracy stanowiła duże wyzwanie dla tych podmiotów. Wymagała bowiem niemal natychmiastowej zmiany w podejściu do organizacji pracy, aktualizacji systemów zarządzania bezpieczeństwem informacji, czy też podjęcia działań w celu zapewnienia pracownikom narzędzi do wykonywania zadań w takiej formie. Wprowadzenie pracy zdalnej skutkuje również szeregiem ryzyk i zagrożeń dla bezpieczeństwa informacji, do której wielu pracowników wykonujących swoje zadania uzyskało dostęp w innym trybie niż dotychczas.

Informacje dotyczące zakresu pracy zdalnej Najwyższa Izba Kontroli uzyskała w trybie art. 29 ust. 1 pkt 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3] w maju 2021 r. od 142 wybranych jednostek wykonujących zadania publiczne w województwie warmińsko-mazurskim.

Infografika nr 1
Wykorzystanie możliwości pracy zdalnej wg liczby jednostek



Źródło: opracowanie własne.

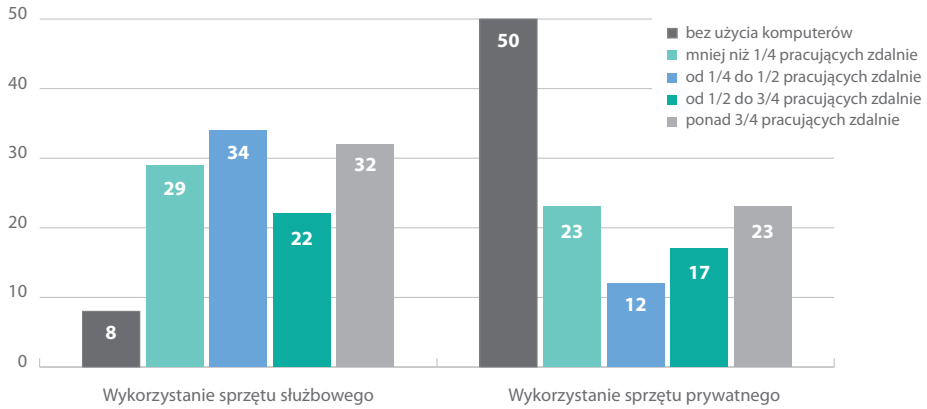
[2] Tj. do dnia zakończenia czynności kontrolnych w jednostkach kontrolowanych.

[3] Dz. U. z 2020 r. poz. 1200, ze zm.

Uzyskane informacje pozwoliły również na zobrazowanie skali wykorzystania komputerów prywatnych w pracy wykonywanej w trybie pracy zdalnej, co stanowiło dodatkowe ryzyko w zapewnieniu bezpiecznego przetwarzania informacji. Na wykresie poniżej zaprezentowano liczbę jednostek oraz udział pracowników wykonujących pracę w trybie zdalnym, wykorzystujących sprzęt komputerowy w podziale na służbowy i prywatny.

Infografika nr 2

Liczba jednostek, w których określona częśc pracowników zdalnych wykorzystywała sprzęt komputerowy z podziałem na służbowy i prywatny



Źródło: opracowanie własne.

Dane te były jednym z kryteriów, według których dokonano wyboru jednostek do kontroli.

2. OCENA OGÓLNA

Niekompletne zarządzanie bezpieczeństwem informacji w pracy zdalnej

System zarządzania bezpieczeństwem informacji w pracy na odległość nie był prawidłowo zorganizowany, gdyż nie zapewniał właściwego poziomu bezpieczeństwa każdego rodzaju danych. Wprawdzie w kontrolowanych jednostkach ustanawiano i wdrażano zasady w tym zakresie, niemniej często nie były one przestrzegane oraz aktualizowane. Zabrakło również monitorowania i ewentualnego korygowania na poziomie centralnym wytycznych dotyczących zapewnienia bezpieczeństwa przetwarzania informacji.

Niewłaściwie zarządzano bezpieczeństwem informacji, ponieważ w połowie skontrolowanych podmiotów nie opracowano i nie wdrożono wymaganego przepisami rozporządzenia KRI systemu zarządzania bezpieczeństwem informacji (SZBI), w którym należało określić sposób postępowania ze wszystkimi kategoriami przetwarzanych informacji. W jednostkach tych ograniczono się do ustalenia zasad dotyczących bezpieczeństwa danych osobowych. W części urzędów nie dokonywano przeglądów regulacji dotyczących zarządzania bezpieczeństwem informacji oraz nie dokonywano ich aktualizacji. W ograniczonym zakresie wykorzystywano zewnętrzny audyt bezpieczeństwa systemów informatycznych. W jednym z urzędów, w których regulacje wewnętrzne umożliwiały wykorzystywanie w pracy zdalnej prywatnych komputerów, nie określono w tym zakresie szczegółowych wymagań dotyczących zasad zapewnienia pożądanego poziomu ochrony informacji.

Część jednostek nie stosowała także ustalonych własnych zasad i regulacji, obniżając skuteczność przyjętych rozwiązań w obszarze bezpieczeństwa informacji. Stwierdzone nieprawidłowości dotyczyły m.in. nieprzestrzegania wymogu pracy na indywidualnych kontach systemu operacyjnego, braku szyfrowania dysków twardych komputerów wykorzystywanych w pracy zdalnej, a także nieprzestrzegania przyjętych zasad postępowania z zewnętrznymi nośnikami danych.

W Kancelarii Prezesa Rady Ministrów, jako jednostce obsługującej Prezesa Rady Ministrów, aktualnie pełniącego funkcję ministra cyfryzacji, opracowano i upubliczniono rozwiązania będące zbiorem zaleceń i dobrych praktyk dotyczących pracy na odległość w czasie pandemii Covid-19. Nie gromadzono jednak danych o skali wdrożenia pracy zdalnej w jednostkach administracji publicznej, a także nie monitorowano i nie weryfikowano sposobu ich wdrożenia. Zdaniem NIK posiadanie takich danych mogłoby pozwolić na rozpoznawanie zagrożeń i korygowanie lub uzupełnianie opracowanych rozwiązań. Dane w tym zakresie powinny być także wykorzystywane nie tylko w odniesieniu do poszczególnych podmiotów, ale również w aspekcie strategicznym, tj. w odniesieniu do realizowanych zadań ministra właściwego do spraw informatyzacji, w celu podnoszenia poziomu cyberbezpieczeństwa.

3. SYNTEZA WYNIKÓW KONTROLI

Działania w celu podniesienia poziomu odporności systemów informatycznych

W celu podniesienia poziomu odporności systemów informatycznych administracji publicznej opracowane zostały Narodowe Standardy Cyberbezpieczeństwa, mające wpłynąć przede wszystkim na zwiększenie odporności systemów teleinformatycznych administracji publicznej. Jest to zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informatycznych skierowanych do podmiotów mających zamiar efektywnie zarządzać systemami bezpieczeństwa informacji. Zaprezentowane publikacje stanowiły przewodniki metodyczne, zalecane do stosowania 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 m.in. standardy kategoryzacji bezpieczeństwa, minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych oraz poradnik planowania awaryjnego. [str. 14]

Rekomendacje działań dla bezpieczeństwa pracy zdalnej

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, 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. [str. 15–16]

Ograniczony monitoring sposobu przetwarzania danych w pracy na odległość

KPRM nie prowadziła zadań koncentrujących się na bezpieczeństwie przetwarzania przez jednostki administracji publicznej danych w pracy na odległość. W ograniczonym zakresie monitorowano zapewnienie przez te jednostki bezpieczeństwa informacji w pracy na odległość i mobilnym przetwarzaniu danych. Wprawdzie opracowano procedury dotyczące rozwiązań teleinformatycznych możliwych do zastosowania w czasie pandemii Covid-19, w tym szczegółowe wytyczne i rekomendacje działań, jednak nie posiadano danych o skali wdrożenia pracy zdalnej w tych jednostkach. Nie monitorowano również sposobu wdrożenia przez te jednostki zaleceń i rekomendacji działań dotyczących podniesienia poziomu bezpieczeństwa teleinformatycznego, w tym m.in. narodowych standardów cyberbezpieczeństwa.

Dotychczas w jednym podmiocie Kancelaria przeprowadziła kontrolę dotyczącą wykorzystania systemów teleinformatycznych do realizacji zadań publicznych, w tym bezpieczeństwa informacji w pracy zdalnej. Objęto nią Ministerstwo Rodziny i Polityki Społecznej. W jej wyniku pozytywnie oceniono działania Ministerstwa mające na celu zapewnienie bezpieczeństwa informacji w aspekcie zarządzania infrastrukturą informatyczną. [str. 16–17]

SYNTEZA WYNIKÓW KONTROLI

Zdaniem NIK, pomimo braku obowiązku gromadzenia informacji dotyczących skali wdrożenia pracy zdalnej w jednostkach administracji publicznej, w celu monitorowania zadań publicznych pożądane byłoby 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. Stosowne działania, w ramach swoich uprawnień, mógłby również podjąć Pełnomocnik Rządu do spraw Cyberbezpieczeństwa, do którego kompetencji należy m.in. inicjowanie rozwiązań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym[4]. 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.

Systemy Zarządzania Bezpieczeństwem Informacji

Wyniki kontroli wskazują na występowanie zagrożeń dla bezpieczeństwa informacji, w tym także w pracy zdalnej, które wynikają przede wszystkim z nierealizowania obowiązków wynikających z rozporządzenia KRI. W połowie urzędów objętych kontrolą (5 z 10) nie opracowano, nie ustanowiono i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji (w tym Polityki Bezpieczeństwa Informacji), stosownie do przepisów tego rozporządzenia. Regulacje, które zostały opracowane i wdrożone w tych urzędach nie obejmowały swoim zakresem wszystkich kategorii przetwarzanych informacji, bowiem zawierały deklaracje stosowania ich jedynie do informacji zawierających dane osobowe. [str. 18–19]

Określenie ról i odpowiedzialności

Odpowiedzialność za poszczególne elementy systemów bezpieczeństwa informacji przydzielana była pracownikom stosownie do zakresu czynności i funkcji pełnionej w urzędzie w takim zakresie jaki obejmowały regulacje wewnętrzne. Wyznaczono inspektorów ochrony danych oraz przypisano im zadania i obowiązki wymagane rozporządzeniem RODO[5]. Pracownikom wykonującym zadania w zakresie obsługi informatycznej, w tym administratorom systemów informatycznych przypisano m.in. odpowiedzialność za prawidłowe działanie tych systemów oraz zapewnienie bezpieczeństwa danych w nich przetwarzanych. Zobowiązano ich do przestrzegania reguł i stosowania procedur określonych w instrukcjach zarządzania systemem informatycznym.

---

[4] Art. 62 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, ze zm.).

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz 127 z 23.05.2018, str. 2.).

Jednak nie wszystkie zadania, które miały wpływ na prawidłowe zarządzanie bezpieczeństwem informacji zostały przypisane. Stwierdzono bowiem, że w jednej jednostce nie wyznaczono osoby odpowiedzialnej za aktualizacje Polityki bezpieczeństwa informacji, a w innej nie określono odpowiedzialności za zapewnienie zgodności Polityki bezpieczeństwa informacji z wymaganiami normy PN-EN ISO/IEC 27001 określonej w rozporządzeniu KRI. [str. 19]

Zapewnienie ochrony danych osobowych

Wszystkie kontrolowane jednostki posiadały ustanowione i wdrożone Polityki Ochrony Danych Osobowych. Wskazano w nich administratora danych osobowych, tj. podmiot odpowiedzialny za ustalanie celów i sposobów przetwarzania tych danych. Zgodnie z art. 37 ust. 1 lit. a rozporządzenia RODO w zw. z art. 8 i 9 ustawy z 10 maja 2018 r. o ochronie danych osobowych[6] wyznaczono inspektorów ochrony danych i określono zakresy ich obowiązków wynikające z art. 39 ust. 1 tego rozporządzenia. Część urzędów funkcje inspektorów ochrony danych powierzało zatrudnionym pracownikom, a część osobom zatrudnionym w podmiotach zewnętrznych, z którymi zawierano stosowne umowy w tym zakresie. [str. 19–20]

Zasady postępowania z nośnikami, wynoszenia aktywów i przesyłania informacji

Wszystkie skontrolowane jednostki posiadały ustanowione i wdrożone reguły dotyczące postępowania z nośnikami danych, jednak w pięciu z nich reguły te zawierały postanowienia zobowiązujące wyłącznie do stosowania ich w odniesieniu do nośników zawierających dane osobowe. Zasady wynoszenia aktywów określono we wszystkich jednostkach. Przyjęto w nich ogólny zakaz wynoszenia dokumentacji papierowej. Procedury bezpiecznej eksploatacji komputerów przenośnych w siedmiu jednostkach określono w przyjętych politykach, a w trzech uzupełniono w zarządzeniach i regulaminach wprowadzających pracę zdalną. W zasadach przesyłania informacji niezbędnych do wykonywania zadań w trybie pracy zdalnej dopuszczono stosowanie poczty elektronicznej oraz szyfrowanych połączeń VPN umożliwiających dostęp do usług pulpitu zdalnego udostępnianych z komputerów stacjonarnych użytkowanych przez pracowników pracujących na odległość.

W jednym z kontrolowanych urzędów nie określono warunków korzystania z prywatnych kont pocztowych, pomimo dopuszczenia takiej możliwości w pracy zdalnej. [str. 20–22]

Zarządzanie incydentami bezpieczeństwa

Zarządzanie incydentami bezpieczeństwa informacji realizowane było w niepełnym zakresie. Połowa skontrolowanych urzędów, ustanawiając zasady obowiązujące w tym zakresie, ograniczyła je do przypadków związanych z ochroną danych osobowych. W pozostałych jednostkach regulacje obejmujące zgłaszanie i obsługę incydentów oraz prowadzenie rejestrów tych zdarzeń obejmowały bezpieczeństwo informacji w szerokim zakresie. Zarejestrowane w nich zdarzenia nie były związane z pracą zdalną. [str. 22]

Regulaminy pracy zdalnej uzupełniały nieuregulowane aspekty

Wprowadzanie w kontrolowanych urzędach pracy zdalnej i ustanawianie zasad w tym zakresie było procesem rozłożonym w czasie. Początkowe działania koncentrowały się na zapewnieniu dystansu społecznego i ograniczeniu kontaktów pomiędzy pracownikami. Wdrażanie w jednostkach trybu

[6] Dz. U. z 2019 r. poz. 178 t.j.

pracy określanej jako rotacyjna lub naprzemienna nie zapewniało możliwości realizacji dotychczasowych zadań, gdyż praca ta odbywała się bez dostępu do sprzętu komputerowego, systemów informatycznych jednostek i niezbędnych informacji. Wydając odpowiednie zarządzenia i ustanawiając regulaminy kierownicy jednostek kontrolowanych wprowadzali przede wszystkim organizacyjne zasady przechodzenia na pracę zdalną oraz warunki dostępu do niezbędnych narzędzi informatycznych i systemów dziedzinowych. [str. 22–23]

Ograniczone działania szkoleniowe dotyczące bezpieczeństwa informacji

Działania szkoleniowe w zakresie bezpieczeństwa informacji nie zapewniały pracownikom uzyskania pełnej wiedzy o zagrożeniach i sposobach przeciwdziałania ich skutkom. Jednostki kontrolowane, korzystając z różnych rozwiązań i form umożliwiających szkolenia, tj. platform do szkoleń *on-line*, przesyłania prezentacji zawierających materiały szkoleniowe oraz ostrzeżenia przed zagrożeniami podnosiły świadomość pracowników, przede wszystkim w zakresie ochrony danych osobowych. W dwóch urzędach w okresie objętym kontrolą nie organizowano szkoleń dotyczących bezpieczeństwa informacji, a jedyną formą przekazywania wiedzy w tym zakresie było udzielanie przez administratora systemów informatycznych instruktażu w trakcie przekazywania sprzętu. [str. 24]

Brak regularnych przeglądów wdrożonych reguł bezpieczeństwa informacji

Kierownicy jednostek nie dysponowali rzetelną oceną skuteczności stosowanych rozwiązań dotyczących bezpieczeństwa informacji. Tylko trzy jednostki spośród 10 kontrolowanych przeprowadziły w okresie objętym kontrolą zewnętrzny audyt bezpieczeństwa systemów informatycznych. Część jednostek badała ten obszar w ramach audytu wewnętrznego oraz uwzględniała go w przeprowadzanych analizach ryzyka. Dwa urzędy nie posiadały dokumentacji potwierdzającej dokonywanie przeglądów obowiązujących w nich polityk bezpieczeństwa informacji, pomimo określenia takiego obowiązku w § 20 ust. 2 pkt 14 rozporządzenia KRI oraz w Polskiej Normie ISO/IEE27001, która jest wyznacznikiem do stwierdzenia zgodności ustanowionych regulacji z wymaganiami tego rozporządzenia. [str. 25]

Skala pracy zdalnej

W 2020 roku, w 10 kontrolowanych urzędach 612 pracowników spośród 841 zatrudnionych (72,8%) otrzymało co najmniej jedno polecenie pracy zdalnej. W 2021 r. (do 30 listopada) było to 379 na 798 zatrudnionych (47,5%). W początkowym okresie praca zdalna wykonywana była bez wykorzystania urządzeń teleinformatycznych, a następnie wyposażano pracowników w sprzęt służbowy lub zezwalano na używanie prywatnego sprzętu komputerowego. W 2020 r. w służbowy sprzęt komputerowy wyposażono 281, a w 2021 r. 233 pracowników wykonujących pracę zdalną. Z komputerów prywatnych w 2020 r. korzystało 177 pracowników, a 70 w roku 2021. [str. 26–28]

Samokształcenie było podstawową formą poszerzania wiedzy

Większość jednostek egzekwowała od pracowników potwierdzenia o zapoznaniu się z obowiązującymi regułami w zakresie bezpieczeństwa informacji. W jednym z kontrolowanych urzędów w prowadzonej dokumentacji brakowało oświadczeń wymaganych w przyjętej Polityce Bezpieczeństwa Informacji. Większość kontrolowanych jednostek udostępniała materiały szkoleniowe i informacyjne do zapoznania się w formie samokształcenia.

Jedynie dwie jednostki zorganizowały w okresie objętym kontrolą szkolenia w zakresie bezpiecznego łączenia się z siecią wewnętrzną urzędu. [str. 27–28]

Nie w pełni stosowano obowiązujące reguły ochrony informacji

Do udostępnienia usług sieci wewnętrznej jednostki stosowano szyfrowane połączenia VPN, zarówno w przypadku służbowych, jak i prywatnych komputerów. Faktyczny poziom bezpieczeństwa informacji był jednak niższy od zakładanego, gdyż w części jednostek nie szyfrowano dysków komputerów przenośnych, a w jednej nie skonfigurowano indywidualnych kont użytkowników. W jednym urzędzie nie zastosowano ustawień serwerowych wymuszających od użytkowników stosowanie haseł o złożoności wymaganej w regulacjach wewnętrznych. [str. 29–30]

Połowa kontrolowanych urzędów umożliwiła wykorzystywanie sprzętu prywatnego

W celu uzupełnienia braków w zakresie przenośnego sprzętu komputerowego połowa kontrolowanych jednostek uruchomiła rozwiązania pozwalające na korzystanie w pracy zdalnej z komputerów prywatnych. Poprzez zastosowanie rozwiązań teleinformatycznych uruchomiono szyfrowane połączenia do sieci wewnętrznej urzędów umożliwiające dostęp do systemów dziedzinowych. W czterech urzędach komputery prywatne wykorzystywane były do realizacji zadań niewymagających połączenia z siecią wewnętrzną jednostki. [str. 30–31]

Organizacja bezpieczeństwa dokumentów oryginalnych

Oryginalna dokumentacja źródłowa była na ogół prawidłowo chroniona. Dokumenty w formie papierowej i ich kserokopie nie były wynoszone do miejsc wykonywania pracy zdalnej w siedmiu z 10 kontrolowanych jednostek. Wgląd do nich zorganizowano poprzez dostęp do użytkowanych systemów informatycznych. W jednym z trzech pozostałych urzędów pracownicy pobierali dokumentację papierową bez sporządzania i podpisywania stosownych protokołów i oświadczeń. [str. 31]

Ograniczony zakres monitorowania bezpieczeństwa informacji w pracy zdalnej

Monitorowanie pracy zdalnej dotyczyło przede wszystkim rozliczenia pracowników z wykonania powierzonych im zadań. Nie wszystkie zadania określone w regulacjach wewnętrznych związane z monitorowaniem działań mających wpływ na bezpieczeństwo informacji realizowano w pełnym zakresie. [str. 32]

4. WNIOSKI

Pozyskiwanie od jednostek administracji publicznej informacji o skali wykorzystania systemów teleinformatycznych w pracy zdalnej i o stosowaniu wydanych przez ministra zaleceń i rekomendacji.

Minister właściwy do spraw informatyzacji

Dokonanie przez jednostki administracji publicznej przeglądu regulacji wewnętrznych w obszarze bezpieczeństwa informacji i zmodyfikowanie ich tak, aby nie ograniczały się one wyłącznie do ochrony danych osobowych.

Jednostki administracji publicznej

5. WAŻNIEJSZE WYNIKI KONTROLI

5.1. Monitorowanie przetwarzania przez jednostki administracji publicznej danych w pracy na odległość w celu zachowania bezpieczeństwa informacji

W Kancelarii Prezesa Rady Ministrów, jako jednostce nadzorującej wykonywanie zadań publicznych oraz pełniącej funkcję urzędu Ministra ds. Cyfryzacji nie prowadzono zadań koncentrujących się w szczególności na bezpieczeństwie przetwarzania przez jednostki administracji publicznej danych w pracy na odległość. W ograniczonym zakresie monitorowano zapewnienie przez te jednostki bezpieczeństwa informacji w pracy zdalnej i mobilnym przetwarzaniu danych, w tym również sposób wdrożenia przez nie zaleceń i rekomendacji działań dotyczących podniesienia poziomu bezpieczeństwa teleinformatycznego, tj. m.in. narodowych standardów cyberbezpieczeństwa.

5.1.1. Strategia cyberbezpieczeństwa RP na lata 2014–2020

Wzrost znaczenia bezpieczeństwa teleinformatycznego

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. 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 kraju w obszarze cyberbezpieczeństwa (5).

Zadania na rzecz wdrożenia Strategii Cyberbezpieczeństwa

Zgodnie z założeniami Strategii wyznaczono Plan Działań w aspekcie m.in. podniesienia poziomu odporności systemów informacyjnych administracji publicznej. 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 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 oraz utworzenia siedmiu Regional-

nych Centrów Cyberbezpieczeństwa, działających na poziomie regionalnym wg podziału NUTS 1[7] (zakończenie ich realizacji zaplanowano na czwarty kwartał 2024 r.).

5.1.2. Wytyczne i rekomendacje działań w czasie pandemii Covid-19

Narodowe Standardy Cyberbezpieczeństwa

Departament Cyberbezpieczeństwa opracował i udostępnił Narodowe Standardy Cyberbezpieczeństwa, 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";
- Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.

Propozycje i zalecenia dotyczące bezpieczeństwa pracy zdalnej

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,

[7] NUTS 1 – makroregiony (grupujące województwa) – siedem jednostek.

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

[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.

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. Informacje te udostępniono od marca 2020 r. poprzez ich publikację w Internecie[10].

5.1.3. Monitorowanie sposobu wdrożenia zaleceń i rekomendacji działań

Naruszenia bezpieczeństwa danych

Z danych posiadanych przez Departament Cyberbezpieczeństwa KPRM, przekazanych przez CSIRT NASK[11] 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.

Z uzyskanych w toku kontroli wyjaśnień wynikało m.in., że CSIRT-y nie będąc zobligowane do przekazywania do organów właściwych szczegółowych informacji o incydentach, nie przekazywały ich do KPRM. W związku z tym nie posiadano 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.

W ograniczonym zakresie monitorowano zapewnienie przez jednostki administracji publicznej bezpieczeństwa informacji w pracy na odległość

W latach 2020–2021 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. 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. Nie nakładają one również

[10] Cyfryzacja KPRM; Serwis RP – portal gov.pl – https://www.gov.pl/web/cyfryzacja/razem-ale-osobno—to-powinniscie-wiedziec-o-pracy-zdalnej.

[11] 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 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.

na ministra właściwego do spraw informatyzacji, ani na Pełnomocnika Rządu do spraw Cyberbezpieczeństwa obowiązku gromadzenia informacji w przedmiotowym zakresie.
Zdaniem NIK, 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. 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.

Pozytywna ocena działań Ministerstwa Rodziny i Polityki Społecznej w zakresie bezpieczeństwa informacji

W okresie objętym kontrolą KPRM przeprowadziła jedną kontrolę dotyczącą wykorzystania systemów teleinformatycznych do realizacji zadań publicznych.
Objęto nią Ministerstwo Rodziny i Polityki Społecznej. 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 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.

5.2. Organizacja bezpieczeństwa informacji

Regulacje wewnętrzne ustanowione i wdrożone w części kontrolowanych jednostek nie były kompletne i nie zapewniały odpowiedniego poziomu bezpieczeństwa informacji w przypadku nagłego wprowadzenia pracy zdalnej. Wymagały dostosowywania do warunków zewnętrznych i możliwości urzędów poprzez wprowadzanie dodatkowych zarządzeń i regulaminów.

W okresie objętym kontrolą w jednej z kontrolowanych jednostek ustanowiono i wdrożono wymagany przepisami rozporządzenia KRI kompletny system zarządzania bezpieczeństwem informacji.

5.2.1. Systemy Zarządzania Bezpieczeństwem Informacji

Organizacja bezpieczeństwa informacji obejmowała głównie ochronę danych osobowych

W pięciu urzędach spośród 10 objętych kontrolą w tym zakresie (50%) stwierdzono, że opracowane i wdrożone w tych jednostkach regulacje zawierały deklaracje stosowania ich do ochrony danych osobowych i nie obejmowały bezpieczeństwa innych rodzajów informacji. Tym samym nie zapewniono w nich systemowego podejścia do zagadnień bezpieczeństwa informacji, o których mowa w § 20 ust. 1 rozporządzenia KRI.

Zgodnie z tym przepisem podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Ponadto § 20 ust. 3 rozporządzenia KRI wskazuje, że wymagania określone w ww. ust. 1 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-EN ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą. W punkcie 5.1 normy PN-EN ISO/IEC 270028 wskazano wymóg opracowania i stosowania dokumentu polityki bezpieczeństwa informacji.

Regulacje, które zostały opracowane i wdrożone w tych urzędach nie obejmowały wszystkich rodzajów informacji jakie są w nich przetwarzane, lecz dotyczyły głównie danych osobowych.

W czterech jednostkach, w których stwierdzono brak systemowego podejścia do zapewnienia bezpieczeństwa informacji kontrolowani byli przekonani o zgodności regulacji przez nich wprowadzonych z obowiązującymi przepisami oraz wskazywali, że ich regulacje spełniają wymagania wynikające z rozporządzenia KRI i mogą być stosowane w szerszym zakresie.

Przykład

Starosta Powiatu Bartoszyckiego wyjaśnił, że dokumentacja zawarta w Polityce Ochrony Danych Osobowych określa zasady i reguły dotyczące bezpieczeństwa przetwarzania informacji danych osobowych w sposób kompleksowy i jej zasady mogą zostać rozszerzone do ich stosowania w ogólnym pojęciu przetwarzania informacji służbowej i jego zdaniem jest wystarczająca do odpowiedniego zabezpieczenia przetwarzanych informacji przez pracowników wyznaczonych do pracy zdalnej.

W jednej jednostce już na etapie kontroli zadeklarowano dokonanie uzupełnienia w tym zakresie.

Przykład

Burmistrz Olsztynka zadeklarował zamiar aktualizacji obowiązującej dokumentacji w związku ze stwierdzonymi brakami, tj. m.in. opracowanie dokumentu o szerszym zakresie, który będzie spinał ramowo i systemowo uporządkuje wszystkie obowiązujące w Urzędzie procedury i dokumenty.

W takim zakresie jaki obejmowały regulacje wewnętrzne, odpowiedzialność za poszczególne elementy systemów bezpieczeństwa informacji przydzielana była pracownikom stosownie do zakresu czynności i roli pełnionej w urzędzie.

W toku kontroli ustalono, że wszyscy pracownicy, którzy zostali upoważnieni do przetwarzania danych osobowych zobowiązani byli do stosowania zasad obowiązujących w tym zakresie. Nadzór nad podległymi pracownikami w zakresie zapewnienia ochrony informacji przypisano kierownikom komórek organizacyjnych. W jednostkach kontrolowanych określono zadania i obowiązki dla inspektorów ochrony danych (dalej: IOD).

We wszystkich kontrolowanych jednostkach pracownikom pełniącym funkcję administratorów systemów informatycznych przypisano odpowiedzialność w zakresie bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych. Byli oni odpowiedzialni m.in. za przygotowanie stanowisk komputerowych oraz przeprowadzanie szkoleń stanowiskowych dla pracowników urzędów, nadawanie i odbieranie uprawnień użytkownikom, stosowanie w sieciach komputerowych urzędów rozwiązań technicznych podnoszących bezpieczeństwo systemów informatycznych i danych w nich przetwarzanych.

Kontrola wykazała jednak, że w jednej jednostce nie określono osoby odpowiedzialnej za aktualizacje Polityki bezpieczeństwa informacji co skutkowało nieprawidłowościami opisanymi w dalszej części informacji (na str. 25).

W jednym urzędzie nie określono odpowiedzialności za zapewnienie zgodności Polityki bezpieczeństwa informacji z wymaganiami normy ISO określonej w rozporządzeniu KRI.

5.2.2. Ochrona danych osobowych

Prawidłowo zorganizowano zasady ochrony danych osobowych

Odpowiedzialność za bezpieczeństwo danych osobowych we wszystkich kontrolowanych jednostkach przypisano stosownie do zakresu obowiązków i roli przydzielonej w ramach ustanowionych polityk ochrony danych osobowych. W jednostkach tych zgodnie z wymogami rozporządzenia RODO wskazano administratora danych osobowych (dalej: ADO), tj. podmiot odpowiedzialny za ustalanie celów i sposobów przetwarzania tych danych.

Zgodnie z art. 37 ust. 1 lit. a rozporządzenia RODO w związku z art. 8 i 9 ustawy z 10 maja 2018 r. o ochronie danych osobowych, wyznaczono inspektorów ochrony danych. W pięciu jednostkach kontrolowanych funkcje IOD powierzono podmiotom zewnętrznym zawierając stosowne umowy, w których m.in. określono zakresy obowiązków wynikające z art. 39 ust. 1 rozporządzenia RODO. W pozostałych pięciu jednostkach obowiązki te przypisano zatrudnionym pracownikom, przy czym w czterech urzędach były to obowiązki dodatkowe. W jednym przypadku utworzono osobne stanowisko inspektora ochrony danych, w ramach którego zatrudniony na nim pracownik pełnił tę rolę w stosunku do ogółem ośmiu jednostek organizacyjnych starostwa.

W okresie kontrolowanym w trzech urzędach nastąpiły zmiany osób pełniących rolę IOD. W jednej jednostce nowa osoba wyznaczona do pełnienia funkcji IOD nie spełniała wszystkich wymagań określonych w art. 37 ust. 5 RODO jednak zaplanowano dla tej osoby odpowiednie szkolenia w celu uzyskania właściwych kompetencji do realizacji powierzonych zadań.

Przykład

W **Wojewódzkim Inspektoracie Farmaceutycznym w Olsztynie**, ze względu na rozwiązanie umowy o pracę w sierpniu 2021 r. przez osobę wyznaczoną na IOD, zatrudniono nowego pracownika, który nie spełniał wymagań RODO w momencie powierzania obowiązków IOD. Według wyjaśnień Wojewódzkiego Inspektora na lokalnym rynku pracy nie ma specjalistów w zakresie prowadzenia spraw RODO, zainteresowanych wynagrodzeniem, jakie może zaoferować WIF w ramach dostępnych środków finansowych. W związku z tym przeszkolono pracownika, któremu w ramach obowiązków służbowych powierzono prowadzenie spraw związanych z RODO. Został on również zakwalifikowany na szkolenie indywidualne uwzględniające specyfikę jednostki.

W pozostałych dziewięciu kontrolowanych urzędach osoby pełniące funkcję inspektora ochrony danych posiadały kwalifikacje wskazane w art. 37 ust. 5 rozporządzenia RODO.

5.2.3. Regulacje określające zasady postępowania z nośnikami

Zasady postępowania z nośnikami

Wszystkie kontrolowane jednostki określiły reguły dotyczące postępowania z nośnikami danych. Jednak należy zaznaczyć, że w pięciu jednostkach, w których nie opracowano i nie wdrożono SZBI w oparciu o pełną inwentaryzację i klasyfikację rodzajów przetwarzanych informacji reguły te odnoszono jedynie do informacji zawierających dane osobowe. We wszystkich przypadkach dla ochrony informacji znajdujących się na nośnikach wprowadzono obowiązek stosowania rozwiązań kryptograficznych zapewniających szyfrowanie dysków. Określono możliwość przechowywania danych jedynie przez czas niezbędny do spełnienia celu w jakim są przetwarzane, tj. nałożono obowiązek usuwania danych po ich wykorzystaniu. Pracownicy byli zobowiązani do zabezpieczenia nośników informacji przed utratą oraz nieuprawnionym dostępem. Przyjęte w urzędach regulacje zawierały zakazy wynoszenia nośników poza siedzibę urzędu bez zgody lub upoważnienia administratora danych. Przyjęte zasady zakładały prowadzenie rejestru nośników i przypisanie ich użytkownikom odpowiedzialności za bezpieczeństwo informacji w nich przechowywanych.

5.2.4. Zasady zapewnienia bezpieczeństwa dla aktywów wynoszonych poza siedzibę urzędu

Zasady wynoszenia aktywów określiło w politykach ochrony informacji 70% urzędów

Zasady wynoszenia aktywów określono we wszystkich kontrolowanych jednostkach. W podstawowych politykach dotyczących bezpieczeństwa informacji (w części jednostek danych osobowych) przyjęto ogólny zakaz wynoszenia dokumentacji papierowej. Siedem jednostek posiadało procedury bezpiecznej eksploatacji komputerów przenośnych, a pozostałe trzy kontrolowane urzędy dookreśliły reguły dotyczące użytkowania poza siedzibą komputerów przenośnych w wydanych zarządzeniach i ustano-

wionych regulaminach pracy zdalnej. W zarządzeniach wprowadzających pracę zdalną oraz regulaminach jej wykonywania dopuszczono możliwość wynoszenia aktywów, tj. sprzętu komputerowego oraz dokumentów lub ich kopii, poza siedzibę jednostki pod warunkiem uzyskania upoważnienia lub zgody ADO. Wymagano przy tym potwierdzenia protokołem przyjęcia powierzonego sprzętu oraz zobowiązania się do stosowania przyjętych reguł mających na celu zapewnienie bezpieczeństwa informacji wynoszonych poza obszar ich dotychczasowego przetwarzania. Warunkiem umożliwiającym wynoszenie sprzętu komputerowego było stosowanie w nim elementów zabezpieczających w postaci szyfrowania dysków, zainstalowania aktualizacji systemowych oraz programu antywirusowego oraz stosowania indywidualnych kont użytkowników zabezpieczonych hasłem spełniającym wymagania zgodne z przyjętą polityką.

5.2.5. Zasady przesyłania informacji

Przesyłanie informacji wymagało stosowania haseł i mechanizmów kryptograficznych

Podstawowymi kanałami przesyłania informacji niezbędnych do wykonywania zadań w trybie pracy zdalnej było stosowanie poczty elektronicznej oraz szyfrowanych połączeń VPN umożliwiających dostęp do usług pulpitu zdalnego udostępnianych z komputerów stacjonarnych użytkowanych przez pracowników pracujących na odległość.

W zakresie korzystania z poczty elektronicznej wszystkie jednostki zapewniły pracownikom służbowe konta pocztowe. W zasadach dotyczących korzystania z Internetu i poczty elektronicznej zawarte były wymagania dotyczące używania ich wyłącznie w celach służbowych. Przesyłanie załączników zawierających informacje chronione (dane osobowe) wymagało szyfrowania i zabezpieczenia ich hasłem, które należało przekazać adresatowi innym kanałem łączności (np. za pośrednictwem telefonu, SMS). W trzech urzędach dopuszczono możliwość wykorzystywania w celach służbowych także prywatnych kont mailowych, a w dwóch z nich określono warunki jakie należało spełnić aby z tej możliwości można było korzystać. Jednym z nich był warunek uzyskania pisemnej zgody administratora danych lub administratora systemów informatycznych.

W jednym urzędzie w obowiązujących w latach 2020–2021 uregulowaniach dotyczących bezpieczeństwa informacji nie określono warunków korzystania z prywatnych kont pocztowych pomimo dopuszczenia takiej możliwości w pracy zdalnej.

Przykład

W uregulowaniach dotyczących bezpieczeństwa informacji obowiązujących w **Urzędzie Ochrony Zabytków w Olsztynie** w latach 2020–2021 nie uwzględniono zasad korzystania z prywatnych kont pocztowych do celów służbowych, mimo że dopuszczono taką możliwość podczas pracy zdalnej, a reguły takie zostały określone jako „zabezpieczenia do obszaru" w sporządzonej w kwietniu 2020 r. analizie ryzyka pracy zdalnej. Wyniki analizy ryzyka stanowiły rekomendowane dla Urzędu rozwiązania organizacyjne i informatyczne mające na celu wyeliminowanie lub ograniczenie zidentyfikowanych ryzyk m.in. w zakresie korzystania z prywatnych skrzynek e-mail do zadań służbowych.

Ustanowione zasady dostępu do informacji przetwarzanych w miejscu wykonywania pracy zdalnej za pomocą szyfrowanych kanałów VPN w pięciu urzędach dopuszczały stosowanie jedynie sprzętu służbowego powierzonego przez pracodawcę. W pięciu pozostałych urzędach dopuszczono możliwość korzystania z dostępu w tym trybie zarówno z komputerów służbowych jak i prywatnych (nie będących własnością pracodawcy). Przyjęte w tym zakresie uregulowania zawierały wymagania, które musiały być spełnione przed dopuszczeniem komputerów prywatnych do nawiązywania połączeń VPN z zasobami informatycznymi urzędów. Najważniejsze dotyczyły obowiązku aktualizacji systemu operacyjnego, zainstalowania programu antywirusowego, stosowania indywidualnego konta i hasła zgodnego z przyjętą w urzędach polityką haseł.

5.2.6. Zasady zarządzania incydentami związanymi z bezpieczeństwem informacji

Połowa urzędów ograniczyła zarządzanie incydentami bezpieczeństwa do danych osobowych

Wszystkie kontrolowane jednostki posiadały ustanowione regulacje dotyczące zarządzania incydentami związanymi z bezpieczeństwem informacji, jednak w połowie kontrolowanych jednostek obejmowały one jedynie przypadki i zdarzenia związane z naruszeniem ochrony danych osobowych, co było skutkiem braku SZBI ustanowionych w pełnym zakresie wymaganym przez rozporządzenie KRI i normę ISO-27001. We wszystkich jednostkach zdefiniowano katalog zdarzeń mających wpływ na bezpieczeństwo informacji, określono procedury zgłaszania incydentów oraz wyznaczono osoby odpowiedzialne za poszczególne działania w obrębie obsługi zgłaszanych problemów. Za przyjmowanie zgłoszeń, analizę i podejmowanie środków zaradczych lub minimalizujących skutki incydentów odpowiedzialność przydzielano inspektorom ochrony danych oraz administratorom systemów informatycznych. Pracownicy kontrolowanych urzędów zobowiązani byli do zgłaszania wyznaczonym osobom zdarzeń mających wpływ na bezpieczeństwo informacji lub skutkujących naruszeniem tego bezpieczeństwa.

Zasady obsługi incydentów zawierały czynności wynikające z obowiązków nałożonych rozporządzeniem RODO oraz ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

W okresie kontrolowanym w jednym urzędzie wystąpiły dwa incydenty, które zostały ujęte w prowadzonym rejestrze naruszeń bezpieczeństwa danych osobowych, a w dwóch urzędach trzy zdarzenia ujęte w ewidencji incydentów związanych z bezpieczeństwem informacji. Żaden z powyższych przypadków nie był związany z wykonywaniem pracy zdalnej gdyż miały miejsce podczas pracy wykonywanej w siedzibach urzędów.

5.2.7. Regulaminy pracy zdalnej

Regulaminy pracy zdalnej określały przede wszystkim reguły organizacyjne

Pomimo obowiązku ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, wynikającego z § 20 ust. 2 pkt 8 rozporządzenia KRI, tylko w dwóch urzędach zasady pracy zdalnej (świadczonej poza miejscem jej stałego wykonywania) uregulowane były w przyjętych Politykach bezpieczeństwa danych osobowych. W pozostałych ośmiu kontrolowanych urzędach zasady pracy zdalnej

doprecyzowane zostały w ustanowionych regulaminach i zarządzeniach. W trzech jednostkach nastąpiło to w marcu i kwietniu 2020 r. bezpośrednio przed wprowadzeniem przez te urzędy systemu pracy zdalnej. Kolejne trzy urzędy dodatkowe regulacje dotyczące pracy zdalnej wprowadziły w październiku 2020 r. tj. przed jesienno-zimową falą zakażeń.

Jedna jednostka wprowadziła zasady pracy zdalnej w marcu, a jedna we wrześniu 2021 r.

Wprowadzanie i organizowanie pracy zdalnej w kontrolowanych jednostkach było procesem rozłożonym w czasie. Wyposażanie pracowników w sprzęt i narzędzia do pracy zdalnej oraz uruchamianie usług teleinformatycznych umożliwiających realizację zadań na odległość realizowano stopniowo, w miarę posiadanych możliwości.

W początkowym okresie pandemii jednostki kontrolowane wprowadzając zarządzenia dotyczące pracy zdalnej koncentrowały się przede wszystkim na zapewnieniu dystansu społecznego i ograniczeniu kontaktów pomiędzy pracownikami w celu ograniczenia rozprzestrzeniania się COVID-19. Nie będąc przygotowanymi do szybkiego uruchomienia pracy zdalnej zapewniającej pełną realizację zadań wprowadzały tzw. pracę rotacyjną, nazywaną w niektórych jednostkach naprzemienną polegającą na podziale pracowników na grupy, które według sporządzonych grafików naprzemiennie pracowali w trybie normalnym i zdalnym.

Przykłady

Na polecenie Burmistrza Olsztynka, w celu ograniczenia rozprzestrzeniania się pandemii COVID-19, wprowadzono w **Urzędzie Miejskim** pracę naprzemienną, tzn. pracownicy zgodnie z przyjętym grafikiem jeden dzień pracowali w trybie normalnym i kolejny w trybie zdalnym. Praca zdalna w tym trybie odbywała się bez wykorzystywania sprzętu teleinformatycznego, zarówno prywatnego, jak i będącego własnością Urzędu. Pracownicy świadczący pracę zdalną na podstawie polecenia wydanego na indywidualny wniosek pracownika (tj. w okresie dłużnym niż jeden dzień) mieli zagwarantowane do pracy służbowe komputery.

W **Urzędzie Miejskim w Morągu** od 14 marca 2020 r. pracę zorganizowano tak, aby zachować jej ciągłość. W związku z tym, w 2020 r. dwukrotnie wprowadzono okresowo naprzemienny system pracy pracowników. Praca rotacyjna wprowadzona od 30 marca 2020 r. była pracą naprzemienną bez wykorzystania systemów informatycznych, a sposób organizacji pracy Urzędu w tym okresie był pracownikom zakomunikowany ustnie na spotkaniu z kierownictwem Urzędu z 16 marca 2020 r. Natomiast praca rotacyjna wprowadzona w Urzędzie 20 października 2020 r. miała charakter naprzemiennej pracy zdalnej z wykorzystaniem systemów informatycznych, a jej regulamin został wdrożony zarządzeniem w sprawie pracy zdalnej.

Zasady zabezpieczania komputerów używanych w pracy na odległość

W ustanowionych regulaminach pracy zdalnej dookreślano zasady nieujęte wcześniej w obowiązujących politykach bezpieczeństwa informacji (ochrony danych osobowych), tj. m.in. wymagania dotyczące zabezpieczania komputerów oraz dokumentów wykorzystywanych w miejscu wykonywania pracy na odległość, określano wzory stosowanych poleceń pracy zdalnej, zasady zgłaszania rozpoczęcia i zakończenia pracy oraz raportowania o wykonaniu wydanych poleceń i wykonaniu przydzielonych zadań.

5.2.8. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji

Szkolenia w obszarze bezpieczeństwa informacji dotyczyły głównie ochrony danych osobowych

Jednostki kontrolowane korzystały z różnych rozwiązań i form umożliwiających szkolenia i zapoznawanie pracowników z zagrożeniami dla bezpieczeństwa informacji przetwarzanych w pracy zdalnej. Stosowano platformy do szkoleń *on-line*, przesyłano prezentacje zawierające materiały szkoleniowe oraz ostrzeżenia przed kampaniami nakłaniającymi do nieświadomego zainstalowania niepożądanych programów wyłudzających informacje.

W latach objętych kontrolą spośród 10 kontrolowanych jednostek w siedmiu z nich organizowano szkolenia obejmujące swym zakresem bezpieczeństwo danych osobowych, z tego w trzech takie szkolenia odbywały się corocznie. W pięciu urzędach część pracowników została zapoznana z zagrożeniami dla bezpieczeństwa informacji przetwarzanych za pomocą systemów teleinformatycznych oraz z ogólnymi zagadnieniami cyberbezpieczeństwa. Dwie jednostki po wprowadzeniu rozwiązań umożliwiających dostęp zdalny do zasobów informatycznych przeprowadziły szkolenia z obsługi oprogramowania wykorzystywanego do pracy zdalnej oraz zasad bezpiecznego jej wykonywania.

W jednym urzędzie, który w roku 2021 ustanowił i wdrożył, zgodnie z rozporządzeniem KRI, system zarządzania bezpieczeństwem informacji, zapewniono szkolenie dla czterech pracowników odpowiedzialnych za prawidłowe funkcjonowanie SZBI.

Pięć urzędów posiadało udokumentowane potwierdzenia zapoznania się przez pracowników z obowiązującymi zasadami dotyczącymi bezpieczeństwa informacji.

W dwóch urzędach w objętym kontrolą okresie nie organizowano szkoleń, a jedyną formą przekazywania wiedzy w zakresie bezpieczeństwa informacji było udzielanie przez administratora systemów informatycznych instruktarzu w trakcie przekazywania sprzętu przeznaczonego do pracy zdalnej oraz przesyłanie przez IOD materiałów informacyjnych zawierających zasady bezpiecznego przetwarzania informacji w pracy zdalnej.

W jednym urzędzie, pomimo zawarcia w POD oraz PBI uregulowań wymagających przeprowadzania szkoleń w przypadku każdej istotnej zmiany zasad bezpieczeństwa informacji oraz obowiązku szkolenia nie rzadziej niż raz w roku osób zaangażowanych w proces przetwarzania informacji, w objętym kontrolą okresie nie realizowano tego obowiązku. Należy również podkreślić, że zgodnie z PBI oraz POD wiedza nowo zatrudnionych pracowników powinna być weryfikowana poprzez test na platformie e-learningowej, lecz urząd nie posiadał ani nie dysponował dostępem do takiej platformy. Obowiązek zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji wynika również z przepisów § 20 ust. 2 pkt 6 rozporządzenia KRI.

5.2.9. Przeglądy i aktualizacje systemów zarządzania bezpieczeństwem informacji

Uregulowania dotyczące bezpieczeństwa informacji nie były poddawane regularnym przeglądom

W okresie objętym kontrolą jedynie w trzech spośród 10 urzędów przeprowadzano audyt zewnętrzny systemów teleinformatycznych w zakresie zapewnienia bezpieczeństwa informacji.

W trzech urzędach oceny regulacji wprowadzonych w obszarze bezpieczeństwa informacji dokonywano w ramach audytu wewnętrznego.

W siedmiu jednostkach kontrolowanych przeprowadzano analizy ryzyka w dziedzinie bezpieczeństwa informacji, w tym w pięciu dokonano tego w ramach przygotowań do wprowadzenia w urzędach pracy zdalnej.

Dwa spośród kontrolowanych urzędów nie posiadały dokumentacji potwierdzającej dokonywanie przeglądów obowiązujących w nich polityk bezpieczeństwa informacji (danych osobowych). Należy przy tym podkreślić, że kontrolowani z jednej strony byli przekonani o zgodności funkcjonujących w ich urzędach regulacji z rozporządzeniem KRI twierdząc jednocześnie, że nie mają obowiązku wykonywania przeglądów i aktualizacji polityki bezpieczeństwa informacji. Polska Norma ISO/IEE27001, która jest wyznacznikiem do stwierdzenia zgodności ustanowionych regulacji z wymaganiami rozporządzenia KRI wymaga aby kierownictwo przeprowadzało przegląd systemu zarządzania bezpieczeństwem informacji w zaplanowanych odstępach czasu, w celu zapewnienia jego stałej przydatności, adekwatności i skuteczności. Jednocześnie wymaga aby organizacja zachowała udokumentowane informacje jako dowód wyników przeglądów zarządzania.

Przykłady

Według **Starosty Powiatu Bartoszyckiego** dokumentacja zawarta w PODO określa zasady i reguły dotyczące bezpieczeństwa przetwarzania informacji danych osobowych w sposób kompleksowy i jej zasady mogą zostać rozszerzone do ich stosowania w ogólnym pojęciu przetwarzania informacji służbowej i jego zdaniem jest wystarczająca do odpowiedniego zabezpieczenia przetwarzanych informacji przez pracowników wyznaczonych do pracy zdalnej.

Starosta wyjaśnił, że aktualnie nie ma obowiązku wykonania przeglądu i aktualizacji wdrożonej polityki bezpieczeństwa informacji PODO, ale zaplanowano już na grudzień 2021 r. audyt bezpieczeństwa Urzędu, którego elementem jest przegląd i aktualizacja polityki PODO.

Burmistrz Morąga wyjaśnił, że obowiązujące w Urzędzie regulacje wewnętrzne były aktualne, a ich aktualizacja w zakresie zmieniającego się otoczenia przeprowadzana będzie wg potrzeb. Dodatkowo procedury zawarte w regulacjach były na bieżąco analizowane i monitorowane przez osoby odpowiedzialne za dany zakres regulacji. Sekretarz Gminy dodał, że były to analizy bieżące, jednak działania te nie zostały w żaden sposób utrwalone.

5.3. Wdrożone i stosowane rozwiązania organizacyjne i techniczne mające na celu zapewnienie bezpieczeństwa informacji w pracy zdalnej

Kontrole wdrożonych i stosowanych rozwiązań organizacyjnych i technicznych mających na celu zapewnienie bezpieczeństwa informacji w pracy zdalnej przeprowadzono w jednostkach, w których co najmniej 50% pracowników wykonywało pracę w formie zdalnej. Dodatkowym kryterium wyboru było stosowanie rozwiązań organizacyjnych i technicznych umożliwiających wykorzystywanie w tej pracy zarówno służbowego jak i prywatnego sprzętu teleinformatycznego.

5.3.1. Skala i zakres wprowadzonej pracy zdalnej

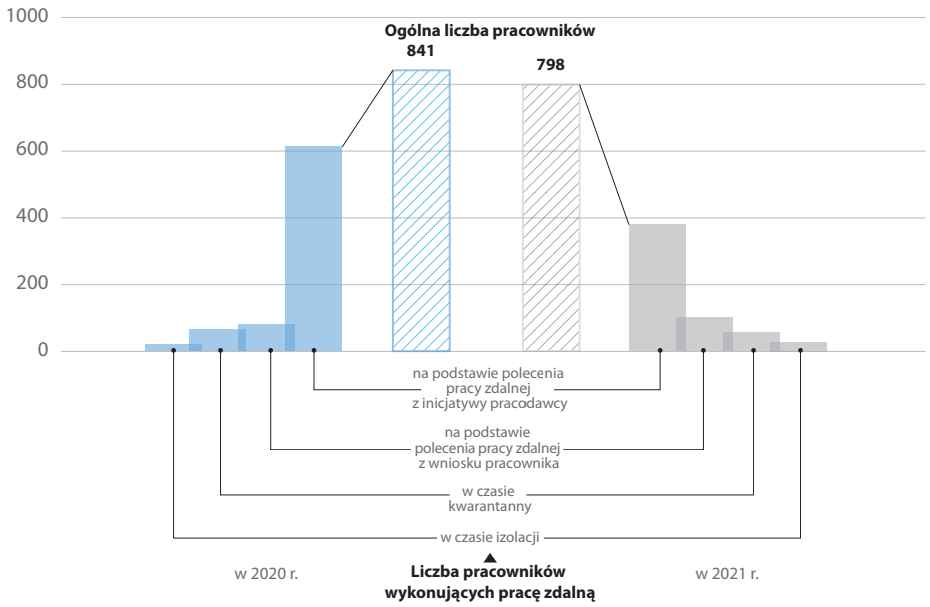
Liczba pracowników skierowanych do pracy zdalnej w 2021 r. była mniejsza niż w 2020 r.

W latach 2020–2021 (do 30 listopada) praca zdalna w kontrolowanych jednostkach wykonywana była na podstawie poleceń wydawanych z inicjatywy pracodawcy lub na wniosek pracownika. Wykonywana była także przez niektórych pracowników objętych kwarantanną lub izolacją.

W 2020 roku w 10 kontrolowanych jednostkach zatrudnionych było 841 pracowników (wg stanu na 31 grudnia 2020 r). Polecenia pracy zdalnej z inicjatywy pracodawcy wydano dla 612 pracowników (tj. 72,8% zatrudnionych), a dla 80 (9,5%) na podstawie wniosku pracownika. Pracę zdalną w okresie kwarantanny wykonywało 64, a w czasie izolacji 19 pracowników.

W 2021 roku na 798 zatrudnionych polecenia pracy zdalnej z inicjatywy pracodawcy wydano dla 379 pracowników (tj. 47,5% zatrudnionych), a dla 100 (12,5%) na podstawie wniosku pracownika. Pracę zdalną w okresie kwarantanny wykonywało 56, a w czasie izolacji 27 pracowników.

Infografika nr 3
Liczba pracowników jednostekkontrolowanych wykonujących pracę zdalną



Źródło: opracowanie własne.

W początkowym okresie wprowadzenia pracy zdalnej w jednostkach kontrolowanych stosowano tryb określany przez kontrolowanych jako system rotacyjny. Polegał on na podziale pracowników na grupy, które zgodnie z przyjętym harmonogramem aby ograniczyć ryzyko zakażenia wykonywały pracę naprzemiennie tj. jeden dzień w formie tradycyjnej (stacjonarnej) i jeden dzień w formie zdalnej. W tym trybie praca zdalna odbywała się bez dostępu do systemów teleinformatycznych.

Jednostki kontrolowane nie były przygotowane na natychmiastowe wprowadzenie pracy zdalnej zapewniającej warunki do realizacji zadań w takim samym lub zbliżonym zakresie jak trybie stacjonarnym. Sytuacja ta wymagała podjęcia dodatkowych działań polegających na przygotowaniu rozwiązań technicznych i organizacyjnych umożliwiających pracownikom zdalny dostęp do informacji przetwarzanych za pośrednictwem użytkowanych systemów teleinformatycznych.

Przykład

Wójt Gminy Jedwabno wyjaśnił, że w marcu 2020 r. wydał wszystkim pracownikom ustne polecenie wykonywania pracy zdalnej w systemie rotacyjnym, tj. w taki sposób, aby w pomieszczeniu biurowym nie pracował więcej niż jeden pracownik. Zapewnienie obsługi informatycznej, w tym zapewnienie bezpieczeństwa przetwarzania informacji polecono informatykowi. Pracownicy wykonywali pracę zdalną w oparciu o zadania wynikające z zakresów czynności, z wykorzystaniem własnego sprzętu komputerowego. Do dnia wprowadzenia do użytku pulpitu zdalnego (tj. do kwietnia 2020 r.) zadania zlecane pracownikom wykonującym pracę zdalną nie wymagały dostępu do sieci Urzędu i oprogramowania. Polegały one głównie na uczestniczeniu pracowników w konferencjach i szkoleniach oraz na opracowywaniu ogólnych dokumentów.

Jednostki kontrolowane, w zależności od potrzeb i możliwości udostępniały pracownikom komputerowy sprzęt przenośny lub określały warunki i zasady korzystania w pracy zdalnej z komputerów nie będących własnością pracodawcy.

5.3.2. Przygotowanie pracowników do zapewnienia bezpieczeństwa informacji w pracy zdalnej

Większość urzędów zapoznawała pracowników z zasadami bezpieczeństwa informacji.

Ustanowione regulacje obejmujące zagadnienia bezpieczeństwa informacji oraz wydawane polecenia pracy zdalnej zawierały postanowienia zobowiązujące pracowników do przestrzegania zasad określonych w wewnętrznych regulacjach dotyczących bezpieczeństwa informacji oraz wymagały potwierdzenia zapoznania się z tymi zasadami.

W jednej jednostce nie egzekwowano tego obowiązku i w dokumentacji urzędu brakowało złożonych oświadczeń.

Przykład

W **Urzędzie Gminy w Gietrzwałdzie**, wbrew określonemu w PBI obowiązkowi przyjęcia od pracowników pisemnych „Oświadczeń o znajomości Polityki Bezpieczeństwa Informacji i zachowaniu w poufności informacji", 32 pracowników Urzędu potwierdziło pisemnie zapoznanie się z ww. dokumentem dopiero w trakcie kontroli NIK. Nastąpiło to w dniach od 27 października do 2 listopada 2021 r., pomimo że ww. dokument obowiązywał od 27 lutego 2017 r.

Oprócz tego, pomimo określonego w POD wymogu pisemnego potwierdzenia zapoznania się z tym dokumentem, potwierdzenie takie w „Wykazie osób zapoznanych z Polityką Ochrony Danych" sporządzonym według wzoru stanowiącego załącznik nr 1 do ww. polityki złożyło jedynie 20 z 45 pracowników Urzędu (44,4%) przetwarzających dane osobowe w latach 2020–2021.

W ramach realizacji obowiązków inspektorzy ochrony danych przekazywali drogą mailową informacje zawierające zalecenia i zasady zwiększające świadomość pracowników w zakresie zagrożeń dla bezpieczeństwa informacji.

W większości kontrolowanych urzędów informacje o zasadach zwiększających bezpieczeństwo informacji w pracy zdalnej udostępniane były drogą elektroniczną, a pracownicy zapoznawali się z nimi w formie samokształcenia.

Dwie kontrolowane jednostki, przed udostępnieniem usługi „pulpitu zdalnego" pracownikom wykonującym pracę na odległość, zorganizowały szkolenia w zakresie bezpiecznego łączenia się z siecią wewnętrzną urzędu.

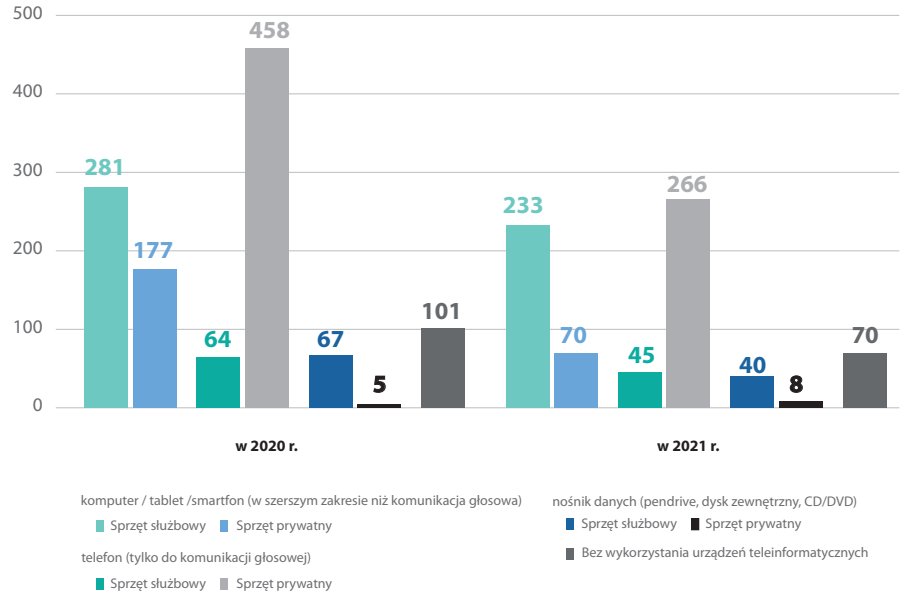
5.3.3. Zakres wykorzystania urządzeń teleinformatycznych

Sprzęt prywatny był istotnym wsparciem w realizacji zadań

W 2020 r. w służbowy sprzęt komputerowy wyposażono 281, a w 2021 r. 233 pracowników wykonujących pracę zdalną. Ze służbowych telefonów używanych jedynie do komunikacji głosowej korzystało w 2020 r. 64, a w 2021 r. 45 pracowników.

Z komputerów prywatnych w 2020 r. korzystało 177 pracowników, a 70 w roku 2021. Telefony prywatne (tylko do komunikacji głosowej) wykorzystywane były w 2020 r. przez 458 pracowników a w 2021 r. przez 266 wykonujących pracę zdalną.

Infografika nr 4
Liczba pracowników wykonujących pracę zdalną z wykorzystaniem określonego sprzętu teleinformatycznego



Źródło: opracowanie własne.

Podstawowym sposobem wykorzystania komputerów (zarówno służbowych jak i prywatnych) do realizacji zadań wykonywanych w trybie pracy zdalnej było korzystanie z usług „pulpitu zdalnego" udostępnianego za pośrednictwem szyfrowanych połączeń VPN. Stosowanie takiego rozwiązania zapewniało pracownikom wykonującym pracę na odległość dostęp do systemów informatycznych urzędu w takim samym zakresie jak w przypadku pracy w systemie tradycyjnym.

5.3.4. Zastosowane środki służące ochronie przetwarzanych informacji

W niepełnym zakresie stosowano własne regulacje wewnętrzne.

We wszystkich jednostkach kontrolowanych, w celu zapewnienia bezpieczeństwa informacji w pracy na odległość, stosowano szyfrowane połączenia VPN umożliwiające korzystanie z usług pulpitu zdalnego, instalowano aktualizacje systemów operacyjnych, używano programów antywirusowych. Wdrożono mechanizmy sporządzania kopii bezpieczeństwa danych. Konta użytkowników nie posiadały uprawnień administratora zezwalających na instalowanie oprogramowania. Oględziny komputerów, które były przeznaczone do pracy zdalnej wykazały jednak, że nie wszystkie ustalone środki i zasady służące ochronie przetwarzanych informacji były stosowane przez kontrolowane urzędy.

W trzech jednostkach nie szyfrowano dysków twardych komputerów przenośnych użytkowanych poza siedzibą urzędu.

Przykłady

W **Urzędzie Miejskim w Olsztynku** nie zabezpieczono laptopów do pracy zdalnej przed ujawnieniem zawartych w nich informacji w przypadku utraty sprzętu, tj., nie szyfrowano dysków tych komputerów, pomimo zaleceń sformułowanych w wyniku przeprowadzonego audytu bezpieczeństwa informacji.

Burmistrz wyjaśnił, że komputery przenośne (laptopy) wykorzystywane do pracy zdalnej służyły wyłącznie jako terminale do połączenia z zasobami sieciowymi Urzędu i na urządzeniach tych nie dochodziło do bezpośredniego przetwarzania danych w postaci plików zapisywanych na dyskach twardych.

W okresie objętym kontrolą w **Starostwie Powiatowym w Bartoszycach** nie szyfrowano dysków twardych komputerów przenośnych używanych w pracy zdalnej.

Starosta wyjaśnił, że dane nie były przetwarzane na dyskach lokalnych komputerów przeznaczonych do pracy zdalnej i nie było potrzeby szyfrowania nośników pamięci.

W jednym spośród kontrolowanych urzędów nie skonfigurowano na komputerach do pracy zdalnej indywidualnych kont użytkowników.

Przykład

Niezgodnie z obowiązującymi w **Urzędzie Miejskim w Olsztynku** politykami nie skonfigurowano na komputerach do pracy zdalnej indywidulanych kont użytkowników uprawniających do korzystania z operacyjnego systemu informatycznego.

Burmistrz wyjaśnił, że po przeanalizowaniu zagrożeń i sposobów przetwarzania danych uznano, że stosowanie hasła dostępu na BIOS oraz do systemu Windows, a także indywidualnych kont do systemów dziedzinowych i poczty

e-mail oraz zasobów serwera plikowego jest wystarczające. Dodał także, że z komputerów przenośnych (laptopów) wykorzystywanych do pracy zdalnej w tym samym czasie korzystał wyłącznie jeden pracownik. Każdorazowo, przed wydaniem urządzenia pracownik obsługi informatycznej przygotowywał komputer do pracy. Przygotowanie polegało na przywróceniu systemu do ustawień sprzed pierwszego wydania.

W jednym urzędzie natomiast nie stosowano ustawień systemowych wymuszających stosowanie haseł spełniających reguły ustalone w przyjętej instrukcji zarządzania systemem informatycznym.

Przykład

Na serwerze obsługującym **Urząd Gminy w Gietrzwałdzie** nie skonfigurowano ustawień wymuszających od użytkowników systemu stosowania haseł zawierających, wymagane Instrukcją zarządzania systemem informatycznym, małe i wielkie litery, cyfry oraz znaki specjalne, pomimo tego, że dokonanie takiej konfiguracji serwera było możliwe. Brak takiej konfiguracji nie dawał rękojmi rzetelnego wywiązywania się użytkowników systemu z przyjętych ww. Instrukcją standardów w zakresie polityki haseł, której celem było zapewnienie dostępu do systemów informatycznych jedynie osób upoważnionych.

Według wyjaśnień Informatyka przyczyną zaistniałej sytuacji było przeoczenie, spowodowane natłokiem wykonywanych obowiązków.

5.3.5. Wykorzystanie w pracy zdalnej sprzętu nie będącego własnością pracodawcy

W połowie jednostek komputery prywatne miały dostęp do sieci wewnętrznej

Podstawową przyczyną dopuszczenia do wykorzystywania w pracy zdalnej komputerów nie będących własnością pracodawcy był brak możliwości zapewnienia wystarczającej ilości sprzętu przez kontrolowane urzędy przy jednoczesnej konieczności zapewnienia ciągłości działania. Stosowano w tym zakresie dwa podstawowe podejścia tj. z możliwością uzyskania dostępu do sieci wewnętrznej urzędu oraz bez takiej możliwości.

W pięciu spośród 10 kontrolowanych urzędów przy wykorzystaniu komputerów nie będących własnością pracodawcy zastosowano rozwiązania umożliwiające nawiązanie połączenia VPN oraz korzystanie z usług pulpitu zdalnego. Określono podstawowe wymagania, które były weryfikowane przez pracowników pełniących role administratorów systemów informatycznych w tych urzędach. Wymagano m.in. zainstalowania najnowszych aktualizacji systemu operacyjnego, programu antywirusowego, ustawienia hasła logowania do komputera.

Przykład

W **Starostwie Powiatowym w Bartoszycach** zgody na wykorzystanie sprzętu prywatnego zawierały m.in. zalecenie aby nie przetwarzać informacji służbowych na lokalnym komputerze, a jedynie na komputerze, do którego dostęp uzyskiwano za pośrednictwem pulpitu zdalnego.

W czterech urzędach stwierdzono wykorzystywanie sprzętu prywatnego pracowników do realizacji niektórych zadań wykonywanych w ramach pracy zdalnej bez dostępu do sieci wewnętrznej Urzędu. Były do zadania szkoleniowe i edukacyjne, korzystanie z informacji dostępnych

w Internecie, komunikacja z wykorzystaniem poczty elektronicznej m.in. do raportowania pracy zdalnej, ale także w jednej jednostce przygotowywanie projektów dokumentów.

Przykłady

W **Izbie Administracji Skarbowej w Olsztynie** pracownicy używający komputerów prywatnych wykorzystywali je do analizy stron internetowych oraz pozyskiwania informacji z ogólnodostępnych baz aktów prawnych.

W **Urzędzie Miejskim w Olsztynku** komputerów prywatnych nie dopuszczono do łączenia się z siecią wewnętrzną urzędu. Pracownicy wykorzystywali je do komunikacji z przełożonymi za pośrednictwem służbowej poczty elektronicznej.

5.3.6. Wykorzystywanie oryginałów, kopii lub skanów dokumentów

Oryginały, kopie lub skany dokumentów nie były wynoszone z 70% kontrolowanych urzędów

W siedmiu spośród 10 kontrolowanych urzędów nie wynoszono do miejsc wykonywania pracy zdalnej dokumentów papierowych ani ich kserokopii. Dostęp do nich realizowany był za pośrednictwem usługi pulpitu zdalnego oraz systemów obiegu dokumentów elektronicznych, a także folderów udostępnianych przez serwery plików oraz przez pocztę elektroniczną.

W pozostałych trzech urzędach przy wykonywaniu pracy zdalnej wykorzystywano dokumenty papierowe lub ich kserokopie pobierane z jednostki.

W dwóch urzędach przy udostępnianiu dokumentów papierowych stosowano przyjęte zasady i sporządzano odpowiednie protokoły potwierdzające pobranie oraz zwrot pobranych akt.

Przykłady

W izbie **Administracji Skarbowej w Olsztynie** przy pobieraniu dokumentacji papierowej sporządzano protokół pobrania akt, który zawierał m.in. uzasadnienie pobrania dokumentacji, miejsce przetwarzania i sposób zabezpieczenia danych, oświadczenie o zapoznaniu się z zasadami w zakresie ochrony informacji oraz potwierdzenie pobrania i zwrotu akt.

W **Starostwie Powiatowym w Bartoszycach** dokumentacja przekazywana była pracownikom na podstawie protokołu zdawczo-odbiorczego, którego wzór określono w Załączniku nr 14 do Polityki Ochrony Danych Osobowych, z adnotacją „dokumenty zabezpieczone w zasznurowanych teczkach i segregatorach przekazano pracownikom do wykonywania niezbędnych zadań".

W jednej z kontrolowanych jednostek pracownicy pobierali dokumentację papierową bez sporządzania i podpisywania stosownych protokołów i oświadczeń.

Przykład

W **Wojewódzkim Urzędzie Ochrony Zabytków w Olsztynie** pracownicy wykonujący pracę zdalną pobierali projektową dokumentację budowlaną lub programy badań i prac konserwatorskich przy zabytku tj. załączniki do wniosków składanych do urzędu. Nie podpisywali przy tym oświadczeń o pobraniu dokumentów, jednak jak wyjaśniła kierownik Wydziału Inspekcji Zabytków Nieruchomych i Ruchomych informacje o dokumentach pobieranych do analizy zawarte były w składanych przez tych pracowników sprawozdaniach tygodniowych.

5.3.7. Monitorowanie i nadzorowanie pracy zdalnej

Bezpieczeństwo informacji monitorowano w ograniczonym zakresie

Monitorowanie pracy zdalnej dotyczyło przede wszystkim rozliczenia pracowników z wykonania powierzonych im zadań. Stosowano w tym zakresie bieżący nadzór bezpośrednich przełożonych oraz wprowadzono zasady okresowego raportowania.

Zagadnienia dotyczące bezpieczeństwa informacji realizowane były w zakresie zabezpieczenia dostępu do sieci wewnętrznej urzędu i monitorowania połączeń. W jednej jednostce, pomimo wprowadzenia takiego obowiązku, nie monitorowano ruchu sieciowego pod kątem wystąpienia niepożądanych połączeń.

Przykład

W **Starostwie Powiatowym w Bartoszycach** obsługa informatyczna nie realizowała monitorowania ruchu sieciowego pod kątem wystąpienia niepożądanych połączeń.

Starosta wyjaśnił, że nie posiada narzędzi umożliwiających monitorowanie pod katem niepożądanego ruchu sieciowego, a komputery pracy zdalnej łączyły się z urzędem za pomocą usługi VPN, która umożliwiała jako jedyny ruch sieciowy protokół dostępu do pulpitu zdalnego, blokując jakikolwiek inny rodzaj połączeń.

Obszar bezpieczeństwa informacji nadzorowany był także poprzez monitorowanie logowań do systemów dziedzinowych, przeglądy przydzielonych uprawnień, weryfikację upoważnień do korzystania z pulpitu zdalnego.

6. ZAŁĄCZNIKI

6.1. Metodyka kontroli i informacje dodatkowe

Cel główny kontroli

Czy podmioty realizujące zadania publiczne zapewniły aktualność rozwiązań w Systemie Zarządzania Bezpieczeństwem Informacji, umożliwiających bezpieczne przetwarzanie informacji w przypadku wprowadzenia trybu pracy zdalnej?

Cele szczegółowe

1. Czy monitorowano sposób przetwarzania przez jednostki administracji publicznej danych w pracy na odległość w celu zachowania bezpieczeństwa informacji?
2. Czy zapewniono należytą organizację bezpieczeństwa informacji?
3. Czy opracowane rozwiązania techniczne i organizacyjne wdrożono, stosowano i egzekwowano?

Zakres podmiotowy

Kontrolę przeprowadzono w 11 wybranych podmiotach wykonujących zadania publiczne, w tym: w Kancelarii Prezesa Rady Ministrów, w Izbie Administracji Skarbowej, dwóch jednostkach wojewódzkiej administracji zespolonej, dwóch starostwach, trzech urzędach miast i dwóch urzędach gmin.

Kryteria kontroli

Siedem jednostek samorządu terytorialnego zostało skontrolowanych na podstawie art. 2 ust. 2 ustawy o NIK z uwzględnieniem kryteriów legalności i rzetelności (art. 5 ust. 2). Kontrole w pozostałych czterech podmiotach przeprowadzono na podstawie art. 2 ust. 1, z uwzględnieniem kryteriów legalności i rzetelności (art. 5 ust. 1).

Okres objęty kontrolą

1 stycznia 2020 r.–30 listopada 2021 r.

Wnioski pokontrolne

Wyniki kontroli przedstawiono w 11 wystąpieniach pokontrolnych, w których sformułowano 18 wniosków oraz jedną uwagę. Na podstawie informacji o sposobie wykonania wniosków pokontrolnych wg stanu na 1 marca 2022 r. zrealizowanych zostało 12 wniosków, a cztery były w trakcie realizacji. Do żadnego z wysłanych wystąpień nie wniesiono zastrzeżeń

Działania na podstawie art. 29 ustawy o NIK

Przed rozpoczęciem kontroli, w trybie art. 29 ust. 1 pkt 1 od 142 jednostek wykonujących zadania publiczne na terenie województwa warmińsko-mazurskiego uzyskano informacje o liczbie osób skierowanych do wykonywania zadań w systemie pracy zdalnej, a także o liczbie osób, które wykonywały tę pracę z wykorzystaniem służbowych urządzeń teleinformatycznych oraz niebędących własnością pracodawcy. Informacje te zostały wykorzystane do wytypowania w ramach doboru celowego jednostek, w których przeprowadzono kontrole.

Wykaz jednostek kontrolowanych

Lp.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
1.	Delegatura w Olsztynie	Kancelaria Prezesa Rady Ministrów	Michał Dworczyk
2.		Izba Administracji Skarbowej w Olsztynie	Mariusz Pawłowski
3.		Wojewódzki Inspektorat Farmaceutyczny w Olsztynie	Elżbieta Kuriata
4.		Wojewódzki Urząd Ochrony Zabytków w Olsztynie	Dariusz Barton
5.		Starostwo Powiatowe w Bartoszycach	Jan Zbigniew Nadolny
6.		Starostwo Powiatowe w Gołdapi	Marzanna Wardziejewska
7.		Urząd Miejski w Morągu	Tadeusz Sobierajski
8.		Urząd Miejski w Pasłęku	Wiesław Śniecikowski
9.		Urząd Miejski w Olsztynku	Mirosław Wojciech Stegienko
10.		Urząd Gminy w Gietrzwałdzie	Jan Kasprowicz
11.		Urząd Gminy w Jedwabnie	Sławomir Ambroziak

Wykaz ocen kontrolowanych jednostek

Lp.	Nazwa jednostki kontrolowanej	Stany mające wpływ na wydaną ocenę:	
		prawidłowe	nieprawidłowe
1.	Kancelaria Prezesa Rady Ministrów	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.	
2.	Izba Administracji Skarbowej w Olsztynie	Izba Administracji Skarbowej właściwie realizowała zadania określone w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Funkcjonujący w Izbie System Zarządzania Bezpieczeństwem Informacji, został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, zawierał reguły, procedury i zasady, według których Izba zarządzała i udostępniała swoje zasoby informacji. Zgodnie z art. 37 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), wyznaczono inspektora ochrony danych. Osoba wyznaczona na to stanowisko spełniała wymagania określone w art. 37 ust 5 RODO. Opracowany SZBI zapewniał bezpieczeństwo informacji w trakcie wykonywania pracy zdalnej. Podczas pracy zdalnej stosowano regulacje i procedury określone w SZBI. Stosowano rozwiązania techniczne i technologiczne podnoszące poziom bezpieczeństwa informacji. Zapoznano pracowników z zasadami zapewnienia bezpieczeństwa informacji w wykonywaniu pracy zdalnej.	
3.	Wojewódzki Inspektorat Farmaceutyczny w Olsztynie	Wprowadzona w listopadzie 2020 r. Polityka bezpieczeństwa danych osobowych została opracowana na podstawie Polskiej Normy PN-ISO/IEC 27001, zawierała ona reguły, procedury i zasady, według których Inspektorat zarządzał i udostępniał swoje zasoby informacji. Wprowadzenie PBDO pozwoliło na właściwe realizowanie zadań określonych w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Zgodnie z art. 37 ust. 1 Rozporządzenia	W Inspektoracie do listopada 2020 r. obowiązywała polityka bezpieczeństwa, która odnosiła się jedynie do bezpieczeństwa przetwarzania danych osobowych określonych w RODO.

Lp.	Nazwa jednostki kontrolowanej	Stany mające wpływ na wydaną ocenę:	
		prawidłowe	nieprawidłowe
		Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) , wyznaczono inspektora ochrony danych (dalej: IOD). W celu zapewnienia ciągłości działania Inspektoratu, wprowadzono system pracy zdalnej, a opracowana PBDO zapewniała bezpieczeństwo informacji w trakcie jej wykonywania.	
4.	Wojewódzki Urząd Ochrony Zabytków w Olsztynie	W Urzędzie określono i przypisano odpowiedzialność za bezpieczeństwo informacji pracownikom oraz wyznaczono Inspektora Ochrony Danych. W obowiązującej Polityce ochrony danych osobowych określono zasady postępowania z nośnikami i urządzeniami przenośnymi, wynoszenia aktywów z Urzędu oraz przesyłania informacji. Zapoznano pracowników z zasadami bezpieczeństwa informacji, w tym w pracy zdalnej. Przeprowadzono analizę ryzyka pracy zdalnej, zaś w oparciu o jej wyniki wprowadzono Regulamin pracy zdalnej i zorganizowano ją w Urzędzie. Wdrożone i stosowane rozwiązania organizacyjne i techniczne służyły zapewnieniu bezpieczeństwa danych osobowych w pracy zdalnej. Wprowadzona organizacja pracy (m.in. dostęp do sieci Urzędu wyłącznie za pomocą służbowego sprzętu komputerowego, założenie przekazywania pracownikom korzystającym ze sprzętu prywatnego zadań niewymagających przetwarzania danych chronionych) minimalizowała ryzyko naruszenia bezpieczeństwa danych osobowych. Stosowano sprzętowe i programowe środki służące ochronie informacji podnoszące poziom ich bezpieczeństwa, zgodnie z zasadami przyjętymi w Urzędzie.	Nieopracowanie, nieustanowienie i niewdrożenie w Urzędzie systemu zarządzania bezpieczeństwem informacji (w tym polityki bezpieczeństwa informacji), stosownie do przepisów rozporządzenia KRI, obejmujących swoim zakresem wszystkie kategorie przetwarzanych w Urzędzie informacji. Przyjęcie Instrukcji postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych po dwóch latach i ośmiu miesiącach od wprowadzenia obowiązku jej stosowania w Urzędzie. Nieuwzględnienie zasad korzystania z prywatnych komputerów i prywatnych kont pocztowych do celów służbowych w uregulowaniach Urzędu, mimo że dopuszczono możliwość korzystania z takiego sprzętu podczas pracy zdalnej, a reguły takie zostały określone analizie ryzyka pracy zdalnej, Nieprecyzyjne określenie w Regulaminie pracy zdalnej obowiązków pracownika w przypadku udostępnienia mu dokumentacji w wersji papierowej w celu wykonywania pracy zdalnej.
5.	Starostwo Powiatowe w Bartoszycach	Wszystkim pracownikom administracyjnym Urzędu przypisano w zakresach czynności pracowniczych odpowiedzialność za ochronę danych osobowych, pracownicy merytoryczni Urzędu potwierdzili zapoznanie z treścią Polityki Ochrony Danych Osobowych. Starosta wypełnił wymóg z art. 37 ust. 1 Rozporządzenia 679/2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE powołując Inspektorów Ochrony Danych w Starostwie. W Urzędzie prowadzona była ewidencja osób upoważnionych do przetwarzania danych osobowych według wzoru określonego w załączniku nr 9 do PODO.	W kontrolowanym okresie nie dokonywano przeglądów PODO i tym samym nie modyfikowano zawartych w nich procedur. Nie opracowano, nie ustanowiono i nie wdrożono w Urzędzie Systemu Zarządzania Bezpieczeństwem Informacji (w tym Polityki Bezpieczeństwa Informacji), stosownie do przepisów rozporządzenia KRI, obejmujących swoim zakresem wszystkie kategorie przetwarzanych w Urzędzie informacji, Nie realizowano niektórych zadań określonych w zasadach pracy zdalnej z wykorzystaniem sprzętu komputerowego, tj. monitorowania ruchu sieciowego pod kątem wystąpienia niepożądanych połączeń oraz włączania i konfigurowania zapory sieciowej w celu uniemożliwienia podłączenia komputera do niezabezpieczonych sieci Wi-Fi.

		Administrator Danych Osobowych stosował opracowane i ustanowione zasady wobec osób wykonujących pracę zdalną zawarte w PODO. Stosowano także rozwiązania techniczne i technologiczne podnoszące poziom bezpieczeństwa przetwarzanych informacji. Pracownicy zatrudnieni w Starostwie, wykonujący pracę zdalną w latach 2020/2021 potwierdzili w formie oświadczenia zapoznanie się z zasadami ochrony danych osobowych podczas pracy zdalnej zawartymi w PODO.	
6.	Starostwo Powiatowe w Gołdapi	Starostwo zapewniło warunki organizacyjne do realizacji zadań objętych kontrolą. Opracowano oraz wdrożono w tym celu odpowiednie zasady systemu zarządzania bezpieczeństwem informacji, obejmujące politykę tego bezpieczeństwa i instrukcję zarządzania systemem informatycznym w Starostwie, z uwzględnieniem przepisów krajowych i UE w zakresie ochrony danych osobowych, w tym krajowych ram interoperacyjności i polskich norm. Zasady te poddawano regularnym przeglądom, wyciągając z nich wnioski organizacyjne. Powołano też inspektora ochrony danych osobowych, który posiadał odpowiednie przygotowanie zawodowe i kwalifikacje oraz brał udział w szkoleniach specjalistycznych. Przydzielono mu obowiązki wynikające z tych przepisów, za wyjątkiem audytowania zagadnień związanych z ochroną danych osobowych, gdyż zadanie to było obowiązkiem audytora wewnętrznego. Odpowiedzialność za bezpieczeństwo teleinformatyczne oraz administrowanie zasobami informacji ponosił informatyk urzędu, prowadząc odpowiednie rejestry posiadanego sprzętu/ aktywów informatycznych. Wprowadzone zasady i rozwiązania techniczno--technologiczne, które uwzględniały zidentyfikowane ryzyka, zapewniły odpowiedni poziom bezpieczeństwa informacji oraz jakość i ciągłość funkcjonowania urzędu w warunkach epidemii COVID-19, przy czym ich aktualizacja podniosła ten poziom adekwatnie do zagrożenia epidemią. Wdrażając te regulacje zorganizowano odpowiednie szkolenie wewnętrzne dla wszystkich pracowników oraz zapoznawano ich z aktualizacją lub modyfikacją zasad dotyczących bezpieczeństwa informacji, w tym warunków pracy zdalnej i rotacyjnej	
7.	Urząd Miejski w Morągu	Regulacje oraz rozwiązania techniczne i informatyczne w zakresie wykonywanej przez pracowników Urzędu pracy zdalnej wprowadzono 20 października 2020 r., dopuszczając jej świadczenie przy wykorzystaniu urządzeń służbowych oraz prywatnych. Do zapewnienia, iż praca ta, wykonywana w oparciu o zasoby informatyczne Urzędu, była realizowana w taki sam sposób jak w siedzibie jednostki, wykorzystano bezpieczne połączenie z siecią Urzędu poprzez VPN i zdalny pulpit. Przed rozpoczęciem wykonywania pracy zdalnej przeszkolono pracowników w zakresie bezpiecznego łączenia się z siecią wewnętrzną Urzędu.	Nieopracowanie, nieustanowienie, niewdrożenie systemu zarządzania bezpieczeństwem informacji, w tym polityki bezpieczeństwa informacji, do czego był zobligowany jako podmiot realizujący zadania publiczne. W Urzędzie, co prawda, opracowano politykę danych osobowych, instrukcję określającą sposób zarządzania systemem informatycznym oraz regulamin pracy zdalnej, jednak nie zostały one przygotowane na podstawie Polskiej Normy PN-EN ISO/IEC 27001. W okresie objętym kontrolą obowiązujące w Urzędzie regulacje wewnętrzne nie były poddawane udokumentowanym, regularnym przeglądom, a ostatnie

Lp.	Nazwa jednostki kontrolowanej	Stany mające wpływ na wydaną ocenę:	
		prawidłowe	nieprawidłowe
			aktualizacje posiadanych dokumentów w zakresie danych osobowych były wykonane w 2019 r. Regulamin pracy zdalnej wdrożono dopiero 221 dni po rozpoczęciu wykonywania przez pracowników Urzędu pracy w tej formie, a odpowiedzialności za zapewnienie bezpieczeństwa informacji zostały przypisane odpowiednim pracownikom tylko w zakresie danych osobowych. W obowiązującym w Urzędzie regulaminie organizacyjnym nie uwzględniono stanowiska inspektora ochrony danych osobowych wyznaczonego 22 maja 2018 r. przez Burmistrza.
8.	Urząd Miejski w Pasłęku	Wprowadzony zarządzeniem Burmistrza Pasłęka System Zarządzania Bezpieczeństwem Informacji, spełniający wymogi określone w § 20 ust. 1 i 2 ww. rozporządzenia, obowiązywał od 21 czerwca 2021 r. Pracownicy Urzędu wykonywali swoje zadania w ramach pracy zdalnej z wykorzystaniem rozwiązań technicznych i technologicznych podnoszących poziom bezpieczeństwa informacji ukierunkowanych na ochronę danych osobowych. Dostępu do zasobów Urzędu na potrzeby wykonywania pracy zdalnej udzielano na ogół na podstawie stosownych upoważnień. Pracownicy Urzędu zostali zapoznani z zasadami bezpieczeństwa informacji w pracy na odległość. Zasady te były stosowane w zakresie korzystania z zasobów Urzędu oraz oprogramowania w ramach udzielonych pracownikom upoważnień.	Do 20 czerwca 2021 r. w Urzędzie Miejskim w Pasłęku nie ustanowiono i nie wdrożono systemu zarządzania bezpieczeństwem informacji wymaganego rozporządzeniem KRI, do czego Urząd, jako podmiot realizujący zadania publiczne, był zobligowany. Obowiązująca w Urzędzie Polityka Bezpieczeństwa spełniała część minimalnych wymagań Polskiej Normy PN-ISO/IEC 27001 (dalej: PN-ISO/IEC 27001) w odniesieniu do bezpieczeństwa przetwarzania danych osobowych.
9.	Urząd Miejski w Olsztynku	W okresie objętym kontrolą aktualizację obowiązujących w Urzędzie regulacji wewnętrznych dotyczących bezpieczeństwa danych osobowych przeprowadzano w szczególności w zakresie obowiązujących procedur, powołano Inspektora Ochrony Danych, któremu powierzono realizację zadań, stosownie do art. 37 ust. 1 lit. a rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), a także zapewniono pracownikom Urzędu dostęp do szkoleń w zakresie przetwarzania danych osobowych. Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI przeprowadzano audyty w zakresie bezpieczeństwa informacji. Stosowano i egzekwowano zasady wprowadzone regulaminem pracy zdalnej oraz związane z czasową zmianą organizacji pracy, a przed przystąpieniem przez pracowników do świadczenia pracy zdalnej zapoznano ich z zasadami bezpieczeństwa informacji podczas jej wykonywania, przede wszystkim jednak z zasadami ochrony danych osobowych.	Nie opracowano i nie wdrożono kompletnego systemu zarządzania bezpieczeństwem informacji, w szczególności kompletnej polityki bezpieczeństwa informacji, co było niezgodne z § 20 ust. 1 w związku z ust. 3 rozporządzenia KRI nie skonfigurowano na trzech komputerach przenośnych (laptopach) indywidulanych kont użytkowników uprawniających do korzystania z operacyjnego systemu informatycznego, co było niezgodne z Polityką Ochrony Danych oraz Polityką Ochrony Danych Osobowych, a także nie zabezpieczono ww. laptopów przed utratą poufności informacji w przypadku ich utraty, co było niezgodne z Polską Normą EN ISO/IEC 27001:2017 A.11.2.6. dotyczącą m.in. bezpieczeństwa sprzętu i aktywów poza siedzibą.

10.	Urząd Gminy w Gietrzwałdzie	Prawidłowo wdrożono i stosowano określone w SZBI rozwiązania organizacyjne i techniczne mające na celu zapewnienie bezpieczeństwa informacji w pracy zdalnej. Zagadnienia dotyczące pracy zdalnej uregulowano stosownymi zarządzeniami Wójta, a przyjęte rozwiązania techniczne i informatyczne umożliwiały jej wykonywanie. Realizację zadań w systemie pracy zdalnej poprzedzono działaniami zmierzającymi do przekazania pracownikom informacji w zakresie bezpiecznego łączenia się z siecią wewnętrzną Urzędu.	W Urzędzie nie w pełni przestrzegano wymogów określonych w SZBI. Dotyczyło to nierealizowania obowiązków w zakresie: pisemnego potwierdzania zapoznawania pracowników z regulacjami wewnętrznymi, wydawania pracownikom upoważnień do przetwarzania danych osobowych oraz prowadzenia szkoleń dla pracowników zaangażowanych w proces przetwarzania informacji. Stwierdzono również przypadki niewywiązywania się z obowiązków nałożonych rozporządzeniem KRI. W 2020 r. w Urzędzie nie zapewniono bowiem wykonania wymaganych tym rozporządzeniem: corocznego audytu zgodności oraz okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji. Nie dokonywano także aktualizacji PBI w celu dostosowania regulacji w niej zawartych do zmieniającego się otoczenia, w związku ze zmianami w powszechnie obowiązujących przepisach. Nie wykorzystano w pełni możliwości skonfigurowania serwera Urzędu w zakresie ustawień wymuszających od użytkowników stosowania haseł o złożoności zgodnej z wymogami obowiązujących regulacji wewnętrznych.
11.	Urząd Gminy w Jedwabnie	W Urzędzie określono i przypisano odpowiedzialność za bezpieczeństwo informacji pracownikom oraz wyznaczono Inspektora Ochrony Danych. W obowiązującej w Urzędzie polityce dotyczącej bezpieczeństwa przetwarzania danych osobowych określono zasady: postępowania z nośnikami i urządzeniami przenośnymi, wynoszenia aktywów z Urzędu, przesyłania informacji oraz zarządzania incydentami związanymi z bezpieczeństwem informacji. Zapoznano pracowników z zasadami bezpieczeństwa informacji przy przetwarzaniu danych osobowych. Po przeprowadzonych analizach ryzyka bezpieczeństwa informacyjnego oraz pracy zdalnej wprowadzano regulacje doprecyzowujące obowiązujące procedury bezpieczeństwa informacji w Urzędzie. W marcu 2021 r. wprowadzono regulamin pracy zdalnej, w którym określono: warunki podjęcia pracy zdalnej, warunki jakie musi spełniać miejsce jej świadczenia oraz zasady ochrony informacji i danych osobowych. Wdrożone rozwiązania organizacyjne i techniczne służyły zapewnieniu bezpieczeństwa danych osobowych w pracy zdalnej.	Nieopracowanie, nieustanowienie i niewdrożenie w Urzędzie Systemu Zarządzania Bezpieczeństwem Informacji (w tym Polityki Bezpieczeństwa Informacji), stosownie do przepisów rozporządzenia KRI, obejmujących swoim zakresem wszystkie kategorie przetwarzanych w Urzędzie informacji. Nieprzestrzeganie określonych w Urzędzie zasad bezpieczeństwa informacji w pracy zdalnej, tj. uregulowań w zakresie zasad postępowania z pamięciami przenośnymi oraz obowiązków wynikających z Regulaminu pracy zdalnej.

6.2. Analiza stanu prawnego i uwarunkowań organizacyjno-ekonomicznych

Przepisy wprowadzające możliwość pracy zdalnej

W ustawie z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (dalej: ustawa Covid) w art. 3 określono, że w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii, ogłoszonego z powodu COVID-19, oraz w okresie 3 miesięcy po ich odwołaniu, w celu przeciwdziałania COVID-19 pracodawca może polecić pracownikowi wykonywanie, przez czas oznaczony, pracy określonej w umowie o pracę, poza miejscem jej stałego wykonywania (praca zdalna). Zgodnie z tymi przepisami:

- wykonywanie pracy zdalnej może zostać polecone, jeżeli pracownik ma umiejętności i możliwości techniczne oraz lokalowe do wykonywania takiej pracy i pozwala na to rodzaj pracy;
- praca zdalna może być wykonywana w szczególności przy wykorzystaniu środków bezpośredniego porozumiewania się na odległość lub dotyczyć wykonywania części wytwórczych lub usług materialnych;
- pracodawca zapewnia narzędzia i materiały potrzebne do wykonywania pracy oraz jej obsługę logistyczną;
- pracownik może używać narzędzi lub materiałów niezapewnionych przez pracodawcę pod warunkiem, że umożliwia to poszanowanie i ochronę informacji poufnych i innych tajemnic prawnie chronionych, w tym tajemnicy przedsiębiorstwa lub danych osobowych, a także informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

Wykonywanie zadań w systemie pracy zdalnej przez pracowników jednostek realizujących zadania publiczne wymaga dostępu do informacji, baz danych, zbiorów dokumentów, które wchodzą w skład aktywów informacyjnych jednostki. Zasady wykonywania pracy zdalnej powinny zatem zapewnić spełnienie warunków bezpiecznego przetwarzania z uwzględnieniem wszystkich atrybutów opisujących bezpieczeństwo informacji.

W zależności od typu jednostki, możliwości technicznych, poziomu wykorzystywania narzędzi informatycznych, rangi realizowanych zadań i innych uwarunkowań praca zdalna mogła być wykonywana m.in.:

- z wykorzystaniem służbowych komputerów (przenośnych lub stacjonarnych) zapewnionych przez pracodawcę z dostępem zdalnym (lub bez takiego dostępu) do systemów teleinformatycznych jednostki;
- na prywatnych komputerach, z wykorzystaniem poczty elektronicznej, aplikacji klienckich lub webowych służących do komunikacji i wymiany informacji;
- w oparciu o dokumenty tradycyjne (lub ich kopie) pobrane z jednostki z wykorzystaniem prywatnego sprzętu komputerowego i oprogramowania;
- w oparciu o dokumenty tradycyjne (lub ich kopie) bez wykorzystania sprzętu komputerowego.

Każda z form wykonywania pracy zdalnej może być obarczona innym zbiorem ryzyk obejmujących szeroko rozumiane bezpieczeństwo informacji. Niewłaściwe zarządzanie bezpieczeństwem informacji może umożliwić wyciek, utratę lub sfałszowanie danych i w konsekwencji doprowadzić do strat, kosztów, a nawet do całkowitego paraliżu pracy urzędu.

Przepisy dotyczące bezpieczeństwa informacji

Zgodnie z obowiązującymi przepisami[12] podmiot realizujący zadania publiczne powinien opracować i ustanowić, wdrożyć i eksploatować, monitorować i przeglądać oraz utrzymywać i doskonalić system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Wymaga to opracowania dokumentacji SZBI zawierającej szereg regulacji wewnętrznych oraz zapewnienia ich aktualizacji w zakresie zmieniającego się otoczenia.

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w punkcie 4;
6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

[12] § 20 ust.1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247); dalej: rozporządzenie KRI.

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
   a) dbałości o aktualizację oprogramowania,
   b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
   e) zapewnieniu bezpieczeństwa plików systemowych,
   f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
   g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
   h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Wprowadzenie systemu pracy zdalnej w celu zapewnienia ciągłości działania jednostki w zmieniającym się otoczeniu spowodowało pojawienie się nowych ryzyk dotyczących bezpieczeństwa informacji. Część z nich mogła się już zmaterializować powodując szkody i straty (materialne lub

wizerunkowe). Należy przy tym zauważyć, że w powszechnym odbiorze bezpieczeństwo informacji kojarzy się przede wszystkim z zapewnieniem poufności, natomiast oceniać je należy również według kryterium dostępności i integralności z uwzględnieniem takich cech jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Dodatkowo, doświadczenia uzyskane w czasie izolacji społecznej mogły otworzyć potrzeby i możliwości wykonywania pracy zdalnej nie tylko w sytuacji wymuszonej okolicznościami wynikającymi z sytuacji epidemicznej ale również na podstawie innych przesłanek, co również w przypadku braku regulacji w tym zakresie wymaga aktualizacji SZBI. Według ekspertów, przynajmniej częściowa praca zdalna (tzw. model hybrydowy) zagości na dłużej. Dlatego zasadne jest, aby w jednostkach, które wprowadziły pracę zdalną funkcjonowały stosowne regulaminy, które dookreślają zasady ponoszenia odpowiedzialności za poszczególne jej elementy. Należy również zwrócić uwagę, że ustalanie reguł jest elementem systemu kontroli zarządczej.

Nieregularna praca zdalna nie jest unormowana w polskich przepisach, a regulacje dotyczące pracy zdalnej zawarte w ustawie Covid-19 są bardzo podstawowe i nie wychodzą naprzeciw wielu zagadnieniom związanym z pracą zdalną, takim jak:

- odpowiedzialność za bezpieczeństwo i higienę pracy pracownika zdalnego;
- reguły ustalania ekwiwalentu za korzystanie z własnych narzędzi przez zatrudnionych (jak Internet, telefon itp.);
- postępowanie z informacjami stanowiącymi tajemnicę przedsiębiorstwa lub informacjami zawierającymi dane osobowe;
- zasady przewożenia, przesyłania i transmisji dokumentów pomiędzy biurem a miejscem zamieszkania pracownika oraz ich odpowiedniego przechowywania w miejscu pracy zdalnej.

Minister Rodziny i Polityki Społecznej złożył w grudniu 2021 r. projekt ustawy o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw, zakładający m.in. dodanie w ustawie Kodeks Pracy w dziale drugim rozdziału IIc – „Praca zdalna" regulującego zasady wykonywania pracy w miejscu wskazanym przez pracownika i uzgodnionym z pracodawcą, w tym pod adresem zamieszkania pracownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość (praca zdalna)[13].

Bezpieczeństwo informacji to nie tylko bezpieczna sieć, programy antywirusowe, hasła i poufność. To także ludzie i ich wiedza oraz słabości, sposób wykonywania codziennych zadań, zamknięte drzwi i porządek na biurku, dostępność do informacji oraz jej kompletność. W przypadku pracy zdalnej pracodawca nie ma bezpośredniej kontroli nad wieloma jej elementami dlatego oprócz regulaminów i procedur niezbędne są szkolenia uświadamiające pracownikom zagrożenia, ryzyka i odpowiedzialność.

[13] https://legislacja.rcl.gov.pl/docs//2/12354104/12835646/dokument543273.DOCX

System informacyjny może być uważany za bezpieczny wtedy, gdy spełnia oczekiwania, że dane i informacje do niego wprowadzone będą tam tak długo jak potrzeba, nie zostaną odczytane przez nikogo, kto nie powinien ich odczytać, a ich modyfikacja możliwa jest wyłącznie przez użytkowników do tego uprawnionych.

Cykl życia informacji składa się z tworzenia (gromadzenia), przekazywania, przetwarzania, archiwizacji i niszczenia. Na poszczególnych etapach tego cyklu niezbędne jest podejmowanie różnych działań pozwalających na zapewnienie odpowiedniej ochrony. Na etapie tworzenia (gromadzenia) informacji ochrona polega na zapisaniu informacji kompletnej, niesprzecznej, w sposób czytelny, we właściwym miejscu, formie i czasie. Ochrona na etapie przekazywania informacji polega na przekazywaniu jej właściwym adresatom, w terminie, odpowiednim kanałem oraz w tajemnicy przed niepożądanymi adresatami. Przetwarzanie powinno być realizowane z zachowaniem poufności, tak aby ci którzy powinni mieli dostęp oraz bez utraty informacji. Archiwizowanie (przechowywanie) powinno dotyczyć tych informacji, które trzeba i można przechowywać oraz być realizowane odpowiednio długo w odpowiednich miejscach oraz formie z możliwością szybkiego odtworzenia. Niszczenie (usuwanie) informacji które trzeba i można usunąć powinno odbywać się skutecznie i w odpowiednim czasie.

Informacje mogą być klasyfikowane według różnych kryteriów. Z punktu widzenia zarządzania bezpieczeństwem informacji istotne jest powiązanie rodzajów informacji z zasadami dotyczącymi ich ochrony oraz rodzajami tajemnic określonych w różnych przepisach.

Opracowując SZBI i dokonując klasyfikacji informacji istotnych dla instytucji, kierownictwo jednostki nie może pominąć kryteriów określających poszczególne rodzaje tajemnic (przedsiębiorstwa, skarbowa, korespondencji, dane osobowe, itp.).

W łańcuchu decyzyjnym występują ludzie, urządzenia, programy komputerowe, kanały transmisyjne. Każdy z tych elementów wykazuje określoną podatność na zagrożenia, które mogą zmaterializować się w postaci wydania niewłaściwej decyzji. Ponieważ podejmowanie decyzji zarządczych, wydawanie decyzji administracyjnych oraz realizacja zadań własnych czy zleconych oparte jest na przetwarzaniu informacji niezbędne jest podjęcie odpowiednich działań, dzięki którym uzyskane zostanie zapewnienie, że informacje, które są podstawą podejmowanych decyzji są prawdziwe, rzetelne i wiarygodne.

Podejmowanie szybkich decyzji będących reakcją na zmiany w otoczeniu oraz wprowadzanie nowych rozwiązań w zakresie organizacji pracy powinno być zrównoważone odpowiedzialnością, przejrzystością i uczciwością w zarządzaniu.

6.3. Wykaz aktów prawnych dotyczących kontrolowanej działalności

1. Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2021r. poz. 2095, ze zm.).
2. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2071, ze zm.).
3. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz.1369, ze zm.).
4. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2021 r. poz. 735, ze zm.).
5. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247).
6. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).
7. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz 127 z 23.05.2018, str. 2.).
8. Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2021 r. poz. 305, ze zm.).
9. Komunikat Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. MF. z 2009 r. nr 15, poz. 84).
10. Polska Norma Technika informatyczna, techniki bezpieczeństwa, Systemy zarządzania bezpieczeństwem informacji, Wymagania (PN-EN ISO/IEC 27001:2017-06).

6.4. Wykaz podmiotów, którym przekazano informację o wynikach kontroli

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów
5. Prezes Trybunału Konstytucyjnego
6. Rzecznik Praw Obywatelskich
7. Sejmowa Komisja do Spraw Kontroli Państwowej (KOP)
8. Sejmowa Komisja Administracji i Spraw Wewnętrznych (ASW)
9. Sejmowa Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (CNT)
10. Senacka Komisja Samorządu Terytorialnego i Administracji Państwowej
11. Prezes Urzędu Ochrony Danych Osobowych
12. Wojewodowie
13. Marszałkowie województw