NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie

LOL.410.017.09.2021

Mirosław Wojciech Stegienko
Burmistrz Olsztynka
Urząd Miejski w Olsztynku
Ratusz 1
11-015 Olsztynek

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie
ul. Artyleryjska 3e, 10-165 Olsztyn
T +48 89 678 82 00, F +48 89 678 82 30
lol@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Olsztynku, Ratusz 1, 11-015 Olsztynek, dalej: Urząd
Kierownik jednostki kontrolowanej	Mirosław Wojciech Stegienko, Burmistrz Olsztynka, od 22 listopada 2018 r., dalej: Burmistrz
Zakres przedmiotowy kontroli	1. Organizacja bezpieczeństwa informacji. 2. Wdrożone i stosowane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji w pracy zdalnej.
Okres objęty kontrolą	Lata 2020-2021 (do 16 listopada) z uwzględnieniem zdarzeń wcześniejszych, jeżeli miały one wpływ na kontrolowane obszary działalności.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Olsztynie
Kontroler	Lidia Wójcik, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LOL/113/2021 z 16 września 2021 r.

(akta kontroli str.1-3)

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą obowiązujące w Urzędzie regulacje wewnętrzne dotyczyły przede wszystkim bezpieczeństwa danych osobowych. W tym zakresie przeprowadzano w szczególności: aktualizację obowiązujących procedur, powołano Inspektora Ochrony Danych[3], 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)[4], a także zapewniono pracownikom Urzędu dostęp do szkoleń w zakresie przetwarzania danych osobowych. Zgodnie z § 20 ust. 2 pkt 14 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[5] 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.

[1] Dz. U. z 2020 r. poz. 1200, ze zm., dalej: ustawa o NIK.
[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[3] Dalej: IOD.
[4] Dz. Urz. UE L 119 z 4 maja 2016 r., dalej: rozporządzenie RODO.
[5] Dz. U. z 2017 r. poz. 2247, dalej: rozporządzenie KRI.

W Urzędzie nie zapewniono należytego bezpieczeństwa informacji oraz nie stosowano wystarczających rozwiązań służących ochronie przetwarzania danych na urządzeniach mobilnych wykorzystywanych przez pracowników Urzędu przy wykonywaniu pracy zdalnej. Stwierdzono bowiem, że:

– 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.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[6] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. W Urzędzie nie opracowano, nie ustanowiono i nie wdrożono systemu zarządzania bezpieczeństwem informacji (w tym polityki bezpieczeństwa informacji), o którym mowa w § 20 ust. 1 w zw. z § 20 ust. 3 rozporządzenia KRI.

W okresie objętym kontrolą, w zakresie bezpieczeństwa przetwarzania danych, obowiązujące w Urzędzie regulacje wewnętrzne dotyczyły, przede wszystkim przetwarzania danych osobowych.

Były to:

- Polityka Ochrony Danych[7] przygotowana w oparciu o rozporządzenie RODO oraz ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych[8] obejmująca także pracę w systemach informatycznych. Celem opracowania i wdrożenia tej Polityki było zdefiniowanie ogólnych wymagań i zasad ochrony, które będą fundamentem dla wszystkich dokumentów związanych z ochroną danych osobowych.
- Polityka Ochrony Danych Osobowych[9] opracowana została w celu spełnienia wymagań wynikających z rozporządzenia RODO, ustawy o ochronie danych osobowych, rozporządzenia KRI, przepisów szczególnych regulujących funkcjonowanie Urzędu i przetwarzanych w ramach jej działalności danych osobowych oraz dobrych praktyk z zakresu bezpieczeństwa informacji oraz ochrony danych osobowych. Polityka ta zawierała instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, a zakres jej stosowania obejmował dane osobowe przetwarzane w systemach informatycznych oraz w postaci papierowej będących w zasobach Urzędu.

[6] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

[7] Polityka Ochrony Danych wprowadzona Zarządzeniem Nr K/70/2018 Burmistrza Olsztynka z dnia 17 września 2018 r. w sprawie Polityki Ochrony Danych, ze zm. Polityka ta obowiązywała od 17 września 2018 r. do 14 lutego 2021 r.

[8] Dz. U. z 2019 r. poz. 1781, dalej: ustawa o ochronie danych osobowych.

[9] Polityka Ochrony Danych Osobowych wprowadzona Zarządzeniem Nr K/9/21 z dnia 28 stycznia 2021 r. w sprawie aktualizacji Polityki Ochrony Danych Osobowych, zmienionym Zarządzaniem nr K/31/21 z dnia 21 maja 2021 r. Polityka ta obowiązywała od 15 lutego 2021 r. do dnia zakończenia czynności kontrolnych NIK.

- Rejestr czynności przetwarzania danych osobowych[10].
- Analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych za lata 2020-2021 opracowane na podstawie rozporządzenia RODO oraz ustawy o ochronie danych osobowych, a także na bazie Polskich Norm: PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005.
- Raport z przeglądu podmiotowej strony Biuletynu Informacji Publicznej[11] oraz strony internetowej administratora[12] sporządzony 26 kwietnia 2021 r. przez IOD na podstawie rozporządzenia RODO i ustawy o ochronie danych osobowych.
- Raport z realizacji zadań IOD sporządzony 6 września 2021 r. na podstawie rozporządzenia RODO i ustawy o ochronie danych osobowych.
- Szacowanie ryzyka w Urzędzie na lata 2020-2021 uwzględniające zagrożenia wynikające z pandemii wirusa SARS-CoV-2 we wszystkich obszarach działalności Urzędu i związane z tym ryzyko czasowej zmiany organizacji pracy Urzędu na pracę zmianową lub zdalną.
- Zasady korzystania ze służbowych telefonów komórkowych przez pracowników Urzędu.[13]
- Audyty bezpieczeństwa informacji przeprowadzane w lutym 2020 r. oraz marcu 2021 r., na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[14], rozporządzeń: KRI i RODO, norm ISO: 27001:2017 i 27005:2017, a także udostępnionej przez Urząd dokumentacji (procedur) sprzętu. Ustalenia audytów w zakresie pracy zdalnej szczegółowo opisano w punkcie 1.9. wystąpienia pokontrolnego.

(akta kontroli str. 4-298)

Analiza zapisów Polityki Ochrony Danych oraz Polityki Ochrony Danych Osobowych[15] wykazała, że w obu tych dokumentach określono zasady dotyczące: postępowania z nośnikami, zarządzania uprawnieniami użytkowników, wynoszenia aktywów (m.in. sprzętu, nośników, kopii i oryginałów dokumentów papierowych), bezpieczeństwa sprzętu i aktywów poza siedzibą, pozostawienia sprzętu bez opieki, zabezpieczenia przed szkodliwym oprogramowaniem, zabezpieczenia sieci, przesyłania informacji, zabezpieczenia wiadomości w formie elektronicznej, zarządzania incydentami[16]. Dokumenty te zostały zatwierdzone przez Burmistrza i przedstawione do zapoznania się i stosowania pracownikom Urzędu. Wszyscy pracownicy Urzędu świadczący pracę zdalną (38 osób) w okresie objętym kontrolą potwierdzili podpisem zapoznanie się z ww. Politykami, a w ich aktach osobowych znajdowały się złożone przez nich oświadczenia o zachowaniu poufności danych osobowych oraz upoważnienia do przetwarzania danych osobowych.

Zgodnie z wymogami wynikającymi z rozporządzenia KRI ww. dokumentacja powinna odnosić się do zinwentaryzowanych i sklasyfikowanych informacji przetwarzanych w Urzędzie (nie zaś ograniczać się jedynie do danych osobowych), co szczegółowo opisano w sekcji stwierdzone nieprawidłowości.

(akta kontroli str. 4-146, 299-333)

[10] Wprowadzony Zarządzeniem Nr K/79/2019 Burmistrza Olsztynka z dnia 25 listopada 2019 r. w sprawie wprowadzenia zaktualizowanego Rejestru czynności przetwarzania danych osobowych w Urzędzie, ponownie zaktualizowany Zarządzeniami: Nr K/10/21 z dnia 1 lutego 2021 r. oraz Nr K/59/21 z dnia 5 października 2021 r.
[11] Dalej: BIP.
[12] Zgodnie z definicją zawartą w Polityce Ochrony Danych i jej aktualizacji administratorem była Gmina Olsztynek reprezentowana przez Burmistrza Olsztynka, dalej: administrator.
[13] Zarządzenie Burmistrza Nr K/47/21 z dnia 8 lipca 2021 r. w sprawie ustalenia zasad korzystania ze służbowych telefonów komórkowych przez pracowników Urzędu.
[14] Dz. U. z 2020 r. poz. 346, dalej: ustawa o informatyzacji.
[15] Dalej: Polityki.
[16] Zagadnienie wprowadzone w Polityce Ochrony Danych Osobowych z 28 stycznia 2021 r.

1.2. W Urzędzie zostali wyznaczeni pracownicy odpowiedzialni za bezpieczeństwo informacji. Na podstawie zakresów obowiązków oraz stosownych zarządzeń Burmistrza ustalono, że za poszczególne zadania w badanym okresie odpowiadali:

- osoby zajmujące kierownicze stanowiska w strukturze Urzędu, osoby zatrudnione na samodzielnych stanowiskach pracy oraz inni użytkownicy dopuszczeni przez administratora do przetwarzania danych osobowych w zakresie danych osobowych. W Politykach określono podmioty odpowiedzialne za ochronę i przetwarzanie danych osobowych. Były to: administrator, IOD, pracownicy IT oraz użytkownicy,
- Skarbnik Miasta w zakresie ochrony tajemnicy skarbowej,
- Sekretarz Miasta w ramach ogólnego nadzoru nad funkcjonowaniem Urzędu,
- pracownicy pionu ochrony pełniący funkcję inspektora bezpieczeństwa teleinformatycznego oraz administratorzy systemu teleinformatycznego[17],
- podmiot zewnętrzny – w zakresie danych osobowych IOD,
- pełnomocnik do spraw ochrony informacji niejawnych[18],
- pracownicy wchodzący w skład utworzonego w Urzędzie pionu ochrony informacji niejawnych,[19]
- Inspektor do spraw obsługi informatycznej w Referacie Organizacyjnym i Kadr wyznaczony do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa[20].

(akta kontroli str. 334-407)

Zgodnie z Politykami, odpowiedzialność za przeprowadzenie analizy zagrożeń i ryzyka, analizę incydentów oraz aktualizację zasad i procedur w nich ujętych przy przetwarzaniu danych osobowych przypisano administratorowi przy współpracy z IOD.

(akta kontroli str. 8-146)

1.3. Zgodnie z art. 37 ust. 1 litera a rozporządzenia RODO w Urzędzie został wyznaczony IOD. Osoba pełniącą tę funkcję w latach 2020-2021 działała na podstawie stosownych umów i posiadała niezbędne kwalifikacje wynikające z art. 37 ust. 5 rozporządzania RODO. Zgodnie umowami[21] z zawartymi na wykonywanie zadań IOD oraz świadczenie usług w zakresie doradztwa informatycznego, do zadań IOD należało, m.in:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzenie im w tej sprawie, w tym do udzielania konsultacji, wydawania zaleceń oraz wsparcia merytorycznego w sprawach związanych z przetwarzaniem danych osobowych w systemie informatycznym oraz wykonywania audytu informatycznego w oparciu o przepisy rozporządzenia KRI,
- monitorowanie przestrzegania rozporządzenia RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub

[17] Wyznaczeni Zarządzeniem Burmistrza Nr K/17/21 z dnia 30 marca 2021 r. w sprawie wyznaczenia pracowników pionu ochrony pełniący funkcję inspektora bezpieczeństwa teleinformatycznego oraz administratorzy systemu teleinformatycznego.

[18] Powołany Zarządzeniem Burmistrza Nr 20/2020/K z dnia 12 marca 2020 r. w sprawie powołania pełnomocnika ochrony niejawnych.

[19] Utworzony Zarządzeniem Burmistrza Nr K/52/2021 z dnia 6 sierpnia 2021 r. w sprawie utworzenia pionu ochrony informacji niejawnych w Urzędzie.

[20] Osoba wyznaczona Zarządzeniem Burmistrza Nr K/11/21 z dnia 15 lutego 2021 r. w sprawie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w Urzędzie.

[21] Nr: CBI/2525/2019/MZ/P z dnia 21 października 2019 r. obowiązująca do 31 października 2020 r. oraz Nr: CBI/2584/2019/NJ/P z dnia 20 października 2020 r. obowiązująca do 31 grudnia 2021 r.

podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 rozporządzenia RODO,
- współpraca z Prezesem Ochrony Danych Osobowych (organ nadzorczy),
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia RODO oraz w stosowanych przypadkach prowadzenie konsultacji we wszystkich innych sprawach.

(akta kontroli str. 379-401)

1.4. W okresie świadczenia pracy zdalnej przez pracowników Urzędu, tj. od 11 maja 2020 r.[22] do 16 kwietnia 2021 r.[23] obowiązywały w Urzędzie zasady postępowania dotyczące pracy na odległość. Zarządzeniem Burmistrza z dnia 16 marca 2020 r. ustanowiono w Urzędzie regulamin pracy zdalnej pracowników Urzędu[24], w którym określono m.in. wytyczne korzystania z powierzonego pracownikom sprzętu, danych i dokumentów, dotyczące w szczególności:
- stosowania hasła zabezpieczającego dostęp do komputerów służbowych,
- nieudostępniania służbowego sprzętu, oprogramowania ani haseł osobom trzecim,
- nieinstalowania żadnego oprogramowania na służbowym komputerze bez wyraźnego uzgodnienia z pracodawcą lub osobą wyznaczoną przez pracodawcę,
- przechowywania powierzonych dokumentów i danych w sposób całkowicie ograniczający dostęp do nich osób nieuprawionych,
- zabezpieczenia powierzonego sprzętu przed nieuprawnionym wykorzystaniem, zniszczeniem lub kradzieżą,
- prawidłowego zabezpieczenia powierzonych danych i informacji.

W regulaminie pracy zdalnej zawarto definicję „home office", przez którą należało rozumieć czasowe wykonywanie przez pracowników pracy zdalnej, w tym przy pomocy urządzeń elektronicznych w miejscu ich zamieszkania. Szerzej o ww. regulaminie opisano w punkcie 1.5. wystąpienia pokontrolnego.

Dodatkowo regulamin ten zobowiązywał pracowników Urzędu do przestrzegania wszelkich zasad obowiązujących u pracodawcy dotyczących korzystania z powierzonego mu sprzętu, danych i dokumentów, w tym w szczególności do przestrzegania obowiązujących u pracodawcy zasad ochrony danych, w tym danych osobowych określonych obowiązującą Polityką bezpieczeństwa oraz danych stanowiących tajemnicę pracodawcy.

Obowiązujące w Urzędzie Polityki zarówno przed rozpoczęciem świadczenia pracy zdalnej, jak i w czasie jej wykonywania określały zasady dotyczące korzystania z Internetu, przesyłania informacji oraz wynoszenia poza siedzibę jednostki aktywów (tj. sprzętu komputerowego, nośników, oryginałów dokumentów i ich kopii). Zawierały także procedury postępowania w sytuacjach szczególnych (awarie sprzętu lub oprogramowania lub ich utrata), a także metody zabezpieczenia przekazywanych informacji. Procedury zawarte w Politykach nie dopuszczały bez zgody administratora do korzystania z prywatnego sprzętu elektronicznego

[22] Data złożenia pierwszego indywidualnego wniosku o pracę zdalną w okresie objętym kontrolą.
[23] Data złożenia ostatniego indywidualnego wniosku o pracę zdalną w okresie objętym kontrolą.
[24] Zarządzenie Nr K/8/20 Burmistrza w sprawie ustalenia regulaminu pracy zdalnej pracowników Urzędu, dalej: regulamin pracy zdalnej.

(np. laptopów, telefonów, nośników typu pendrive) do wykonywania zadań służbowych.

Inspektor do spraw obsługi informatycznej wyjaśnił, że w latach 2020-2021 pracownicy świadczący pracę zdalną nie występowali o zgodę na korzystanie z prywatnego sprzętu elektronicznego (np. laptopów, telefonów, nośników typu pendrive), ponieważ nie było takiej potrzeby. Na polecenie Burmistrza, w celu ograniczenia rozprzestrzeniania się pandemii COVID-19, wprowadzono w Urzędzie 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 i pendrive'y.

Zgodnie z określonymi w Politykach zasadami użytkownik zobowiązany był m.in. do:

- przechowywania danych na dysku szyfrowanym zabezpieczonym hasłem,
- transportu nośnika w sposób minimalizujący ryzyko kradzieży lub zniszczenia oraz stosownego zabezpieczenia nośnika przed uszkodzeniem,
- zdecydowanego i skutecznego uniemożliwienia skorzystania z nośnika osobom nieuprawnionym (np. rodzina, dzieci, znajomi),
- korzystania ze sprzętu elektronicznego w sposób zgodny z jego przeznaczeniem i jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem,
- używania wyłącznie oprogramowania przekazanego lub udostępnionego przez administratora,
- podłączania do systemu informatycznego wyłącznie urządzeń zatwierdzonych przez administratora.

W Politykach tych określono także zasady wycofania sprzętu elektronicznego z użycia oraz zabezpieczenia dokumentów papierowych zawierających dane osobowe przed dostępem do nich osób trzecich.

Szczegółowe zasady dotyczące pracy z urządzeniami mobilnymi określono w Polityce obowiązującej od 15 lutego 2021 r., w której m.in.:

- dopuszczono możliwość wykonywania pracy zdalnej wyłącznie z urządzeń mobilnych (laptopów) będących własnością administratora i łączenia się z siecią administratora za pośrednictwem kanałów wirtualnej sieci prywatnej (VPN)[25].
- zabroniono wykorzystywania służbowych urządzeń mobilnych do celów prywatnych oraz udostępniania ich osobom trzecim, jak również instalowania aplikacji, które nie są niezbędne do wykonywania obowiązków danego pracownika,
- zabroniono korzystania z publicznych sieci WiFi oraz pozostawiania urządzenia bez nadzoru pracownika, w szczególności w miejscach ogólnodostępnych dla osób trzecich,
- zakazano pożyczania sprzętu osobie trzeciej oraz pozostawienie urządzenia bez opieki.

(akta kontroli str. 8-148, 408-414,480-520)

1.5. W okresie świadczenia pracy zdalnej przez pracowników Urzędu obowiązywały w Urzędzie zasady przesyłania informacji, które określono w regulaminie pracy zdalnej oraz obowiązujących w Urzędzie Politykach.

W regulaminie pracy zdalnej zobowiązano pracowników m.in. do:

[25] Dalej: VPN.

– poinformowania pracodawcy o rozpoczęciu i zakończeniu pracy w trybie zdalnym w danym dniu poprzez wysyłanie wiadomości email lub smsa do swojego bezpośredniego przełożonego,
– bieżącego sprawdzania korespondencji elektronicznej i pozostawania w dostępności za pomocą telefonu służbowego lub innego uzgodnionego z pracodawcą środka komunikacji na odległość.

W Politykach Urzędu zobowiązano pracowników m.in. do:
– korzystania z przyznanego adresu mailowego wyłącznie w celu prowadzenia korespondencji służbowej,
– stosowania zabezpieczeń kryptograficznych polegających m.in. na przesłaniu plików w formie załącznika opatrzonych hasłem, przy czym hasło powinno być przekazane adresatowi za pośrednictwem innego źródła,
– zachowania szczególnej ostrożności podczas odbierania poczty elektronicznej, w tym plików i linków w niej zawartych w przypadku braku pewności co do autentyczności adresata wiadomości,
– korzystania z metody „ukryte do wiadomości" w przypadku wysyłania maili do wielu adresatów jednocześnie.

Polityki zabraniały użytkownikom w szczególności rozsyłania maili do wielu adresatów z użyciem opcji „do wiadomości", używania służbowego adresu mailowego do celów prywatnych, w tym do rejestracji na portalach społecznościowych i dokonywania zakupów w sklepach internetowych.

W okresie objętym kontrolą w ramach pracy zdalnej w Urzędzie:
- Nie dopuszczono możliwości korzystania z prywatnych kont pocztowych do przesyłania służbowych informacji, bowiem zgodnie z Politykami pracownicy Urzędu zobowiązani byli do wyłącznego korzystania z przyznanego adresu mailowego w celu prowadzenia korespondencji służbowej. Jak wyjaśnił inspektor do spraw obsługi informatycznej wszyscy pracownicy Urzędu, w tym również pracownicy świadczący pracę zdalną posiadali dostęp do służbowej poczty elektronicznej bez względu na miejsce świadczenia pracy i sprzęt z którego korzystali, gdyż dostęp do służbowej poczty elektronicznej odbywał się z pośrednictwem strony www.
- Nie określono przypadków wymagających stosowania dodatkowych zabezpieczeń wiadomości przekazywanych w formie elektronicznej, bowiem zasady korzystania z poczty elektronicznej, jak i zasady korzystania z innych nośników określono w Politykach Urzędu. Jak wyjaśnił inspektor do spraw obsługi informatycznych zapisy w Polityce Urzędu obowiązującej w trakcie świadczenia pracy zdalnej przez pracowników Urzędu uznano za wystarczające. Podał także, że pracownicy świadczący pracę zdalną nie używali (poza komputerami i telefonami) innych urządzeń jako środka komunikacji na odległość i nie występowali też o wyrażenie zgody na ich używanie.

Obowiązek przestrzegania zasad określonych w obowiązującej Polityce zawarto w regulaminie pracy zdalnej.

(akta kontroli str. 8-148, 408-414)

1.6. Zasady zarządzania incydentami wprowadzono w Urzędzie Polityką Ochrony Danych Osobowych obowiązującą od 15 lutego 2021 r. Zasady te obejmowały w szczególności: obsługę incydentu uwzględniającą wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu, obowiązki użytkowników, obsługi informatycznej oraz administratora w tym zakresie.

Analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych przeprowadzone w lutym 2020 r. oraz w marcu 2021 r. uwzględniały szacowanie

prawdopodobieństwa wystąpienia incydentu, w tym wystąpienia zagrożeń wywołanych przez człowieka.

Dodatkowo w lutym 2021 r. Burmistrz wyznaczył w Urzędzie, na podstawie Zarządzenia[26], osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Zgodnie z tym Zarządzeniem, do zadań osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa należało w szczególności:

- zapewnienie zarządzania incydentem bezpieczeństwa komputerowego,
- zgłaszanie incydentów do CSIRT NASK[27],
- zapewnienie obsługi incydentu i incydentu krytycznego we współpracy z CSIRT NASK,
- zapewnienie osobom, na rzecz których zadanie publiczne było realizowane, dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na stronie internetowej,
- przekazywanie do CSIRT NASK danych osoby odpowiedzialnej za utrzymywanie kontaktów, a także informacji o zmianie tych danych,
- realizacja innych zadań określonych ustawą o krajowym systemie cyberbezpieczeństwa.

W maju, czerwcu oraz we wrześniu 2021 r. inspektor do spraw obsługi informatycznej, będący osobą odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu bezpieczeństwa uczestniczył w trzech konferencjach dotyczących cyberbezpieczeństwa, a w dniach od 31 maja do 27 czerwca 2021 r. uczestniczył w kursie pn. „Bezpieczeństwo w cyberprzestrzeni" prowadzonym przy udziale Wydziału Cybernetyki Wojskowej Akademii Technicznej w Warszawie. Jak wyjaśnił ww. inspektor, w trakcie wykonywanych zadań zapoznał się także z poradnikiem dotyczącym cyberbezpieczeństwa dostępnym na rządowej stronie internetowej www.gov.pl oraz na bieżąco śledził aktualności związane z bezpieczeństwem w sieci. Dodatkowo podał, że kontakty z podmiotami krajowego systemu cyberbezpieczeństwa obejmowały w szczególności: zgłoszenie osób kontaktowych (zgłoszenia osób do CSIRT NASK dokonano 2 marca 2021 r.), zgłoszenie incydentów oraz kontakty telefoniczne w celu zasięgnięcia opinii na temat incydentów i procedury ich zgłaszania. W okresie objętym kontrolą dokonano dwóch zgłoszeń incydentów, które nie dotyczyły pracy na odległość i mobilnego przetwarzania danych. Pierwszy dotyczący próby wymuszenia dokonania przelewu zgłoszono 14 maja 2021 r., zaś drugi 6 lipca 2021 r. (próba pobrania/otwarcia załącznika). Zgłoszenia incydentów dokonano w dniu ich wystąpienia za pośrednictwem strony internetowej www.incydent.cert.pl. Odnośnie zapewnienia osobom na rzecz których zadanie publiczne było realizowane dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, inspektor do spraw obsługi informatycznej podał, że na stronie internetowej Urzędu (www.olsztynek.pl) umieszczono link do bazy wiedzy z zakresu cyberbezpieczeństwa (www.gov.pl/web/bazawiedzy/cyberbezpieczeństwo) oraz na bieżąco w miarę potrzeb udzielał on pracownikom Urzędu instruktażu w tym zakresie.

(akta kontroli str. 8-148, 403-404, 415-428)

[26] Na podstawie Zarządzenia Nr K/11/21 w sprawie wyznaczenia osoby odpowiedzialnej z utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
[27] Computer Security Incident Response Team.

1.7. Regulamin pracy zdalnej[28], wprowadzono w Urzędzie 16 marca 2020 r. Określono w nim m.in.:

- tryb zastosowania pracy zdalnej uwzględniający m.in. świadczenie pracy zdalnej na czas oznaczony i podstawie polecenia wykonywania pracy zdalnej wydanego przez pracodawcę, z inicjatywy pracodawcy lub na wniosek pracownika, również w sytuacji zamknięcia szkoły, przedszkola lub żłobka dziecka pracownika,
- miejsce świadczenia pracy zdalnej, tj. miejsce zamieszkania pracownika, z zastrzeżeniem, że praca taka nie stanowiła podróży służbowej i nie uprawniała z tego tytułu do wypłacania diet,
- prawa i obowiązki pracodawcy i pracownika, w tym dotyczące awarii sprzętu służbowego oraz prawidłowego zabezpieczenia powierzonych danych i informacji,
- zasady wykonywania pracy zdalnej, w tym zasady dotyczące w szczególności: bezpieczeństwa pracy zdalnej w zakresie BHP, informowania pracodawcy o rozpoczęciu i zakończeniu pracy zdalnej, ewidencji czasu pracy pracowników świadczących pracę zdalną oraz korzystania z powierzonego mu sprzętu, danych i dokumentów.

Ww. regulamin zawierał trzy załączniki, tj.: polecenie wykonania pracy zdalnej obejmujące także zobowiązanie pracownika do stosowania poleceń przełożonych i procedur wprowadzonych przez pracodawcę, wniosek o umożliwienie pracy zdalnej, oświadczenie pracownika o zapoznaniu się z regulaminem i zobowiązanie się do jego przestrzegania.

Zasady wykonywania pracy zdalnej opisano w punkcie 2.2. wystąpienia pokontrolnego.

Dodatkowo od 6 listopada 2020 r. wprowadzono Zarządzeniem Burmistrza[29] okresową zmianę organizacji pracy w Urzędzie. Na podstawie ww. dokumentu zarządzono, że:

- pracowników Urzędu podzielono na dwie stałe grupy – bez możliwości zmiany składu osobowego pracujące w tygodniu – co drugi dzień rotacyjnie (naprzemiennie) – gdy pierwsza grupa pracowników pracuje w Urzędzie, druga świadczy pracę zdalną[30],
- w każdym tygodniu w siedzibie Urzędu pracowała grupa pracowników obejmująca połowę składu osób pracujących w jednym pokoju biurowym, tak aby w danym dniu w pomieszczeniu biurowym świadczyła pracę jedna osoba,
- pracownik świadczący pracę zdalną zobowiązany był do stosowania zasad określonych w regulaminie pracy zdalnej,
- pracownicy zobowiązani byli do wykonywania pracy w sposób zgodny z przepisami i zasadami BHP.

(akta kontroli str. 408-414, 429-436)

1.8. W okresie objętym kontrolą pracownicy Urzędu uczestniczyli w dwóch szkoleniach z zakresu ochrony danych osobowych zorganizowanych przez IOD. W szkoleniu przeprowadzonym w:

- 2020 r. uczestniczyło 41 pracowników Urzędu. Tematyka tego szkolenia dotyczyła w szczególności zasad i sposobów przetwarzania danych osobowych,

[28] Zarządzenie Nr K/8/20 Burmistrza w sprawie ustalenia regulaminu pracy zdalnej pracowników Urzędu, dalej: regulamin pracy zdalnej.
[29] Zarządzenie Nr K/50/20 z dnia 5 listopada 2020 r. w sprawie okresowej zmiany organizacji pracy Urzędu, dalej: Zarządzenie w sprawie okresowej zmiany organizacji pracy Urzędu.
[30] Z podziału na grupy wyłączono: Burmistrza i jego Zastępcę, Skarbnika i Sekretarza Miasta oraz radcę prawnego i straż miejską.

ich naruszeń i zagrożeń związanych z umyślnym i nieumyślnym naruszeniem danych osobowych, a także stosowanych środków technicznych i organizacyjnych do ochrony danych osobowych, jak również sposobów ochrony urządzeń (telefonów i komputerów) przed utratą danych.

– 2021 r., którego zakres obejmował: spełnienie obowiązku informacyjnego, rejestrowanie czynności przetwarzania oraz powierzanie i udostępnianie danych osobowych - uczestniczyło 42 pracowników Urzędu.

Oba szkolenia swoim zakresem nie obejmowały wprost zagadnień dotyczących zdalnego/mobilnego przetwarzania danych. Szkolenia i instruktaże dotyczące cybebezpieczeństwa opisano w punkcie 1.6 wystąpienia pokontrolnego.

Jak wyjaśnił Inspektor do spraw obsługi informatycznej Urzędu, w latach 2020-2021 pracownicy Urzędu byli systematycznie informowani o zagrożeniach bezpieczeństwa informacji w odniesieniu do zdalnego przetwarzania danych. Odbywało się to m.in. przez udzielanie instruktażu każdorazowo przed wydaniem pracownikom laptopów, pendrive'ów i dysków sieciowych, podczas którego informowano o zasadach wykorzystania sprzętu, zagrożeniach i sposobach minimalizacji ryzyka.

(akta kontroli str. 437-444, 415-425)

1.9. W okresie objętym kontrolą w Urzędzie dokonywano przeglądu Polityki Ochrony Danych[31]. Efektem przeglądów, poprzedzonych przeprowadzeniem analizy ryzyka udokumentowanych raportami było wprowadzenie w styczniu 2021 r. zaktualizowanej Polityki Ochrony Danych Osobowych, w której wprowadzono m.in. zasady pracy zdalnej z wykorzystaniem służbowego i prywatnego sprzętu do zadań służbowych oraz pracy z dokumentacją papierową, a także zapisy dotyczące zarządzania incydentem oraz pracy z urządzeniami mobilnymi[32].

Corocznie przeprowadzano także audyty stanu bezpieczeństwa informacji, które zawierały ustalenia i rekomendacje dotyczące pracy zdalnej. Ustalenia dotyczyły w szczególności niewystarczającego zabezpieczenia urządzeń mobilnych (tj. laptopów wynoszonych z Urzędu), a rekomendacje obejmowały zastosowanie m.in. szyfrowania przestrzeni dyskowej.

W marcu 2020 r., w związku z pandemią wirusa SARS-CoV-2 wprowadzono regulamin pracy zdalnej, a w listopadzie 2020 r. okresową zmianę organizacji pracy Urzędu. Szacowanie ryzyka na potrzeby audytu wewnętrznego i kontroli zarządczej na 2021 r. uwzględniało zagrożenia wynikające z pandemii COVID-19 i ewentualną w związku z tym konieczność zmiany organizacji pracy Urzędu.

W kwietniu 2021 r. Wojewoda Warmińsko-Mazurski[33] przeprowadził w Urzędzie kontrolę w trybie zdalnym w zakresie oceny działania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego[34] do realizacji zadań zleconych z zakresu administracji rządowej. Kontrolą objęto okres od 1 stycznia 2019 r. do 31 grudnia 2020 r. W wyniku kontroli skierowano do Burmistrza 12 kwietnia 2021 r. wystąpienia pokontrolne zawierające trzy ustalenia niezwiązane z typowymi ryzykami występującymi w pracy zdalnej. W odpowiedzi na otrzymane wystąpienie pokontrolne, 15 kwietnia 2021 r. Burmistrz poinformował Wojewodę o rozpoczęciu prac nad wykonaniem zaleceń pokontrolnych.

(akta kontroli str. 8-148, 150-230, 242-298, 445-475)

---

[31] W dokumencie tym, w sierpniu 2020 r. zmieniono załącznik dotyczący umowy powierzenia danych osobowych do przetwarzania.

[32] W dokumencie tym, w maju 2021 r. wprowadzono zasady tworzenia i wykonywania kopii bezpieczeństwa.

[33] Dalej: Wojewoda.

[34] Dalej: jst.

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

W Urzędzie do dnia zakończenia kontroli, tj. do 16 listopada 2021 r. nie opracowano, nie ustanowiono i nie wdrożono systemu zarządzania bezpieczeństwem informacji (w tym polityki bezpieczeństwa informacji), spełniającego wymogi określone przepisami § 20 ust. 2 rozporządzenia KRI, do czego zobowiązywał § 20 ust. 1 ww. rozporządzenia.
Zgodnie z ww. przepisem, jednostki realizujące zadania publiczne mają obowiązek opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia SZBI zapewniającego poufność, dostępność i integralność informacji, z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Wymagania dotyczące opracowania SZBI uznaje się za spełnione, jeżeli został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 (§ 20 ust. 3 ww. rozporządzenia), a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń; PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem; PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

W Urzędzie brak było systemowego podejścia dla zapewnienia bezpieczeństwa informacji, o którym mowa w § 20 ust. 1 rozporządzenia KRI, gdyż opracowane i wdrożone w Urzędzie regulacje dotyczyły głównie danych osobowych i nie obejmowały bezpieczeństwa innych informacji.

Burmistrz Urzędu w wyjaśnieniach 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.

(akta kontroli str. 4-298, 559-565)

OCENA CZĄSTKOWA

W okresie objętym kontrolą podejmowane w Urzędzie działania na rzecz bezpieczeństwa informacji w pracy na odległość i mobilnym przetwarzaniu danych nie uwzględniały wszystkich rodzajów przetwarzanych informacji. Regulacje wewnętrzne obowiązujące w Urzędzie dotyczyły przede wszystkim bezpieczeństwa przetwarzania danych osobowych. W tym zakresie przeprowadzano w szczególności: aktualizację obowiązujących procedur, powołano IOD i umożliwiono mu realizację zadań, stosowanie do art. 37 ust. 1 lit. a RODO oraz 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. W toku kontroli stwierdzono nieprawidłowość dotyczącą nieopracowania, nieustanowienia i niewdrożenia w Urzędzie systemu zarządzania bezpieczeństwem informacji.

OBSZAR

2. Wdrożone i stosowane organizacyjne i techniczne zapewniające bezpieczeństwo informacji w pracy zdalnej

Opis stanu faktycznego

2.1. Według stanu na koniec 2020 r. w Urzędzie zatrudnionych było 73 pracowników, 38 wykonywało pracę zdalną z inicjatywy pracodawcy, 12 pracowało na podstawie polecenia pracy zdalnej z wniosku pracownika, z tego w czasie kwarantanny – dwóch (żaden z pracowników nie przebywał na izolacji).

Według stanu na 22 września 2021 r. w Urzędzie: pracowało 76 pracowników, żaden pracownik nie wykonywał pracy zdalnej z inicjatywy pracodawcy, czterech pracowników pracowało na podstawie polecenia pracy zdalnej z wniosku pracownika, przy czym żaden z pracowników nie wykonywał pracy w czasie kwarantanny i w czasie izolacji.

Analiza wniosków do Burmistrza o umożliwienie wykonywania pracy zdalnej składanych przez pracowników Urzędu wykazała, że:

- 14 pracowników składało ww. wnioski tylko w trzech miesiącach 2020 r. (maj, październik i listopad) i trzech miesiącach 2021 r. (styczeń, marzec i kwiecień),
- wszystkie wnioski zostały zatwierdzone przez Burmistrza.
- pracownicy świadczyli pracę zdalną łącznie przez 107 dni, z czego: 12 pracowników przez 88 dni w 2020 r. oraz 4 przez 19 dni w 2021 r.,
- praca zdalna świadczona była od 2 do 12 dni w 2021 r. oraz od 2 do 6 dni w 2021 r.

Analiza poleceń wykonywania pracy zdalnej w Urzędzie wykazała, że wykonywanie pracy na polecenie pracodawcy poprzedzono wprowadzeniem Zarządzenia w sprawie okresowej zmiany organizacji pracy Urzędu. Praca zdalna wykonywana na podstawie polecenia pracy zdalnej z inicjatywy pracodawcy świadczona była tylko w listopadzie i grudniu 2020 r. I tak 38 pracowników, podzielonych na dwa stałe zespoły w każdym z siedmiu Referatów świadczyło pracę w przeważającej większości w systemie naprzemiennym, tj. jeden dzień pracy zdalnej, a następny dzień pracy na miejscu w Urzędzie. W tym systemie praca zdalna odbywała się bez wykorzystywania służbowego sprzętu teleinformatycznego. W regulaminie pracy zdalnej dopuszczono korzystanie z telefonów prywatnych i służbowych (do komunikacji głosowej i SMS) oraz prywatnych komputerów wyłącznie w celu sprawdzania korespondencji elektronicznej oraz wysyłania wiadomości e-mail o rozpoczęciu i zakończeniu pracy zdalnej. Podział zadań na zespoły w Referatach zatwierdzał Burmistrz.

(akta kontroli str. 476-520)

2.2. W badanym okresie obowiązujące w Urzędzie zasady wykonywania pracy zdalnej zawierały wymagania odnoszące się do zapewnienia bezpieczeństwa informacji. Dotyczyły one w szczególności przestrzegania wszelkich zasad obowiązujących u pracodawcy w zakresie korzystania z powierzonego sprzętu, danych i dokumentów, co szczegółowo opisano w punkcie 1.4. wystąpienia pokontrolnego. Wszyscy pracownicy Urzędu świadczący pracę zdalną zostali zapoznani z zasadami bezpiecznej pracy zdalnej.

Analiza oświadczeń dotyczących zapoznania się z treścią regulaminu pracy zdalnej, złożonych przez wszystkich 38 pracowników świadczących taką pracę wykazała, że:

- wszystkie podpisane oświadczenia znajdowały się w teczkach osobowych pracowników,
- wszystkie zostały podpisane przez pracowników przed rozpoczęciem świadczenia pracy zdalnej wykonywanej zarówno na wniosek pracownika, jak i z polecenia pracodawcy.

Dodatkowo wszyscy pracownicy świadczący pracę zdalną zapoznali się z również z Polityką Ochrony Danych z 2018 r. i jej aktualizacją z końca stycznia 2021 r.

(akta kontroli str. 299-304, 408-414, 526-528)

2.3. W latach 2020-2021 (według stanu na 22 września) zakres wykorzystania urządzeń teleinformatycznych wykorzystywanych w ramach pracy zdalnej w Urzędzie przedstawiał się następująco:

- W 2020 r. pięciu pracowników, w tym jeden dwukrotnie korzystało z udostępnionych przez pracodawcę czterech komputerów i czterech z telefonów. Natomiast 34 pracowników korzystało z prywatnych telefonów.
- W 2021 r. dwóch pracowników, w tym jeden dwukrotnie korzystało z udostępnionego przez pracodawcę jednego komputera. Czterech pracowników świadczących pracę zdalną korzystało z prywatnych telefonów tylko do komunikacji głosowej.
- W latach 2020-2021 wszyscy pracownicy świadczący pracę zdalną z wykorzystaniem służbowego sprzętu komputerowego posiadali pełen dostęp do systemów teleinformatycznych, który był realizowany za pośrednictwem kanałów wirtualnej sieci prywatnej (VPN)[35]. Na mechanizmy umożliwiające zapewnienie poziomu bezpieczeństwa systemów i oprogramowania oraz przetwarzania informacji za pośrednictwem ww. sprzętu składały się indywidualne konta i hasła do połączenia VPN oraz automatycznie aktualizowany program antywirusowy.

Warunki zdalnego dostępu do systemów informatycznych oraz zasady korzystania ze służbowego sprzętu i oprogramowania określono w regulaminie pracy zdalnej. Jak wyjaśnił inspektor do spraw obsługi informatycznej, udostępniane komputery wykorzystywane były przede wszystkim do pracy w elektronicznym systemie obiegu dokumentów[36], do kontroli zadań na stanowisku, a także do pracy w systemach służących do zarządzania budżetami w jst.

(akta kontroli str. 479, 528-540, 543-546)

2.4. W badanym okresie ustalono, że podczas świadczenia pracy zdalnej przez pracowników Urzędu z wykorzystaniem służbowych komputerów przenośnych nie skonfigurowano na nich indywidulanych kont użytkowników uprawniających do skorzystania z operacyjnego systemu informatycznego oraz, że dyski twarde tych komputerów nie były szyfrowane, co szczegółowo opisano w sekcji stwierdzone nieprawidłowości.

W Urzędzie, w celu zwiększenia poziomu bezpieczeństwa oraz zapewnienia ciągłości działania wprowadzono zasady wykonywania kopii bezpieczeństwa, którymi objęto serwery oraz bazy danych systemów dziedzinowych. Za sporządzenie ww. kopii odpowiedzialny był pracownik obsługi informatycznej, zaś użytkownicy we własnym zakresie odpowiadali za sporządzanie kopii zapasowych plików (m.in. dokumentów w formacie Microsoft Word) znajdujących się na lokalnych dyskach twardych.

(akta kontroli str. 71-146, 470-475, 535-542)

2.5. W okresie objętym kontrolą podczas świadczenia pracy zdalnej w Urzędzie dopuszczono wykorzystanie prywatnych telefonów i urządzeń komputerowych wyłącznie do wysyłania wiadomości e-mail lub SMS o rozpoczęciu i zakończeniu pracy zdalnej oraz bieżącego sprawdzania korespondencji elektronicznej, co uregulowano w regulaminie pracy zdalnej. Jak wyjaśnił inspektor do spraw obsługi informatycznej, nie określono warunków jakie powinien spełniać dopuszczony komputer prywatny, bowiem w celu wyłącznego sprawdzania poczty elektronicznej nie było to konieczne. Dodał także, że pracownik świadczący pracę zdalną zawsze mógł za pośrednictwem telefonu (prywatnego lub służbowego) poinformować pracodawcę zarówno o rozpoczęciu i zakończeniu pracy, jak i o niemożności wykonywania powierzonych mu zadań, w tym dotyczących bieżącego sprawdzania korespondencji elektronicznej.

[35] Dalej: VPN.
[36] Dalej: EZD.

Do inspektora do spraw obsługi informatycznej nie zgłaszano takich przypadków.

(akta kontroli str. 408-414, 480-513, 543-546)

2.6. W okresie objętym kontrolą pracownicy Urzędu nie wynosili z Urzędu oryginałów, kserokopii lub skanów dokumentów niezbędnych do wykonywania pracy. Kierownicy siedmiu Referatów, którzy zgodnie z regulaminem pracy zdalnej oraz Zarządzeniem w sprawie okresowej zmiany organizacji pracy Urzędu nadzorowali pracę zdalną świadczoną przez podległych im pracowników wyjaśnili, że nie wynoszono z Urzędu żadnych dokumentów w jakiejkolwiek formie, ponieważ nie było takiej potrzeby. Burmistrz wyjaśnił, że pracownicy Urzędu w czasie przebywania na pracy zdalnej uzgadniali z bezpośrednimi przełożonymi zadania niezbędne do wykonania z obszaru działalności całego Urzędu. Będąc do dyspozycji Kierowników Referatów i utrzymując z nimi kontakt telefoniczny udzielali również wyjaśnień, zarówno przełożonym, jak i interesantom w zakresie prowadzonych spraw. Dodatkowo pracownicy zostali zobowiązani do samokształcenia, przeglądania m.in. aktualnych przepisów prawnych i związanych z nimi rozstrzygnięć nadzorczych wojewodów oraz regionalnych izb obrachunkowych, uczestniczenia w szkoleniach on-line oraz brania udziału w sesjach Rady Miejskiej w Olsztynku i w posiedzeniach jej komisji organizowanych w formie teletransmisji. Praca zdalna świadczona w listopadzie i grudniu 2020 r. z inicjatywy pracodawcy odbywała się w systemie naprzemiennym, tj. jeden dzień w Urzędzie, drugi w miejscu zamieszkania, zaś pracownicy którzy świadczyli zdalną pracę na podstawie indywidulanego wniosku posiadali zapewniony stały dostęp do systemów informatycznych za pomocą służbowych komputerów. Każdy z Kierowników podał także, że informował pracowników o zasadach pracy zdalnej określonych w regulaminie pracy zdalnej, w tym o zasadach związanych z zapewnieniem bezpieczeństwa danych.

(akta kontroli str. 408-414, 429-436, 559-565, 559-565)

2.7. W badanym okresie Kierownicy Referatów monitorowali i nadzorowali pracę zdalną podległych im pracowników. Odbywało się to m.in. za pomocą służbowych i prywatnych telefonów, służbowych komputerów oraz służbowej korespondencji elektronicznej. Poprzez ww. środki komunikacji na odległość przełożeni wydawali polecenia swoim pracownikom i sprawdzali wykonanie zleconych im zadań, w tym dotyczących przekazania informacji o rozpoczęciu i zakończeniu pracy. Potwierdzenie wykonania pracy zdalnej odnotowywano na indywidualnych wnioskach pracowników wcześniej zatwierdzonych przez Burmistrza.

(akta kontroli str. 480-513, 547-558)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

W latach 2020-2021 (do 22 września) w czasie świadczenia pracy zdalnej przez pracowników Urzędu z wykorzystaniem trzech służbowych komputerów przenośnych (laptopów):

– nie skonfigurowano na tych komputerach indywidulanych kont użytkowników uprawniających do skorzystania z operacyjnego systemu informatycznego. Było to niezgodne z obowiązującymi w Urzędzie Politykami, bowiem w rozdziale 12.2 Polityki Ochrony Danych obowiązującej od 17 września 2018 r. do 14 lutego 2021 r. wskazano, że w przypadku dostępu do operacyjnych systemów informatycznych użytkownik powinien stosować co najmniej dwuetapową metodę uwierzytelnienia poprzez wpisanie indywidualnego identyfikatora/ login'u oraz hasła, zaś w rozdziale 21.1 Polityki Ochrony Danych Osobowych obowiązującej od 15 lutego 2021 r. zapisano, że w przypadku dostępu

użytkowników do operacyjnych systemów informatycznych należy stosować metodę uwierzytelnienia poprzez wpisanie indywidualnego identyfikatora/loginu oraz hasła,

– nie zabezpieczono ww. laptopów 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. Było to również niewypełnieniem wymagania A.11.2.6 Polskiej Normy EN ISO/IEC 27001:2017 dotyczącego bezpieczeństwa sprzętu i aktywów poza siedzibą.

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. Pracownicy wykorzystywali terminale do połączenia z systemem służącym do kontroli zadań zlecanych przez przełożonych bez konieczności zapisu plików na dysku, połączenia z pocztą e-mail za pomocą przeglądarki www, do pracy z plikami umieszczonymi na serwerze plikowym oraz do połączenia z innymi systemami dziedzinowymi. Jeżeli zaistniała konieczność przeglądu lub edycji jakiegoś załącznika z poczty e-mail bądź danego systemu pracownik zapisywał dany plik wyłącznie na zasobie sieciowym. Wymiana dokumentów między pracownikami odbywa się za pomocą udostępnionych zasobów serwera plikowego, więc nie było potrzeby przesyłania dokumentów służbowych za pośrednictwem poczty e-mail. 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 wystarczająca. 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, kontroli oprogramowania antywirusowego, przygotowania oprogramowania do zdalnego połączenia z siecią Urzędu (VPN). Te działania uniemożliwiały dostęp do jakichkolwiek danych innego pracownika. Zapisy w Polityce Ochrony Danych i w Polityce Ochrony Danych Osobowych zostały zatem zachowane dla dostępu: do VPN, zasobów sieciowych na serwerze plikowym, poczty e-mail oraz systemów dziedzinowych.

Zdaniem NIK zapisy Polityki Ochrony Danych oraz Polityki Ochrony Danych Osobowych w zakresie dostępu do operacyjnych systemów informatycznych dotyczą wszystkich użytkowników tych systemów, również użytkowników świadczących pracę zdalną. Nie określono w tym zakresie wyłączeń dotyczących pracy zdalnej. Należy również zauważyć, że aktywa wynoszone poza siedzibę Urzędu powinny być pod szczególną ochroną, zwłaszcza w aspekcie zabezpieczenia informacji przechowywanych na laptopach w przypadku ich ewentualnej utraty. Taka potrzeba została wskazana także w przeprowadzonych dwóch audytach bezpieczeństwa informacji, które potwierdziły brak stosowania zabezpieczeń urządzeń mobilnych i rekomendowały ich zabezpieczenie przed utratą informacji, poprzez m.in. zaszyfrowanie przestrzeni dyskowej.

(akta kontroli str. 214-227, 228-263)

OCENA CZĄSTKOWA

W okresie objętym kontrolą Urząd stosował i egzekwował zasady wprowadzone regulaminem pracy zdalnej oraz związane z czasową zmianą organizacji pracy. 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. Nadzorowano i monitorowano wykonywanie przez pracowników pracy zdalnej za pomocą służbowych i prywatnych telefonów, służbowych komputerów oraz służbowej korespondencji elektronicznej. Potwierdzenia wykonania pracy zdalnej dłużej niż jeden dzień odnotowywano na indywidualnych wnioskach.
Nie w pełni jednak zapewniono bezpieczeństwo informacji podczas świadczenia przez pracowników Urzędu pracy zdalnej z wykorzystaniem służbowych komputerów przenośnych (laptopy). Stwierdzono bowiem, że nie skonfigurowano na nich indywidulanych kont użytkowników uprawniających do korzystania z systemu operacyjnego i oraz nie zabezpieczono dysków twardych tych komputerów przed utratą poufności informacji w sytuacji utraty sprzętu.

IV. Uwagi i wnioski

Najwyższa Izba Kontroli w wyniku kontroli nie formułuje uwag. W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

Wnioski

1. Opracowanie i wdrożenie kompletnego systemu zarządzania bezpieczeństwem informacji uwzględniającego zalecenia Polskiej Normy PN-ISO/IOC 27001 i norm z nią związanych (PN-ISO/IOC 27002, 27005, 24762).
2. Konfigurowanie na służbowych komputerach przenośnych wykorzystywanych do świadczenia pracy zdalnej indywidulanych kont użytkowników uprawniających do korzystania z operacyjnego systemu informatycznego oraz zabezpieczanie ww. urządzeń przed utratą poufności informacji.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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

Obowiązek poinformowania NIK o sposobie wykonania wniosków

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

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

Olsztyn, 26 listopada 2021 r.

Kontroler

Lidia Wójcik
Starszy inspektor kontroli państwowej

.....
podpis

Najwyższa Izba Kontroli
Delegatura w Olsztynie
Dyrektor

z up.
Piotr Wanic
Wicedyrektor

.....
podpis