NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie

LOL.410.017.07.2021

Tadeusz Sobierajski
Burmistrz Morąga
Urząd Miejski w Morągu
ul. 11 Listopada 9
14-300 Morąg

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 Morągu, ul. 11 Listopada 9, 10-300 Morąg (dalej: Urząd lub Gmina).

Kierownik jednostki kontrolowanej

Tadeusz Sobierajski, Burmistrz Morąga od 23 października 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

Od 1 stycznia 2020 r. do dnia zakończenia kontroli, tj. 16 listopada 2021 r. 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

Anna Kamińska-Bisior, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LOL/118/2021 z 29 września 2021 r.

(akta kontroli str.1-2)

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

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.

Najwyższa Izba Kontroli negatywnie ocenia natomiast działania Burmistrza w zakresie organizacji bezpieczeństwa informacji w Urzędzie, bowiem nie opracował on, nie ustanowił, ani nie wdrożył systemu zarządzania bezpieczeństwem informacji[3], 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[4].

W okresie objętym kontrolą obowiązujące w Urzędzie regulacje wewnętrzne nie były poddawane udokumentowanym, regularnym przeglądom, a ostatnie aktualizacje posiadanych dokumentów w zakresie danych osobowych były wykonane w 2019 r.

[1] Dz. U. z 2017 r. poz. 524 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: SZBI.
[4] Dalej: norma ISO.

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.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[5] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1 Do 19 października 2021 r. Gmina nie opracowała, nie zatwierdziła i nie wdrożyła SZBI (opisano w punkcie 1 sekcji Stwierdzone nieprawidłowości).

(akta kontroli str. 3-5, 402-433, 466-469)

W Urzędzie posiadano zidentyfikowane informacje i inne aktywa z nimi związane oraz środki wykorzystywane do ich przetwarzania w odniesieniu do danych osobowych.

W tej sprawie Burmistrz wyjaśnił, że analiza i identyfikacja rodzajów informacji przetwarzanych w ramach Urzędu przeprowadzana była na bieżąco. Taka analiza odbywała się, w szczególności, w ramach rejestru czynności przetwarzania danych osobowych, którego ostatnia aktualizacja miała miejsce 22 października 2019 r. W elektronicznym rejestrze była, na bieżąco, przeprowadzana inwentaryzacja sprzętu i oprogramowania służącego do przetwarzania informacji. Dodatkowo informatyk Urzędu wraz z inspektorem ochrony danych osobowych[6] przeprowadzali cykliczne kontrole zabezpieczenia sprzętu komputerowego przed dostępem osób nieuprawnionych oraz legalności zainstalowanego oprogramowania. Sekretarz Gminy dodał, że Urząd był w posiadaniu protokołów z kontroli przeprowadzonych przez IOD i informatyka, ale poza danymi osobowymi, nie ma oddzielnego dokumentu w zakresie analizy i identyfikacji informacji, innych aktywów z nimi związanych oraz środków wykorzystywanych do ich przetwarzania.

(akta kontroli str. 27-59, 434-440, 466-469)

W Urzędzie opracowano i wprowadzono natomiast:

1) zasady przetwarzania i bezpieczeństwa danych osobowych[7] obejmujące:
   - politykę ochrony danych osobowych,
   - instrukcję określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
   - instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych,
2) instrukcję określającą sposób zarządzania systemem informatycznym w Urzędzie[8],
3) regulamin pracy zdalnej[9].

[5] 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.
[6] Dalej: IOD.
[7] Wprowadzone zarządzeniem nr 769/18 Burmistrza Morąga z dnia 22 maja 2018 r. w sprawie: wprowadzenia dokumentacji zasad i bezpieczeństwa danych osobowych w Urzędzie Miejskim w Morągu, dalej: zarządzenie w sprawie danych osobowych.
[8] Instrukcja podpisana przez Burmistrza 25 maja 2018 r.
[9] Wprowadzony zarządzeniem nr 385/20 Burmistrza Morąga z dnia 20 października 2020 r. w sprawie: nadania regulaminu pracy zdalnej w Urzędzie Miejskim w Morągu, dalej: zarządzenie w sprawie pracy zdalnej.

W Urzędzie prowadzono także rejestr czynności przetwarzania danych osobowych[10] oraz analizę ryzyka związanego z przetwarzaniem danych osobowych[11].

Opracowane w Urzędzie regulacje w zakresie bezpieczeństwa informacji dotyczyły danych osobowych. Burmistrz wyjaśnił, iż zdecydowana większość informacji przetwarzanych w Urzędzie to dane osobowe. Nawet informacje, które nie odnosiły się bezpośrednio do tych danych były danymi zintegrowanymi z danymi osobowymi i podlegały regulacjom określonym w zarządzeniu w sprawie danych osobowych. Sekretarz Gminy wyjaśnił, iż prawdopodobnie wynikało to z faktu, że pracownicy Urzędu traktowali dane osobowe jako dominujące informacje przetwarzane w Urzędzie i takie zapisy wprowadzono m.in. w instrukcji zarządzania systemem informatycznym. Jednak zamysłem było objęcie instrukcją wszystkich danych i informacji przetwarzanych w Urzędzie.

(akta kontroli str. 8-59, 69-83, 402-433, 466-469)

W okresie objętym kontrolą[12] z zarządzeniem w sprawie danych osobowych zostało zapoznanych 9 osób. Fakt ten nie został potwierdzony pisemnie przez pracowników Urzędu. Natomiast zaświadczenia potwierdzające zapoznanie pracowników z obowiązkami związanymi z ochroną danych osobowych wydane zostały przez IOD.

Z instrukcją określającą sposób zarządzania systemem informatycznym zapoznało się 25 maja 2018 r. 52 pracowników Urzędu, a z zarządzeniem w sprawie pracy zdalnej 54 pracowników Urzędu, którzy potwierdzili ten fakt stosownym podpisem.

(akta kontroli str. 60-68, 73-83)

W ww. dokumentach określono zasady postępowania z nośnikami, zarządzania uprawnieniami użytkowników, wynoszenia aktywów, bezpieczeństwa sprzętu i aktywów poza siedzibą, pozostawiania sprzętu bez opieki, zabezpieczenia przed szkodliwym oprogramowaniem, zabezpieczenia sieci, przesyłania informacji, zabezpieczenia wiadomości w formie elektronicznej oraz zarządzania incydentami związanymi z bezpieczeństwem informacji.

(akta kontroli str. 6-7, 69-83)

1.2 Zarządzeniem w sprawie danych osobowych Burmistrz określił odpowiedzialność i uprawnienia osób pełniących istotną rolę w zapewnieniu bezpieczeństwa informacji w zakresie danych osobowych.

Za wdrażanie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych odbywało się zgodnie z prawem, odpowiedzialny był Burmistrz, jako administrator danych osobowych.

Inspektor ochrony danych[13] był z kolei odpowiedzialny za monitorowanie realizacji wprowadzonych zasad i procedur zabezpieczenia danych (zabezpieczenia organizacyjne), w tym za:

- monitorowane bezpieczeństwa danych,
- bieżącą kontrolę pracy systemu informatycznego,
- przeprowadzanie kontroli wyrywkowych stanu bezpieczeństwa systemów informatycznych i przestrzegania zasad ochrony informacji,
- podejmowanie działań w przypadku naruszenia danych osobowych,

[10] Ostatnia aktualizacja z 22 października 2019 r.
[11] Ostatnia aktualizacja z 5 listopada 2019 r.
[12] Do 20 października 2021 r.
[13] W dokumentach dotyczących bezpieczeństwa informacji Urząd stosował zamiennie nazwy Inspektor Ochrony Danych oraz Inspektor Ochrony Danych Osobowych. W rzeczywistości była to ta sama osoba i funkcja, dalej: IOD.

- okresową analizę zagrożeń i ryzyka w celu weryfikacji środków zabezpieczających oraz inwentaryzację systemów informatycznych i zbiorów danych w celu zapewnienia aktualności polityki bezpieczeństwa.

Zakres czynności IOD w Urzędzie określony był także zarządzeniem Burmistrza[14] i obejmował realizację zadań określonych w art. 39 rozporządzenia Parlamentu Europejskiego i Rady (WE) 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[15] oraz dodatkowo:

- przygotowywanie upoważnień i prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
- prowadzenie rejestru czynności przetwarzania danych osobowych,
- uzgadnianie zapisów umów związanych z przetwarzaniem danych osobowych,
- nadzór nad obiegiem wniosków o udostępnienie danych osobowych w Urzędzie,
- nadzorowanie obowiązków wynikających z zapisów dokumentacji i procedur w sprawie ochrony danych osobowych obowiązujących w Urzędzie.

Z kolei do zadań administratora sieci (informatyka Urzędu) określonych w zarządzeniu Burmistrza w sprawie danych osobowych należało m.in.:

- bieżące kontrolowanie pracy systemu informatycznego,
- formułowanie sposobu określania uprawnień w systemach informatycznych,
- realizacja decyzji administratora danych osobowych dotyczących nadania osobom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania w środowisku IT Urzędu, tj. zarządzanie kontami i hasłami oraz dostarczenie inspektorowi ochrony danych informacji potrzebnych do oceny prawidłowości funkcjonowania sprzętowo-programowych,
- zadania związane z tworzeniem kopii bezpieczeństwa systemów i danych,
- automatyzacja zadań konserwacyjnych w systemie,
- monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników,
- monitorowanie legalności wykorzystywanego oprogramowania,
- zapewnienie serwerom i stacjom roboczym licencji programowanych,
- aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego,
- prowadzenie szkoleń na temat bezpiecznych zachowań użytkowników w środowisku systemów IT,
- informowanie IOD o wszelkich anomaliach w administrowanych urządzeniach, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

W zarządzeniu w sprawie danych osobowych określono także, że każdy pracownik Urzędu był osobiście odpowiedzialny za bezpieczeństwo powierzonych danych osobowych w trakcie ich przetwarzania.

W zakresach czynności pracowników pełniących istotną rolę w zapewnieniu bezpieczeństwa informacji w Urzędzie, tj. IOD i administratora sieci, nie uwzględniono zadań określonych w normie ISO, tj. związanych z zapewnieniem zgodności SZBI z wymaganiami ww. normy oraz z przedstawianiem najwyższemu

[14] Zarządzenie nr 768/18 Burmistrza Morąga z dnia 22 maja 2018 r. w sprawie: wyznaczenia Inspektora Ochrony Danych Osobowych w Urzędzie Miejskim w Morągu.
[15] Dz.U.UE poz. 119.1 z późn. zm., dalej: rozporządzenie RODO.

kierownictwu wyników działania SZBI[16]. W tej sprawie Burmistrz wyjaśnił, że ww. osoby posiadają zakomunikowaną odpowiedzialność i uprawnienia w zakresie zgodnym z wykonywanym rodzajem pracy i realizowanymi zadaniami. Sekretarz dodała natomiast, że osoby te posiadały świadomość o konieczności zapewnienia bezpieczeństwa informacji i realizowały działania w tym zakresie.

(akta kontroli str. 8-26, 84-87, 402-433, 466-469)

1.3 Zarządzeniem Burmistrza z 22 maja 2018 r.[17] w Urzędzie został wyznaczony inspektor ochrony danych osobowych. Obowiązki te były wykonywane przez osobę, która równocześnie była zatrudniona w Urzędzie na stanowisku inspektora ds. Rady Miejskiej w Wydziale Organizacyjnym i Spraw Obywatelskich.

Osoba wyznaczona na stanowisko IOD spełniała wymagania określone w art. 37 ust. 5 rozporządzenia RODO, a zakres jej obowiązków, określony ww. zarządzeniem Burmistrza, obejmował realizację zadań określonych w art. 39 rozporządzenia RODO.

Do 20 października 2021 r. w regulaminie organizacyjnym[18] Urzędu nie uwzględniono stanowiska IOD (opisano w punkcie 2 sekcji Stwierdzone nieprawidłowości).

(akta kontroli str. 86, 88-117, 402-433)

1.4 W zarządzeniu w sprawie danych osobowych oraz w instrukcji określającej sposób zarządzania systemem informatycznym w Urzędzie określone zostały zasady postępowania z nośnikami, tj. komputerami przenośnymi, wydrukami i dokumentami papierowymi zawierającymi dane osobowe, a także z zewnętrznymi nośnikami informacji, jednak nie uwzględniały one czynności i ryzyk związanych z pracą zdalną.

(akta kontroli str. 8-26, 75-83)

W zarządzeniu w sprawie pracy zdalnej dopuszczono możliwość wykonywania pracy z wykorzystaniem urządzeń służbowych oraz własnych pracowników. Określono także zasady postępowania z komputerem stacjonarnym, laptopem, smartfonem, tabletem oraz dokumentacją, uniemożliwiające nieuprawnione ujawnienie, modyfikację, usunięcie lub zniszczenie informacji zapisanych na nośnikach. W przypadku sprzętu komputerowego polegały one na zapewnieniu, aby domownicy nie mieli wglądu w wykonywaną pracę oraz na blokowaniu urządzenia na czas niekorzystania. Natomiast w odniesieniu do dokumentów zobligowano pracowników do organizacji pracy w sposób uniemożliwiający wgląd do nich osobom nieuprawnionym, zakazano zabierania dokumentów papierowych i ich kopii poza siedzibę Urzędu (dopuszczając jednocześnie możliwość pobrania tych dokumentów na podstawie pisemnej zgody przełożonego), dopuszczono elektroniczne kopiowanie dokumentów, nakazano zachowanie ostrożności podczas przewozu dokumentów i zwrot pobranych dokumentów przełożonemu po zakończeniu pracy.

(akta kontroli str. 69-72, 118-120)

Według wyjaśnień Burmistrza, w Urzędzie do 2 listopada 2021 r. nie prowadzono rejestru nośników służących do przechowywania informacji z przypisaniem odpowiedzialności za dany nośnik.

Urząd nie posiadał także udokumentowanego schematu klasyfikacji przetwarzanych w nim informacji. Według wyjaśnień Burmistrza schemat klasyfikacji informacji

[16] Tj. zadań określonych w punkcie 5.3 normy ISO.

[17] Zarządzenie nr 768/18 Burmistrza Morąga z dnia 22 maja 2018 r. w sprawie: wyznaczenia Inspektora Ochrony Danych Osobowych w Urzędzie Miejskim w Morągu.

[18] Wprowadzonym zarządzenie nr 737/18 Burmistrza Morąga z dnia 15 marca 2018 r. w sprawie nadania regulaminu organizacyjnego Urzędu Miejskiego w Morągu.

w Urzędzie oparty był na zasadzie wagi zawartych w nich danych. Wyodrębniono i oddzielnie zabezpieczono według wagi: informacje niejawne, informacje zawierające dane osobowe, pozostałe informacje. Sekretarz Gminy dodała, że ww. schemat nie został stworzony w sposób formalny.

(akta kontroli str. 441-456, 466-469)

1.5 Do 20 października 2020 r. w Urzędzie obowiązywał zakaz wynoszenia i korzystania z komputerów przenośnych zawierających dane osobowe poza jego budynkiem wprowadzony zarządzeniem w sprawie danych osobowych.

(akta kontroli str. 8-26, 120-121)

Zarządzeniem w sprawie pracy zdalnej Burmistrz umożliwił natomiast pracownikom korzystanie ze służbowego sprzętu poza siedzibą Urzędu i zabranie komputera służbowego do miejsca i na czas wykonywania pracy zdalnej. Wprowadził także ogólny zakaz zabierania, poza siedzibę Urzędu, dokumentów papierowych lub ich kopii z pozostawieniem możliwości wynoszenia dokumentów do domu na czas wykonywania pracy zdalnej, pod warunkiem uzyskania pisemnej zgody bezpośredniego przełożonego.

W zarządzeniu w sprawie pracy zdalnej określono także podstawowe warunki niezbędne do zapewnienia bezpieczeństwa sprzętu komputerowego i dokumentów papierowych poza siedzibą jednostki. Pracownik musiał zapewnić właściwe warunki umożliwiające pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji, zakazano wykonywania pracy w miejscach publicznych. Dopuszczono możliwość pracy z wykorzystaniem urządzeń służbowych i prywatnych. Określono także sposoby korzystania z Internetu, zobowiązano pracowników do wykonywania pracy na sprzęcie, który posiadał aktywny i zaktualizowany program antywirusowy oraz z wykorzystaniem, w miarę możliwości, służbowych programów i systemów udostępnionych przez Urząd i zabezpieczonych hasłem dostępu.

W Urzędzie praca zdalna wykonywana była od 16 marca 2020 r., natomiast zasady regulujące jej wykonywanie wdrożono 20 października 2020 r.

(akta kontroli str. 69-72, 120-121, 214, 216-280, 434-440)

Zgodnie z wyjaśnieniami Burmistrza, w Urzędzie zidentyfikowano ryzyka związane z wprowadzeniem w Urzędzie możliwości pracy zdalnej, a sposoby zabezpieczenia przed zdarzeniami wynikającymi ze zmaterializowania się ryzyka związanych z wynoszeniem aktywów zostały szczegółowo opisane w zarządzeniu w sprawie pracy zdalnej. Sekretarz dodała, że analiza ryzyka została przeprowadzona w momencie opracowywania ww. zarządzenia w sprawie pracy zdalnej, jednak nie została ona sformalizowana.

(akta kontroli str. 434-440, 466-469)

1.6 Według wyjaśnień Sekretarza Gminy, w Urzędzie nie wdrożono formalnych polityk przesyłania informacji, a także procedur zabezpieczenia informacji przesyłanych z użyciem wszystkich środków łączności.

(akta kontroli str. 466-469)

W zarządzeniu w sprawie danych osobowych oraz instrukcji określającej sposób zarządzania systemem informatycznym w Urzędzie uwzględniono natomiast zapis, iż pracownicy Urzędu nie mieli prawa przekazywać, za pośrednictwem sieci komputerowej, do stron trzecich, jakichkolwiek danych stanowiących własność Gminy. Według wyjaśnień Burmistrza, ww. zapis nie dopuszczał możliwości korzystania z prywatnych kont pocztowych do przesyłania informacji służbowych.

(akta kontroli str. 8-26, 75-83, 441-456)

W związku z wprowadzeniem w Urzędzie pracy zdalnej dopuszczono natomiast możliwość zdalnego dostępu do jego systemów informatycznych. W zarządzeniu w sprawie pracy zdalnej określono, że jeżeli było to możliwe, pracownik powinien był wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione przez Urząd i zabezpieczone hasłem dostępu. Dodatkowo określono, że zabezpieczeniu powinny były podlegać wszelkiego rodzaju dane osobowe, a hasło powinno było być skomplikowane i niesłownikowe. Każda wiadomość miała być wysyłana z należytą starannością, a w przypadku przekazywania informacji do kilku odbiorców, którzy nie znali się wzajemnie i/lub ich adresy e-mail były adresami prywatnymi, należało skorzystać z opcji tzw. „ukrytej kopii".

Zarządzeniem tym umożliwiono także wykonywanie pracownikom pracy zdalnej z wykorzystaniem urządzeń własnych, w związku z czym zezwolono na obsługę służbowej poczty elektronicznej z urządzeń innych niż służbowe pod warunkiem posiadania aktywnego i zaktualizowanego programu antywirusowego. Zgodnie z wyjaśnieniami Burmistrza w Urzędzie nie obowiązywał elektroniczny system obiegu dokumentów, a dostęp do systemów informatycznych Urzędu był zapewniony pracownikom wykorzystującym do pracy zdalnej zarówno służbowe, jak i prywatne urządzenia, przy wykorzystaniu bezpiecznego połączenia VPN i pulpitu zdalnego.

(akta kontroli str. 69-72, 434-456)

1.7 W okresie objętym kontrolą w Urzędzie obowiązywała instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych stanowiąca załącznik do zarządzenia w sprawie danych osobowych. Określono w niej odpowiedzialności i procedury zapewniające szybką, skuteczną i zorganizowaną reakcję na incydenty związane z bezpieczeństwem danych osobowych.

Ww. instrukcja zawierała definicję naruszenia danych osobowych oraz katalog zdarzeń, których może ono dotyczyć, tj. nieuprawnione ujawnienie danych, udostępnienie lub umożliwienie dostępu do danych osobom nieupoważnionym, zabranie danych przez osobę nieupoważnioną, uszkodzenie elementu systemu informatycznego, nieautoryzowany dostęp do danych, nieautoryzowane modyfikacje lub zniszczenie danych, udostępnienie danych nieautoryzowanym podmiotom, nielegalne ujawnienie danych, pozyskiwanie danych z nielegalnych źródeł.

Zgodnie z zapisami ww. instrukcji, IOD dokumentował przypadki naruszenia bezpieczeństwa danych osobowych, sporządzając raport oraz rejestr incydentów i działań korygujących i zapobiegawczych.

Według wyjaśnień Burmistrza, regulacje związane z bezpieczeństwem pozostałych informacji określone były w zarządzeniu w sprawie pracy zdalnej, a do 27 października 2021 r. w Urzędzie nie wystąpiły przypadki incydentów związanych z bezpieczeństwem informacji.

(akta kontroli str. 8-26, 434-456, 466-469)

1.8 Do 19 października 2020 r. w Urzędzie nie opracowano i nie wdrożono regulacji związanych w wykonywaniem pracy zdalnej. Regulamin pracy zdalnej wprowadzono[19] w Urzędzie 221 dni po rozpoczęciu wykonywania pracy zdalnej[20]. W okresie tym pracę w takiej formie świadczyło 68 pracowników Urzędu.

Według wyjaśnień Burmistrza, od 14 marca 2020 r. w Urzędzie wprowadzono naprzemienny system pracy, który miał na celu ograniczenie możliwości transmisji koronawirusa. Pracownicy wykonywali pracę naprzemiennie w grupach, które się nie spotykały, a były w stanie wykonać zadania urzędowe w przypadku wystąpienia zakażenia wirusem COVID-19 u osób w drugiej grupie. Pierwszy okres rotacyjnego

[19] Tj. 20 października 2020 r.
[20] Tj. od 16 marca 2020 r.

systemu pracy, bez wykorzystania systemu informatycznego Urzędu, obowiązywał do 1 czerwca 2020 r.

W tej sprawi Burmistrz wyjaśnił także, że epidemia była zaskoczeniem, które wymusiło podjęcie natychmiastowych działań zapewniających bezpieczeństwo pracowników i interesantów, a także niezakłócone funkcjonowanie Urzędu. W związku z tym w marcu 2020 r. Burmistrz wydał w formie ustnej polecenia wprowadzenia pracy rotacyjnej. Wynikało to z nagłej, nieprzewidywanej sytuacji i oczekiwanej krótkotrwałej konieczności izolowania pracowników. Praca była świadczona bez wykorzystania systemów informatycznych, ponieważ zarówno systemy, jak i sprzęt Urzędu nie były przygotowane do pracy zdalnej w tym okresie.

(akta kontroli str. 69-74, 402-433, 441-456)

We wprowadzonym 20 października 2020 r. regulaminie pracy zdalnej określono warunki, jakie musiało spełniać miejsce jej świadczenia oraz zasady dotyczące bezpieczeństwa informacji obejmujące: korzystanie z Internetu i urządzeń służących do pracy zdalnej, sposób postępowania z dokumentami w formie papierowej, procedury postępowania w szczególnych sytuacjach, a także metody zabezpieczania przekazywanych informacji (tylko w zakresie danych osobowych).

W regulaminie nie ustanowiono natomiast warunków podjęcia pracy zdalnej i podstawowych zasad dotyczących jej bezpieczeństwa w zakresie BHP. Określono jedynie, że jej warunki i zasady, w tym zakres i harmonogram był określany w Urzędzie.

(akta kontroli str. 69-72, 122)

W poleceniach Burmistrza dotyczących organizacji pracy Urzędu[21] polecono pracownikom wykonywanie pracy zdalnej, która miała być realizowana zgodnie z harmonogramem przekazanym do kadr Urzędu, a zakres pracy zdalnej ustalany był i nadzorowany przez bezpośrednich przełożonych.

(akta kontroli str. 123-139)

Harmonogramy pracy zdalnej zostały w Urzędzie opracowane na okres od 22 października 2020 r. do 2 listopada 2020 r. Poleceniem Burmistrza w sprawie organizacji pracy Urzędu[22], od 3 listopada 2020 r. pracownicy wykonywali pracę zdalną rotacyjnie, zgodnie z ustalonym harmonogramem przekazanym do kadr Urzędu. W dokumentacji nie stwierdzono harmonogramu pracy obowiązującego od 3 listopada 2020 r. W tej sprawie Burmistrz wyjaśnił, że w Urzędzie przyjęto procedurę pisemnych lub ustnych harmonogramów przekazywanych do kadr.

(akta kontroli str. 140-145, 434-440)

Ponadto, od 16 marca 2020 r. do 21 października 2021 r. w Urzędzie wydano dodatkowo 39 indywidualnych poleceń lub zgód na wykonywanie pracy zdalnej. Według wyjaśnień Burmistrza były one wydawane w zależności od pojawiającej się indywidualnej sytuacji pracownika lub organizacji pracy Urzędu, a powodem były nakładane izolacje, kwarantanny na pracowników lub członków ich rodzin i inne szczególne sytuacje występujące o okresie epidemii.

Jedno[23] z indywidualnie wydanych poleceń zawierało informacje o konieczności zachowania podstawowych warunków bezpieczeństwa i higieny pracy. Według wyjaśnień Sekretarza Gminy zapisy dotyczące BHP zostały pominięte przez nieuwagę.

(akta kontroli str. 146-198, 441-469)

[21] Tj. polecenia Burmistrza nr 4/2020, 6/2020, 7/2020, 8/2020, 9/2021, 10/2021, 11/2021, 12/2021, 13/2021, 14/2021, 15/2021, 16/2021, 17/2021, 19/2021, 20/2021, 21/2021.
[22] Polecenie nr 6/2020 Burmistrza Morąga z dnia 3 listopada 2020 r. w sprawie organizacji pracy Urzędu Miejskiego w Morągu.
[23] Polecenie z 16 marca 2020 r.

1.9 Do 13 października 2021 r. IOD przeszkolił dziewięciu pracowników Urzędu z ochrony danych osobowych, w tym z obowiązków wynikających z przepisów rozporządzenia RODO oraz obowiązujących zasad ochrony danych osobowych w Urzędzie.

Dodatkowo 10 września 2020 r. informatyk Urzędu przeprowadził szkolenie dotyczące bezpiecznego, zdalnego połączenia z siecią wewnętrzną Urzędu oraz zasad pracy zdalnej. Wzięło w nim udział 51 pracowników Urzędu, co zostało potwierdzone na liście obecności. Zakres szkolenia obejmował: warunki pracy zdalnej, warunki jakie musi spełniać miejsce świadczenia pracy zdalnej, bezpieczeństwo pracy zdalnej, w tym Internet, urządzenia do pracy zdalnej, zabezpieczanie przekazywanych informacji, zasady korzystania z dokumentów papierowych, sytuacje szczególne. W trakcie szkolenia omówiono również zasady przetwarzania i bezpieczeństwa danych osobowych zawarte w zarządzeniu w sprawie danych osobowych.

Zgodnie z wyjaśnieniami Sekretarza Gminy, informatyk Urzędu przeprowadzał także indywidulane rozmowy z poszczególnymi pracownikami w zakresie bezpieczeństwa informacji.

(akta kontroli str. 60-68, 199-211, 434-440, 466-469)

1.10 Do 19 października 2021 r. w Urzędzie nie opracowano i nie wdrożono SZBI w związku z czym, nie dokonano jego przeglądów.

Nie zachowano także udokumentowanych informacji jako dowodów wyników przeglądu i aktualizacji obwiązujących w Urzędzie regulacji z zakresu bezpieczeństwa danych osobowych. W wyniku tego Urząd posiadał, zarządzenie w sprawie danych osobowych oraz instrukcję określającą sposób zarządzania systemem informatycznym z 2018 r., a także rejestr czynności przetwarzania danych osobowych oraz analizę ryzyka związanego z przetwarzaniem danych osobowych zaktualizowane po raz ostatni w 2019 r.[24]

Natomiast, w związku z obowiązywaniem na terenie kraju stanu epidemii COVID-19, w październiku 2020 r. w Urzędzie wprowadzono, zarządzeniem Burmistrza, regulamin pracy zdalnej, który umożliwiał pracownikom wykonywanie pracy poza siedzibą Urzędu.

W tej sprawie Burmistrz 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.

(akta kontroli str. 3-5, 69-72, 212, 434-440, 466-469)

Stwierdzone nieprawidłowości

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

1. W Urzędzie nie opracowano[25] SZBI, do czego Gmina była zobowiązana zapisami § 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[26].

   W paragrafie tym określono, iż jednostki realizujące zadania publiczne mają obowiązek opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia SZBI zapewniającego poufność,

[24] Tj. odpowiednio: 22 października 2019 r. i 5 listopada 2019 r.
[25] Do 19 października 2021 r.
[26] Dz.U. z 2017 r. poz. 2247, dalej: rozporządzenie w sprawie KRI.

dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

W tej sprawie Burmistrz wyjaśnił, że w Urzędzie wprowadzono:

- instrukcję zarządzania systemem informatycznym służącym przetwarzaniu danych osobowych – zarządzenie 769/18 z 22 maja 2018 r.,
- instrukcję określającą sposób zarządzania systemem informatycznym w Urzędzie Miejskim w Morągu,
- regulamin pracy zdalnej – zarządzenie 385/20 z 20 października 2020 r.

Według wyjaśnień Sekretarza Gminy ww. dokumenty nie zostały opracowane na podstawie normy ISO, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie nie odbywało się na podstawie związanych z ww. normą, normami PN-ISO/IEC 27002, PN-ISO/IEC 27005 oraz PN-ISO/IEC 24762. W związku z tym wymagania, o których mowa z § 20 ust. 1 i 2 rozporządzenia RM w sprawie KRI nie zostały spełnione.

Dodatkowo opracowane w Urzędzie dokumenty w swoich podstawach prawnych nie odwoływały się do zapisów ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[27] ani rozporządzenia RM w sprawie KRI.

(akta kontroli str. 3-5, 402-433, 466-469)

2. W obowiązującym od 19 marca 2018 r. regulaminie organizacyjnym Urzędu nie uwzględniono[28] stanowiska IOD, pomimo iż wyznaczone ono zostało zarządzeniem Burmistrza z 22 maja 2018 r. W strukturze organizacyjnej[29] Urzędu funkcjonował natomiast Administrator Bezpieczeństwa Informacji, który zgodnie z rozporządzeniem RODO, został od 25 maja 2018 r. zastąpiony przez IODO. Regulamin organizacyjny uwzględniał zatem stanowisko, które nie funkcjonowało w Urzędzie od ponad 41 miesięcy.

   Zgodnie natomiast z punktem A3 standardów kontroli zarządczej[30], struktura organizacyjna jednostki powinna być dostosowana do jej aktualnych celów i zadań.

   W tej sprawie Burmistrz wyjaśnił, iż nastąpiło to w skutek omyłki.

   (akta kontroli str. 86, 88-117, 402-433)

OCENA CZĄSTKOWA

NIK negatywnie ocenia działania Burmistrza w zakresie organizacji bezpieczeństwa informacji w Urzędzie, bowiem nie opracował on, nie ustanowił, ani nie wdrożył SZBI, w tym polityki bezpieczeństwa informacji, do czego był zobligowany jako podmiot realizujący zadania publiczne rozporządzeniem RM w sprawie KRI.

W Urzędzie powołano IOD, który posiadał odpowiednie kwalifikacje, a zakres jego obowiązków obejmował zadania określone w rozporządzeniu RODO, jednak stanowisko to nie było uwzględnione w regulaminie organizacyjnym Urzędu.

Odpowiedzialności za zapewnienie bezpieczeństwa informacji zostały przypisane odpowiednim pracownikom, ale tylko w zakresie danych osobowych. Do 13 października 2021 r. obowiązujące w Urzędzie regulacje nie były poddane udokumentowanym, regularnym przeglądom, a regulamin pracy zdalnej wdrożono dopiero 221 dni po rozpoczęciu jej wykonywania. Niemniej jednak należy ocenić, że Urząd do 20 października 2020 r. przygotował się do świadczenia pracy zdalnej

[27] Dz. U. z 2021 r., poz. 670 ze zm.
[28] Do 20 października 2021 r.
[29] Stanowiącej załącznik do Zarządzenia nr 737/18 Burmistrza Morąga z dnia 15 marca 2018 r. w sprawie nadania regulaminu organizacyjnego Urzędu Miejskiego w Morągu, załącznik zawiera omyłkę pisarską w zakresie numeru i daty zarządzenia.
[30] Komunikat nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych.

na wypadek wystąpienia kolejnej fali pandemii m.in. poprzez przygotowanie rozwiązań technicznych i informatycznych, opracowanie i wdrożenie regulaminu pracy zdalnej, a także przeszkolenie swoich pracowników z bezpiecznego, zdalnego połączenia z siecią Urzędu oraz zasad pracy zdalnej.

OBSZAR

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

Opis stanu faktycznego

2.1 W Urzędzie pracę w systemie zdalnym wykonywało w latach 2020-2021 łącznie 73 pracowników.

W 2020 r. było to 73 ze 109 pracowników, w tym:

- na podstawie polecenia pracy zdalnej z inicjatywy pracodawcy – 73 osoby,
- na podstawie polecenia pracy zdalnej z wniosku pracownika – 3 osoby,
- w czasie kwarantanny – 12 osób,
- w czasie izolacji – 9 osób.

Rozpoczęcie wykonywania pracy zdalnej miało miejsce 16 marca 2020 r. Do dnia wejścia w życie zarządzenia w sprawie pracy zdalnej (20 października 2021 r.) 68 pracowników Urzędu wykonywało ją na podstawie ustnego polecenia (jako pracę naprzemienną) oraz 7 indywidualnych poleceń lub zgód na wykonywanie pracy zdalnej wydanych dodatkowo dla 3 pracowników[31].

Od 20 października 2020 r. poleceniami w sprawie organizacji pracy Urzędu[32] Burmistrz kierował pracowników do pracy zdalnej. Wydano także dodatkowo 11 indywidualnych poleceń lub zgód na wykonywanie pracy zdalnej dla 8 pracowników Urzędu[33].

(akta kontroli str. 423-139, 146-178, 213, 215-219, 221-300, 457-465)

Zgodnie z wyjaśnieniami Burmistrza, od 14 marca 2020 r. pracę w Urzędzie 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.

(akta kontroli str. 434-440)

W 2021 r. praca zdalna wykonywana była przez 11 ze 111 pracowników Urzędu w okresie od 18 stycznia 2021 r. do 24 maja 2021 r.[34], w tym:

- na podstawie polecenia pracy zdalnej z inicjatywy pracodawcy – 3 osoby,
- na postawie polecenia pracy zdalnej z wniosku pracownika – 9 osób,
- w czasie kwarantanny - 5 osób,

[31] Tj. trzech pracowników po 1 indywidualnym poleceniu lub zgodzie i jeden pracownik – 4 indywidualne polecenia lub zgody na wykonywanie pracy zdalnej.
[32] Tj. polecenia Burmistrza nr 4/2020, 6/2020, 7/2020, 8/2020, 9/2021, 10/2021, 11/2021, 12/2021, 13/2021, 14/2021, 15/2021, 16/2021, 17/2021, 19/2021, 20/2021, 21/2021.
[33] Tj. jeden pracownik – 4 indywidualne polecenia lub zgody i siedmiu pracowników po 1 indywidualnym poleceniu lub zgodzie.
[34] Według stanu na 21 października 2021 r.

- w czasie izolacji – 1 osoba.

Wszyscy pracownicy wykonywali pracę zdalną na podstawie indywidualnych poleceń lub zgód na jej wykonywanie. Wydano 21 poleceń lub zgód dla 11 pracowników Urzędu[35].

(akta kontroli str. 179-198, 213, 215-218, 220, 301-358, 457-465)

2.2 W szkoleniu pracowników Urzędu z bezpiecznego łączenia się z siecią wewnętrzną Urzędu oraz zasad pracy zdalnej, które odbyło się 10 września 2020 r. i prowadzone było przez informatyka Urzędu wzięło udział 50 z 73 osób wykonujących w Urzędzie pracę zdalną (w tym informatyk prowadzący szkolenie).

Potwierdzenie zapoznania się z regulaminem pracy zdalnej potwierdziło pisemnie 51 z 63 pracowników wykonujących tę pracę po wejściu w życie zarządzenia w sprawie pracy zdalnej[36].

W tej sprawie Burmistrz wyjaśnił, że prawdopodobnie podczas gdy pracownik, odpowiedzialny za przekazanie ww. regulaminu do wiadomości pracowników, przekazywał naczelnikom wydziałów kserokopie dokumentu do użytku i zapoznania się pracowników, a także odbierał od obecnych na stanowiskach pracy podpisy potwierdzające fakt zapoznania się z jego treścią, pracownicy Ci nie byli obecni. Treść regulaminu była dostępna dla pracowników w wydziałach.

(akta kontroli str. 73-74, 200-211, 457-465)

2.3 Zgodnie z wykazem sprzętu komputerowego[37] w posiadaniu Urzędu było 69 zestawów komputerowych stacjonarnych, 15 komputerów przenośnych typu laptop i 1 tablet.

Do 19 października 2020 r. naprzemienna praca rotacyjna w Urzędzie wykonywana była bez wykorzystania systemów informatycznych. Do pracy zdalnej wykorzystano w 2020 r. 5 służbowych komputerów przenośnych oraz 10 telefonów służbowych tylko do komunikacji głosowej, a 10 pracowników wykonywało pracę bez urządzeń[38]. Z prywatnego komputera, tableta lub smartfona skorzystało natomiast 51 pracowników, a z prywatnego telefonu do komunikacji głosowej 53 pracowników. Nie było przypadków wykorzystania nośników danych.

W 2021 r. 2 osoby wykorzystały do pracy zdalnej telefony służbowe do komunikacji głosowej, 10 pracowników używało prywatnych komputerów, tabletów lub smartfonów, a 9 osób wykorzystywało prywatne telefony do komunikacji głosowej. Nie było przypadków wykorzystania nośników danych.

(akta kontroli str. 359, 370-400, 402-440)

W wyniku oględzin wszystkich pięciu służbowych komputerów przenośnych, w które zostali wyposażeni pracownicy Urzędu do wykonywania pracy zdalnej, stwierdzono, że cztery z nich wykorzystywane były jako urządzenia do połączenia z komputerem stacjonarnym w Urzędzie za pomocą „pulpitu zdalnego". Oznaczało to, że na służbowym komputerze przenośnym wykorzystywanym w pracy zdalnej wyświetlany był ekran komputera znajdującego się w biurze, co umożliwiło pracę w taki sam sposób jak w siedzibie Urzędu. Pracownicy mieli zatem pełny dostęp do systemów, programów informatycznych Urzędu, a także pakietu biurowego i służbowej poczty elektronicznej. Na jednym z pięciu komputerów stwierdzono oprogramowanie do Narodowego Spisu Powszechnego.

(akta kontroli str. 360-369)

[35] Tj. jeden pracownik – 6 indywidualnych poleceń lub zgód, jeden pracownik – 4 indywidualne polecenia lub zgody, 2 pracowników – 2 indywidualne polecenia lub zgody i siedmiu pracowników po 1 indywidualnym poleceniu lub zgodzie.
[36] Tj. od 20 października 2020 r.
[37] Wykaz z 19 października 2021 r. prowadzony przez informatyka Urzędu.
[38] Tj. pracowników wykonujących naprzemienną pracę rotacyjną od marca do czerwca 2020 r.

Zgodnie z wyjaśnieniami Burmistrza, zakres pracy zdalnej ustalany był i przekazywany pracownikom w różnych formach ustalanych indywidualnie z bezpośrednim przełożonym, a były to: bezpośredni kontakt telefoniczny, mailowe komunikowanie rozpoczęcia i zakończenia pracy, przesyłanie i odsyłanie zadań mailowo.

(akta kontroli str. 441-456)

2.4 W wyniku oględzin wszystkich pięciu służbowych komputerów przenośnych, w które zostali wyposażeniu pracownicy Urzędu na czas wykonywania pracy zdalnej, stwierdzono, że cztery z nich były wykorzystywane jako urządzenia do połączenia z komputerem stacjonarnym w Urzędzie za pomocą „pulpitu zdalnego". Trzech pracowników Urzędu na komputerach przeznaczonych do pracy zdalnej miało uprawnienia standardowego użytkownika, natomiast jeden pracownik – informatyk Urzędu, posiadał uprawnienia administratora. Nie stwierdzono szyfrowania dysków.

Połączenie z komputerem stacjonarnym w Urzędzie wymagało od pracownika trzyetapowej weryfikacji. W pierwszej kolejności należało zalogować się do komputera za pomocą hasła przypisanego danemu użytkownikowi, następnie utworzyć bezpieczne połączenie VPN wymagające uwierzytelnienia za pomocą indywidualnego loginu i hasła, co zapewniało dostęp do sieci wewnętrznej Urzędu. Na końcu pracownik łączył się, przy wykorzystaniu zdalnego pulpitu, ze swoim komputerem podając login i hasło. Po tej weryfikacji pracownik otrzymywał zdalny dostęp do pulpitu swojego komputera zlokalizowanego w siedzibie Urzędu.

(akta kontroli str. 360-369)

2.5 Zgodnie z zarządzeniem w sprawie pracy zdalnej, w Urzędzie dopuszczono wykonywanie takiej pracy z wykorzystaniem urządzeń własnych pracownika. Od dnia rozpoczęcia wykonywania pracy zdalnej[39] 59 pracowników wykonywało tę pracę z wykorzystaniem sprzętu prywatnego, w tym 51 pracowników na prywatnych komputerach, tabletach lub smartfonach i 53 pracowników przy użyciu prywatnego telefonu do połączeń głosowych.

W zarządzeniu w sprawie pracy zdalnej określono, że sprzęt, na którym wykonywana była praca zdalna powinien posiadać aktywny i zaktualizowany program antywirusowy. Zobligowano także pracowników do konieczności zapewnienia właściwych warunków umożliwiających skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.

Do wykonywania, za pośrednictwem prywatnego sprzętu komputerowego, dopuszczono wszystkie rodzaje czynności, a pracownicy posiadali pełny dostęp do systemów informatycznych Urzędu. W Urzędzie praca na prywatnych komputerach odbywała się z wykorzystaniem „pulpitu zdalnego". Zgodnie z wyjaśnienia Burmistrza połączenie z komputerem stacjonarnym w Urzędzie z prywatnego komputera pracownika wymagało dwuetapowej weryfikacji. Pracownik tworzył bezpieczne połączenie VPN, co wymagało uwierzytelnienia za pomocą indywidualnego loginu i hasła, które umożliwiało dostęp do wewnętrznej sieci Urzędu. Następnie za pomocą zdalnego pulpitu łączył się ze swoim komputerem podając login i hasło. Po tej weryfikacji pracownik otrzymywał zdalny dostęp do pulpitu swojego komputera zlokalizowanego w siedzibie Urzędu.

(akta kontroli str. 69-72, 359, 441-456)

[39] Tj. od 16 marca 2020 r.

2.6 Do dnia 29 października 2021 r. nie wystąpiły przypadki pobierania z Urzędu przez pracowników oryginałów, kserokopii lub skanów dokumentów niezbędnych do wykonywania pracy zdalnej.

(akta kontroli str. 400)

2.7 Zgodnie z wyjaśnieniami Burmistrza, bezpośredni przełożeni ustalali i przekazywali pracownikom zakres pracy zdalnej w różnych formach ustalanych indywidualnie z bezpośrednim przełożonym, przypominali również o obowiązku przestrzegania zasad pracy zdalnej i bezpieczeństwa informacji i systemu. Urząd nie dysponował mailami bezpośrednich przełożonych do pracowników Urzędu przypominających o ww. obowiązku.

Nad bezpieczeństwem systemów i pracy zdalnej czuwał na bieżąco informatyk Urzędu. Dodatkowo na prośbę naczelnika wydziału, informatyk mógł sprawdzić czy dana osoba były zalogowana do systemu. Według wyjaśnień Burmistrza, kontroli logowania wszystkich pracowników Urzędu dokonano dwukrotnie na ustne polecenie Sekretarza Gminy, gdzie informatyk dokonał kontroli, po czym również ustnie przekazał informację zwrotną o logowaniu wszystkich zobowiązanych do tego pracowników.

Zgodnie z wyjaśnieniami Sekretarza, każdy naczelnik wydziału uzgadniał ze swoimi pracownikami sposób nadzoru i monitoringu pracy zdalnej, w tym również w zakresie BHP. Dodatkowo pracownik, któremu zlecono pracę telefonicznie lub mailowo, jej efekty odsyłał do przełożonego.

(akta kontroli str. 441-472)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

NIK pozytywnie ocenia działania Burmistrza w zakresie wdrożonych i stosowanych rozwiązań organizacyjnych i technicznych mających na celu zapewnienie bezpieczeństwa informacji w pracy zdalnej.

W Urzędzie od 20 października 2020 r. wprowadzono zarządzenie w sprawie pracy zdalnej oraz rozwiązania techniczne i informatyczne umożliwiające jej sprawne wykonywanie. Przed rozpoczęciem wykonywania pracy zdalnej przeszkolono pracowników w zakresie bezpiecznego łączenia się z siecią wewnętrzną Urzędu. Zezwolono na realizację zadań w ramach pracy zdalnej przy wykorzystaniu zarówno urządzeń prywatnych, jak i służbowych, a do bezpiecznego łączenia się z siecią Urzędu wykorzystano VPN i zdalny pulpit.

Niemniej jednak należy wskazać, że od 16 marca 2020 r. do 19 października 2020 r. praca zdalna w Urzędzie świadczona była bez narzędzi informatycznych oraz bez wdrożonych pisemnych regulacji. Nie wszyscy pracownicy wykonujący pracę zdalną potwierdzili również zapoznanie się z regulaminem jej świadczenia w formie pisemnej.

IV. Uwagi i wnioski

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

Wnioski

1. Opracowanie, wdrożenie i aktualizowanie systemu zarządzania bezpieczeństwem informacji, w tym polityki bezpieczeństwa informacji w Urzędzie Miejskim w Morągu spełniającego wymogi określone w rozporządzeniu RM w sprawie KRI.
2. Zaktualizowanie w regulaminie organizacyjnym Urzędu zapisów dotyczących IOD.

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 wykorzystania uwag i 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, 29 listopada 2021 r.

Najwyższa Izba Kontroli
Delegatura w Olsztynie
Dyrektor
z up.
Piotr Wanic
Wicedyrektor

.....
podpis

Kontroler
Anna Kamińska-Bisior
Starszy inspektor kontroli państwowej

.....
podpis