NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie

LOL.410.017.04.2021

Dariusz Barton
Warmińsko – Mazurski Wojewódzki
Konserwator Zabytków
Wojewódzki Urząd Ochrony Zabytków w Olsztynie
10-076 Olsztyn, ul. Podwale 1

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	Wojewódzki Urząd Ochrony Zabytków w Olsztynie[1], 10-076 Olsztyn, ul. Podwale 1
Kierownik jednostki kontrolowanej	Dariusz Barton, Warmińsko – Mazurski Wojewódzki Konserwator Zabytków, od 14 listopada 2016 r.
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 zakończenia kontroli[2]) z uwzględnieniem zdarzeń wcześniejszych, jeżeli miały one wpływ na kontrolowane obszary działalności.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Olsztynie
Kontroler	Olga Ratkiewicz, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LOL/121/2021 z 6 października 2021 r.

(akta kontroli str. 1-2)

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą w Urzędzie podejmowano działania na rzecz zapewnienia bezpieczeństwa informacji w pracy na odległość i mobilnym przetwarzaniu danych, jednakże dotyczyły one przede wszystkim danych osobowych.

W Urzędzie określono i przypisano odpowiedzialność za bezpieczeństwo informacji pracownikom oraz wyznaczono Inspektora Ochrony Danych[5]. W obowiązującej Polityce ochrony danych osobowych określono zasady postępowania z nośnikami i urządzeniami przenośnymi, wynoszenia aktywów z Urzędu oraz przesyłania informacji. Zapoznano pracowników z zasadami bezpieczeństwa informacji, w tym w pracy zdalnej. Przeprowadzono analizę ryzyka pracy zdalnej, zaś w oparciu o jej wyniki wprowadzono Regulamin pracy zdalnej i zorganizowano ją w Urzędzie.

Wdrożone i stosowane rozwiązania organizacyjne i techniczne służyły zapewnieniu bezpieczeństwa danych osobowych w pracy zdalnej. Wprowadzona organizacja pracy (m.in. dostęp do sieci Urzędu wyłącznie za pomocą służbowego sprzętu komputerowego, założenie przekazywania pracownikom korzystającym ze sprzętu prywatnego zadań niewymagających przetwarzania danych chronionych) minimalizowała ryzyko naruszenia bezpieczeństwa danych osobowych. Stosowano sprzętowe i programowe środki służące ochronie informacji podnoszące poziom ich bezpieczeństwa, zgodnie z zasadami przyjętymi w Urzędzie.

---

[1] Dalej: WUOZ w Olsztynie lub Urząd.
[2] 19 listopada 2021 r.
[3] Dz. U. z 2020 r. poz. 1200, ze zm., dalej: ustawa o NIK.
[4] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[5] Dalej: IOD.

W toku kontroli stwierdzono jednak nieprawidłowości, które dotyczyły:

- nieopracowania, nieustanowienia i niewdrożenia w Urzędzie systemu zarządzania bezpieczeństwem informacji (w tym polityki bezpieczeństwa informacji), stosownie do przepisów 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*[6], obejmujących swoim zakresem wszystkie kategorie przetwarzanych w Urzędzie informacji,
- przyjęcia Instrukcji postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych po dwóch latach i ośmiu miesiącach od wprowadzenia obowiązku jej stosowania w Urzędzie,
- nieuwzględnienia zasad korzystania z prywatnych komputerów i prywatnych kont pocztowych do celów służbowych w uregulowaniach Urzędu, mimo że dopuszczono możliwość korzystania z takiego sprzętu podczas pracy zdalnej, a reguły takie zostały określone analizie ryzyka pracy zdalnej,
- nieprecyzyjnego określenia w Regulaminie pracy zdalnej obowiązków pracownika w przypadku udostępnienia mu dokumentacji w wersji papierowej w celu wykonywania pracy zdalnej.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[7] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1 W Urzędzie do dnia zakończenia kontroli, tj. do 19 listopada 2021 r., nie opracowano, nie ustanowiono i nie wdrożono systemu zarządzania bezpieczeństwem informacji[8] (w tym polityki bezpieczeństwa informacji), spełniającego wymogi określone przepisami § 20 ust. 2 rozporządzenia KRI, do czego zobowiązywał § 20 ust. 1 ww. rozporządzenia. Nieprawidłowość w tym zakresie opisano szerzej w sekcji Stwierdzone nieprawidłowości.

(akta kontroli str. 3-4)

W okresie objętym kontrolą obowiązujące w Urzędzie uregulowania odnosiły się przede wszystkim do bezpieczeństwa danych osobowych. Były to:

- *Polityka ochrony danych osobowych*, przyjęta zarządzeniem nr 20/2018 Warmińsko - Mazurskiego Wojewódzkiego Konserwatora Zabytków[9] z dnia 5 listopada 2018 r.,
- *Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w WUOZ w Olsztynie,* wprowadzona zarządzeniem nr 7/2021 Wojewódzkiego Konserwatora Zabytków z dnia 22 lipca 2021 r.

W Urzędzie prowadzono rejestr czynności przetwarzania danych osobowych, sporządzono także analizę ryzyka związanego z przetwarzaniem danych osobowych w poszczególnych zbiorach[10] i analizę ryzyka pracy zdalnej[11].

W ww. dokumentach określono m.in. zasady korzystania z urządzeń przenośnych i elektronicznych nośników informacji, bezpieczeństwa sprzętu poza siedzibą,

[6] Dz.U. z 2017 r. poz. 2247, dalej: rozporządzenie KRI.
[7] 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.
[8] Dalej: SZBI.
[9] Dalej: Wojewódzki Konserwator Zabytków.
[10] Sporządzona 1 października 2018 r.
[11] Dokument zatwierdzony 23 kwietnia 2020 r. przez Wojewódzkiego Konserwatora Zabytków.

pozostawiania sprzętu bez opieki, zabezpieczenia przed szkodliwym oprogramowaniem, zabezpieczenia sieci, przesyłania informacji, zabezpieczenia wiadomości w formie elektronicznej oraz zarządzania incydentami związanymi z bezpieczeństwem informacji. Zasady te dotyczyły danych osobowych.

Ponadto w okresie objętym kontrolą w Urzędzie obowiązywały także inne uregulowania dotyczące m.in. bezpieczeństwa informacji, tj.: *Regulamin pracy zdalnej dla pracowników WUOZ w Olsztynie wraz z Delegaturą w Elblągu i Delegaturą w Ełku*[12], *System elektronicznego obiegu dokumentów EZD Spektrum w WUOZ w Olsztynie*[13], *Zasady korzystania ze służbowych telefonów komórkowych przez pracowników WUOZ w Olsztynie*[14], *Zasady (polityka) rachunkowości*[15].

Z Polityką ochrony danych osobowych zapoznało się[16] 43 pracowników Urzędu, a z regulaminem pracy zdalnej 38 pracowników (wszyscy, którzy świadczyli pracę w sposób zdalny w latach 2020-2021).

(akta kontroli str. 3-133, 148-149, 192-196)

W Urzędzie do 19 listopada 2021 r. nie opracowano schematu klasyfikacji informacji, o którym mowa w punkcie A.8.2 Polskiej Normy PN-EN ISO/IEC 27001[17]. Według wyjaśnień Zastępcy Wojewódzkiego Konserwatora Zabytków posiłkowano się rejestrem czynności przetwarzania danych, który klasyfikuje procesy w zbiorach danych, instrukcją kancelaryjną, jak również ustawą z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego[18] i innymi ustawami.

W konsekwencji, nie zidentyfikowano wszystkich informacji ani aktywów z nimi związanymi oraz środków wykorzystywanych do ich przetwarzania w sposób określony w punkcie A.8.2 normy ISO, tj. zapewniający przypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla Urzędu.

Zbiory danych osobowych podlegających przetwarzaniu i zabezpieczeniu w Urzędzie określono w rejestrze czynności przetwarzania, o którym mowa w art. 30 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)*[19]. Dokonano w nim identyfikacji m.in. kategorii osób, których dane dotyczą; informacji będących w posiadaniu Urzędu oraz zbiorów, w których się znajdują; celu przetwarzania; nazwy systemu lub oprogramowania, za pomocą którego dane są przetwarzane; oznaczenia odbiorców danych, którym powyższe informacje mogą być przekazywane; rodzaju zastosowanych środków ochrony danych.

Jak wyjaśnił Zastępca Wojewódzkiego Konserwatora Zabytków, oprócz danych osobowych w zidentyfikowanych zbiorach znajdują się również inne dane, dotyczące m.in. szeroko pojętych informacji o zabytkach ruchomych, nieruchomych i archeologicznych. Dodał także, że identyfikacji informacji dokonano także podczas tworzenia systemu elektronicznego obiegu dokumentów.

(akta kontroli str. 47-80, 134-136, 189-191)

W Urzędzie w okresie objętym kontrolą, stosownie do § 20 ust. 2 pkt 2 rozporządzenia KRI, utrzymywano aktualność inwentaryzacji sprzętu

[12] Wprowadzony zarządzeniem nr 14/2020 Wojewódzkiego Konserwatora Zabytków z dnia 9 października 2020 r., dalej: Regulamin pracy zdalnej
[13] Wprowadzony zarządzeniem nr 8/2019 Wojewódzkiego Konserwatora Zabytków z dnia 22 lutego 2019 r.
[14] Wprowadzone zarządzeniem nr 2/2018 Wojewódzkiego Konserwatora Zabytków z dnia 5 listopada 2018 r.
[15] Wprowadzona zarządzeniem nr 30/2017 Wojewódzkiego Konserwatora Zabytków z dnia 11 kwietnia 2017 r.
[16] Do 30 października 2021 r.
[17] Dalej: norma ISO.
[18] Dz. U. z 2021 r., poz. 735, ze zm.
[19] Dz. Urz. UE L 119 z 4 maja 2016 r., dalej: RODO.

i oprogramowania służącego do przetwarzania informacji, obejmującej jego rodzaj i konfigurację, do czego wykorzystywano odpowiednie oprogramowanie.
Informatyk podał, że na komputerach podpiętych do domeny Urzędu automatycznie instaluje się klient programu, który inwentaryzuje zasoby sprzętowe i oprogramowanie komputera, a następnie przesyła raport do centralnej bazy danych na serwerze Urzędu. Ponadto poinformował, iż inwentaryzacja jest aktualizowana przy każdym zalogowaniu się komputera w sieci Urzędu, co pozwala na bieżącą ewidencję parametrów technicznych sprzętu, konfiguracji sprzętowej i sieciowej, zainstalowanego oprogramowania oraz pojemności dysków.

Na podstawie oględzin funkcjonalności tego oprogramowania stwierdzono, że w bazie znajdowały się informacje o 53 maszynach, w tym 13 laptopach. Program umożliwiał wyświetlenie szczegółowego raportu o parametrach sprzętu i oprogramowania, obejmującego m.in. numer seryjny maszyny i jej nazwę w sieci, nazwę ostatniego użytkownika, adres IP, listę zainstalowanego oprogramowania i ich aktualizacji.

(akta kontroli str. 137-147)

1.2 W obowiązującym Regulaminie organizacyjnym[20] Urzędu odpowiedzialność za bezpieczeństwo informacji przypisano wszystkim pracownikom. I tak, w ich zakresach obowiązków wskazano, że są oni odpowiedzialni za właściwe przechowywanie i zabezpieczenia akt oraz dokumentów dotyczących prowadzonych spraw, przestrzeganie zasad bezpieczeństwa danych zgromadzonych w systemie informatycznym, jak również za przestrzeganie przepisów wynikających z ustawy z 10 maja 2018 r. o ochronie danych osobowych[21]. Kierownikom Delegatur[22] i Wydziałów[23] natomiast przypisano pełnienie nadzoru nad przestrzeganiem ww. zasad przez podległych im pracowników.

(akta kontroli str. 148-174)

Odpowiedzialność i uprawnienia osób pełniących ważną rolę w zapewnieniu bezpieczeństwa danych osobowych w Urzędzie określono w obowiązującej Polityce ochrony danych osobowych. Byli to: Administrator Danych Osobowych, Inspektor Ochrony Danych oraz Administrator Systemów Informatycznych.

Za ustalanie celów i sposobów przetwarzania danych osobowych, wdrażanie środków technicznych i organizacyjnych zapewniających przetwarzanie danych osobowych zgodnie z prawem, ich przeglądy i aktualizacje odpowiedzialny był Wojewódzki Konserwator Zabytków jako Administrator Danych Osobowych.

Inspektor Danych Osobowych odpowiadał m.in. za:
- monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz wdrożonych polityk w zakresie ochrony danych osobowych w Urzędzie,
- udzielanie na żądanie kierownika jednostki zaleceń i opinii co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO,
- prowadzenie centralnego rejestru czynności przetwarzania danych osobowych na podstawie danych otrzymanych od poszczególnych Kierowników komórek organizacyjnych Urzędu,
- zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

[20] Regulamin organizacyjny Wojewódzkiego Urzędu Ochrony Zabytków w Olsztynie nadany zarządzeniem nr 159 Wojewody Warmińsko-Mazurskiego z dnia 24 lipca 2013 r., zmieniony zarządzeniem nr 110 Wojewody Warmińsko-Mazurskiego z dnia 10 kwietnia 2017 r.
[21] Dz. U. z 2019 r., poz. 1781.
[22] W Elblągu i w Ełku.
[23] Wydziału ds. Inspekcji zabytków archeologicznych oraz rejestru zabytków, dokumentacji zabytków i informatyki (dalej: IZAR) oraz Wydziału ds. inspekcji zabytków nieruchomych i ruchomych (dalej: IZNR).

Administratorowi Systemu Informatycznego[24] przypisano odpowiedzialność za zapewnienie prawidłowego funkcjonowania systemu informatycznego zgodnie z ww. polityką, w tym:

- zarządzanie bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym (w tym zarządzanie konfiguracją systemów, oprogramowania i urządzeń),
- doskonalenie i rozwój metod zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,
- przydzielanie identyfikatorów i haseł do systemu informatycznego,
- sprawowanie nadzoru nad mechanizmami kontroli dostępu do oprogramowania i aplikacji służących do przetwarzania danych osobowych.

(akta kontroli str. 7-46, 175-182)

1.3 W latach 2020-2021 Urząd zawierał z podmiotem zewnętrznym[25] umowy[26] na pełnienie funkcji Inspektora Ochrony Danych w celu realizacji zadań wskazanych w art. 37 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*[27]. Zleceniobiorca posiadał kwalifikacje, o których mowa w art. 37 ust. 5 rozporządzenia RODO, a zakres jego obowiązków, określony w zawartych umowach, obejmował realizację zadań określonych w art. 39 ww. rozporządzenia i był spójny z zapisami przyjętej Polityki ochrony danych osobowych.

(akta kontroli str. 183-191)

1.4 W Polityce ochrony danych osobowych obowiązującej w Urzędzie określone zostały zasady korzystania z urządzeń przenośnych, na których przetwarzane są dane osobowe oraz elektronicznych nośników informacji (tj. płyt CD, DVD, pendrive, kart pamięci, dysków zewnętrznych i innych zewnętrznych nośników informacji). Uwzględniały one niektóre ryzyka (organizacyjne, informatyczne, fizyczne, ze strony pracowników) związane z pracą zdalną.

Zgodnie z ww. polityką użytkownik zobowiązany był m.in. do:

- transportu urządzenia lub nośnika w sposób minimalizujący ryzyko kradzieży, lub zniszczenia, w szczególności do transportowania ich w bagażu podręcznym oraz niepozostawiania bez nadzoru,
- niedopuszczania do korzystania z urządzenia lub nośnika przez osoby nieupoważnione,
- korzystania z urządzenia lub nośnika w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabroniono korzystania z urządzenia lub nośnika w miejscach publicznych i w środkach transportu publicznego,
- zabezpieczania dostępu do urządzenia hasłem o odpowiedniej sile oraz systematycznej zmiany haseł,
- zabezpieczania danych osobowych zapisanych na urządzeniu lub nośniku poprzez zastosowanie oprogramowania szyfrującego te dane lub w taki sposób, aby dostęp do danych był możliwy wyłącznie po podaniu hasła,
- blokowania dostępu do urządzenia w przypadku, gdy nie jest ono wykorzystywane przez upoważnionego użytkownika,

[24] Rolę tę zlecono osobie fizycznej prowadzącej działalność gospodarczą, z którą Urząd w latach 2020-2021 zawierał na okres roku umowy na zarządzanie i administrowanie systemem informatycznym Urzędu (umowa nr 4/2020 z 18 grudnia 2019 r. oraz umowa nr 3/2021 z 4 stycznia 2021 r.), w niniejszym wystąpieniu „Informatyk".
[25] Osoba fizyczna prowadząca działalność gospodarczą w formie spółki cywilnej.
[26] Umowa nr 13/2020 z dnia 2 stycznia 2020 r. oraz umowa nr 1/2021 z dnia 4 stycznia 2021 r.
[27] Dalej: Rozporządzenie RODO.

– zapewnienia instalacji i aktualizacji oprogramowania antywirusowego na urządzeniu,
– podjęcia działań mających na celu prawidłowe zabezpieczenie urządzenia przenośnego przed rozpoczęciem korzystania z niego poza obszarem przetwarzania.

Ww. zasady ochrony danych osobowych nie odnosiły się do ochrony informacji znajdujących się na tradycyjnych dokumentach lub wydrukach komputerowych, natomiast w Regulaminie pracy zdalnej zobowiązano pracowników do zabezpieczenia posiadanych danych i informacji (w tym także znajdujących się na nośnikach papierowych) przed zniszczeniem i osobami postronnymi, w tym wspólnie zamieszkującymi z pracownikiem.

(akta kontroli str. 4-46, 97-104, 192-196)

W Urzędzie w latach 2020-2021 nie prowadzono rejestru nośników służących do przechowywania informacji z przypisaniem odpowiedzialności za dany nośnik, ponieważ, jak wyjaśnił Zastępca Wojewódzkiego Konserwatora Zabytków, nie nabywano i nie stosowano takich nośników, z uwagi na bezpieczeństwo danych oraz w celu zminimalizowania ryzyka ich utraty.

(akta kontroli str. 134-136)

1.5 W Urzędzie w okresie objętym kontrolą w Polityce ochrony danych osobowych ustanowiono zasady wynoszenia aktywów oraz podstawowe warunki niezbędne dla zapewnienia ich bezpieczeństwa poza siedzibą jednostki w odniesieniu do danych osobowych i aktywów służących do ich przetwarzania.

Podstawową zasadą wprowadzoną w ww. polityce było ograniczenie do minimum przetwarzania danych osobowych na urządzeniach przenośnych oraz elektronicznych nośnikach informacji[28] (zarówno w siedzibie Urzędu, jak i poza siedzibą Urzędu). Dopuszczalne było użycie w tym celu wyłącznie służbowych urządzeń przenośnych lub służbowych elektronicznych nośników informacji przydzielonych przez Urząd.

Reguły przyjęte zapisami ww. polityki wskazywały, że każda osoba przetwarzająca dane osobowe przy wykorzystaniu urządzenia przenośnego lub elektronicznego nośnika informacji odpowiadała za prawidłowe zabezpieczenie przetwarzanych informacji, zwłaszcza przed nieuprawnionym dostępem, modyfikacją lub zniszczeniem.

Wprowadzono mechanizmy ochrony w celu redukcji ryzyk wynikających z zagrożeń i niebezpieczeństw środowiskowych oraz okazji do nieuprawnionego dostępu, co opisano w punkcie 1.4.

Ponadto w *Polityce (zasadach) rachunkowości* wskazano m.in., że programy komputerowe i dane informatycznego systemu rachunkowości chroni się przed dostępem osób nieupoważnionych i zniszczeniem przez zastosowanie właściwych rozwiązań organizacyjnych i programowych, a udostępnianie danych i dokumentów z zakresu rachunkowości poza siedzibą jednostki jest możliwe po uzyskaniu pisemnej zgody Wojewódzkiego Konserwatora Zabytków i pozostawieniu pisemnego pokwitowania zawierającego spis wydanych dokumentów.

Zapisami zarządzenia Wojewódzkiego Konserwatora Zabytków w sprawie ustalenia zasad korzystania ze służbowych telefonów komórkowych przez pracowników WUOZ w Olsztynie zobowiązano pracowników do nieudostępniania telefonów służbowych innym osobom.

(akta kontroli str. 7-46, 81-96, 124-130)

[28] Płyty CD, DVD, pendrive, kart pamięci, dysków zewnętrznych i innych zewnętrznych nośników informacji.

W sporządzonej w kwietniu 2020 r. analizie ryzyk pracy zdalnej zdefiniowano ryzyka związane z wynoszeniem aktywów z siedziby Urzędu (m.in. nieautoryzowany dostęp do danych przez rodzinę, przypadkowe lub niezgodne z prawem zniszczenie / utrata / modyfikacja danych osobowych, kradzież stacji roboczej) oraz określono mechanizmy i sposoby zabezpieczenia przed zdarzeniami wynikającymi ze zmaterializowania się tych ryzyk.

W konsekwencji, w regulaminie pracy zdalnej określono podstawowe warunki niezbędne do zapewnienia bezpieczeństwa sprzętu komputerowego i dokumentów papierowych poza siedzibą jednostki, co opisano w punkcie 1.8.

(akta kontroli str. 105-113, 192-196)

1.6 W latach 2020-2021 w Urzędzie obowiązywały zasady przesyłania informacji, które określono w Polityce ochrony danych osobowych. I tak:

- przydzielono pracownikom służbowe adresy poczty e-mail w domenie należącej do Urzędu do wykonywania obowiązków służbowych oraz zapewniono możliwość korzystania z klienta poczty do obsługi poczty elektronicznej, przy czym wprowadzono zasadę minimalizacji korzystania z poczty poprzez logowanie bezpośrednio na serwer poczty,
- zobowiązano pracowników do stosowania środków kryptograficznej ochrony danych wobec danych osobowych oraz danych wykorzystywanych do uwierzytelnienia przesyłanych za pośrednictwem sieci Internet; w szczególności dane osobowe pozyskiwane przez Urząd za pośrednictwem stron internetowych należało szyfrować np. poprzez zapewnienie dla strony internetowej certyfikatu SSL,
- wprowadzono zasadę ograniczenia do niezbędnego minimum przesyłania danych osobowych przez Urząd za pośrednictwem sieci Internet, zaś w przypadku przesyłania za pośrednictwem poczty elektronicznej dokumentów elektronicznych zawierających dane osobowe należało zabezpieczyć je przed dostępem osób nieuprawnionych (np. oprogramowaniem szyfrującym dane lub zabezpieczając dokument hasłem), na stacjach roboczych użytkowników zapewniano oprogramowanie szyfrujące dane lub umożliwiające zabezpieczenie plików hasłem.

(akta kontroli str. 7-46)

W regulaminie pracy zdalnej dopuszczono wykorzystanie prywatnych komputerów do celów służbowych. Jednakże w obowiązujących w latach 2020-2021 w Urzędzie uregulowaniach dotyczących bezpieczeństwa informacji nie uwzględniono kwestii korzystania z prywatnych komputerów i prywatnych kont pocztowych do zadań służbowych, w tym nie określono warunków korzystania z nich, mimo że zasady takie określono w analizie ryzyka pracy zdalnej sporządzonej w kwietniu 2020 r. Nieprawidłowość szerzej opisano w sekcji Stwierdzone nieprawidłowości.

(akta kontroli str. 105-113, 192-196)

1.7 W Urzędzie 22 lipca 2021 r. przyjęto instrukcję postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych, której obowiązek stosowania wprowadzono zapisami § 26 Polityki ochrony danych osobowych z 5 listopada 2018 r. (opisano szerzej w sekcji Stwierdzone nieprawidłowości).

W dokumencie tym określono definicję naruszenia danych osobowych oraz jednolite zasady postępowania w przypadku podejrzenia naruszenia lub naruszenia ochrony danych osobowych przetwarzanych zarówno w systemach informatycznych i innych elektronicznych nośnikach informacji, jak również w dokumentach mających postać tradycyjną.

W instrukcji tej zawarto otwarty katalog zdarzeń, których może dotyczyć naruszenie danych osobowych, tj. m.in.:

- dopuszczenie do przetwarzania danych osobowych osoby nie posiadającej odpowiedniego upoważnienia,
- nieupoważniony dostęp, modyfikacja, kopiowanie lub zniszczenie/usunięcie danych osobowych przetwarzanych zarówno w systemie informatycznym, innych elektronicznych nośnikach informacji, jak również w dokumentach papierowych,
- przesyłanie dokumentów papierowych lub nośników elektronicznych zawierających dane osobowe bez zabezpieczenia,
- ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom nieuprawnionym,
- wykrycie lub podejrzenie obecności wirusa komputerowego lub innego złośliwego oprogramowania.

Zgodnie z zapisami ww. instrukcji, za sporządzenie raportu z naruszenia ochrony danych osobowych odpowiedzialny był IOD. Informację o stwierdzonym naruszeniu bezpieczeństwa należało także odnotować w Ewidencji naruszeń ochrony danych osobowych.

IOD wyjaśnił, że w okresie objętym kontrolą nie wpłynęły do niego informacje o naruszeniu ochrony danych osobowych w Urzędzie.

Natomiast Informatyk podał, że w praktyce pracownicy zgłaszali i konsultowali z nim wszelkie wątpliwości dotyczące postępowania z plikami / mailami oraz nietypowe zdarzenia w systemie informatycznym. W badanym okresie nie było przypadków, które zakwalifikowałby jako incydenty bezpieczeństwa teleinformatycznego, tj. m.in. nie było dłuższych przerw w łączności, paraliżujących pracę, ani nie zidentyfikowano prób nieuprawnionego dostępu do konta przez osoby z zewnątrz.

(akta kontroli str. 81-96, 177-182, 189-191)

1.8 Regulamin pracy zdalnej został wprowadzony w Urzędzie 19 października 2020 r. w związku z przeciwdziałaniem i zapobieganiem rozprzestrzenianiu się COVID-19. Określono w nim warunki dopuszczalności[29] pracy zdalnej, prawa i obowiązki pracodawcy i pracownika, zapisy dotyczące ochrony informacji i danych osobowych.

Jak wyjaśnił Wojewódzki Konserwator Zabytków, Regulamin pracy zdalnej przyjęto w Urzędzie tuż przed rozpoczęciem tzw. drugiej fali pandemii, po doprecyzowaniu przepisów odnośnie pracy zdalnej w ustawie z dnia 19 czerwca 2020 r. *o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzeniu układu w związku z wystąpieniem COVID-19*[30].

W regulaminie tym zobowiązano pracowników do zorganizowania stanowiska do pracy zdalnej w sposób zapewniający bezpieczne i higieniczne warunki pracy oraz bezpieczeństwo danych osobowych, zabezpieczenia sprzętu (służbowego oraz prywatnego, jeżeli jest wykorzystywany do celów służbowych) oraz posiadanych danych i informacji (w tym także znajdujących się na nośnikach papierowych) przed zniszczeniem i osobami postronnymi, w tym wspólnie zamieszkującymi z pracownikiem.
Wskazano także, że w przypadku udostępnienia pracownikowi w celu wykonywania pracy zdalnej dokumentacji w wersji papierowej, pracownik podpisuje oświadczenie.

[29] Po złożeniu przez pracodawcę lub bezpośredniego przełożonego pracownika oświadczenia dotyczącego polecenia pracy zdalnej lub po udzieleniu zgodny na pracę zdalną na wniosek pracownika – według wzorów stanowiących załączniki do regulaminów.
[30] Dz. U. z 2021 r., poz. 1072, ze zm.

Nie określono jednak wzoru takiego oświadczenia, a także co powinno zawierać oraz komu powinno zostać przekazane (szerzej opisano w sekcji Stwierdzone nieprawidłowości).

W Regulaminie pracy zdalnej nie określono szczegółowo zasad zachowania bezpieczeństwa informacji w trakcie pracy zdalnej, lecz wskazano, że w sprawach nieuregulowanych regulaminem zastosowanie znajdują procedury wewnętrzne oraz przepisy prawa powszechnie obowiązującego.

Jak wyjaśnił Wojewódzki Konserwator Zabytków, powyższe stanowiło odesłanie do obowiązków wynikających m.in. z Polityki ochrony danych osobowych, RODO, ustawy o ochronie danych osobowych oraz innych przepisów regulujących ochronę danych prawnie chronionych.

(akta kontroli str. 192-205)

1.9 W Urzędzie w okresie objętym kontrolą prowadzono działania mające na celu uświadamianie, kształcenie i szkolenie pracowników z zakresu bezpieczeństwa informacji.

W 2018 r., w związku z wprowadzeniem rozporządzenia RODO i zmianą wewnętrznych polityk Urzędu w tym zakresie, Inspektor Ochrony Danych przeszkolił 29 pracowników Urzędu z ochrony danych osobowych, prawidłowego zabezpieczenia tych danych oraz działań w razie naruszenia ich bezpieczeństwa.

Ponadto Inspektor przesyłał pracownikom mailowe instrukcje dotyczące m.in. zasad zachowania bezpieczeństwa informacji na stanowisku pracy (w tym m.in.: reguły czystego biurka, odpowiedniego niszczenia zbędnych dokumentów, zachowania poufności przetwarzanych danych osobowych), zasad zapewniających poufność i integralność danych osobowych zbieranych i przekazywanych drogą elektroniczną oraz w zakresie cyberbezpieczeństwa (wskazówki na wypadek ataku). Przekazywał także ostrzeżenia przed zagrożeniami m.in. przed kampanią wykorzystującą socjotechnikę, nakłaniającą do zainstalowania złośliwego oprogramowania[31].

Działania zmierzające do podwyższenia świadomości pracowników w zakresie bezpieczeństwa informacji podejmował także Informatyk.

Wyjaśnił, że przy pierwszym podłączeniu przez pracownika laptopa służbowego do sieci Urzędu w celu rozpoczęcia pracy zdalnej, asystował zdalnie (telefonicznie) przy tej czynności i udzielał krótkiego instruktażu, jak się połączyć i pracować zdalnie. Przekazywał informacje, jak się logować do połączenia zdalnego, jak diagnozować i reagować na zerwanie połączeń. Uczulał na zachowanie bezpieczeństwa informacji przed osobami postronnymi.

Podał także, że wykonując obowiązki w zakresie usuwania problemów informatycznych na bieżąco prowadził działania zmierzające do uświadamiania pracowników w zakresie zagrożeń bezpieczeństwa informacji.

(akta kontroli str. 177-182, 189-191, 206-226, 287-314)

1.10 Do dnia zakończenia kontroli, tj. do 19 listopada 2021 r. w Urzędzie nie opracowano i nie wdrożono SZBI, a w konsekwencji nie dokonywano jego przeglądów. Natomiast, jak podał Zastępca Wojewódzkiego Konserwatora Zabytków, w Urzędzie na bieżąco, w miarę potrzeb i sytuacji dokonywano przeglądu uregulowań dotyczących bezpieczeństwa informacji.

W związku z ogłoszeniem na terenie kraju stanu epidemii, w kwietniu 2020 r. przeprowadzono w WUOZ analizę ryzyka dotyczącą przetwarzania danych w okresie pracy zdalnej. W ww. dokumencie przeanalizowano dwie grupy procesów,

[31] Informacja od CERT – zespołu powołanego do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet, działającego w strukturach NASK.

tj. pracę zdalną z wykorzystaniem służbowego komputera (laptop) oraz pracę zdalną w wykorzystaniem prywatnego komputera. W każdej z nich wskazano źródła ryzyk (zagrożeń) w czterech obszarach ryzyk (organizacyjnych, informatycznych, fizycznych oraz ze strony personelu). Określono rekomendowane rozwiązania w związku ze zidentyfikowanymi ryzykami.
Jak wyjaśnił Inspektor Ochrony Danych, analiza była tworzona we współpracy z Zastępcą Wojewódzkiego Konserwatora Zabytków i Informatykiem, którzy określali specyfikę pracy w jednostce oraz wskazywali zagrożenia. Analizowano pozostające w zasięgu jednostki rozwiązania minimalizujące zagrożenia związane z pracą zdalną.
W październiku 2020 r., przed rozpoczęciem pracy zdalnej w Urzędzie wprowadzono, zarządzeniem Wojewódzkiego Konserwatora Zabytków, regulamin pracy zdalnej, w którym unormowano wykonywanie pracy poza siedzibą Urzędu.

(akta kontroli str. 105-113, 189-196)

Stwierdzone nieprawidłowości

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

1. W Urzędzie do dnia zakończenia kontroli, tj. do 19 października 2021 r., nie opracowano, nie ustanowiono i nie wdrożono (a w konsekwencji nie monitorowano i nie przeglądano, nie utrzymano i nie doskonalono) 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.
   Wojewódzki Konserwator Zabytków wyjaśnił, że zasady ujęte w Polityce ochrony danych osobowych wdrożonej w Urzędzie w 2018 r. na podstawie RODO samoczynnie wymuszają ochronę wszystkich przetwarzanych danych, wypełniając tym samym w większości wymogi określone w § 20 ust. 2 rozporządzenia w sprawie KRI.

   Zdaniem NIK, w Urzędzie brak było wprowadzenia 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.

   (akta kontroli str. 3-133, 177-182, 192-205)

2. W Urzędzie przyjęto *Instrukcję postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w WUOZ w Olsztynie*[32] dopiero w lipcu

[32] Wprowadzona zarządzeniem nr 7/2021 WKZ z dnia 22 lipca 2021 r.

2021 r., tj. po dwóch latach i ośmiu miesiącach od wprowadzenia, zapisami § 26 Polityki ochrony danych osobowych z listopada 2018 r., obowiązku stosowania tej instrukcji w Urzędzie.

Wojewódzki Konserwator Zabytków wyjaśnił, że przyjęcie ww. instrukcji w formie zarządzenia dopiero w dniu 22 lipca 2021 roku spowodowane było wybuchem epidemii COVID–19 w marcu 2020 roku, co było sytuacją nową i zaskakującą. W związku z tym, jak podał, działania kierownictwa skupiały się wokół zapewnienia ciągłości pracy Urzędu, tak aby jego działalnie nie narażało życia i zdrowia pracowników, a wdrożenie ww. dokumentu zostało przesunięte na późniejszy termin.

NIK zauważa jednak, że od momentu przyjęcia Polityki ochrony danych osobowych (wprowadzającego obowiązek stosowania instrukcji) do ogłoszenia na terenie kraju stanu epidemii upłynęło ponad 16 miesięcy, a Urząd w tym okresie nie wprowadził dokumentu regulującego zasad zarządzania incydentami związanymi z bezpieczeństwem informacji.

(akta kontroli str. 81-96, 197-205)

3. W uregulowaniach dotyczących bezpieczeństwa informacji obowiązujących w Urzędzie w latach 2020-2021 nie uwzględniono zasad korzystania z prywatnych komputerów i prywatnych kont pocztowych do celów służbowych, mimo że dopuszczono możliwość korzystania z takiego sprzętu podczas pracy zdalnej, a reguły takie zostały określone jako „zabezpieczenia do obszaru" w sporządzonej w kwietniu 2020 r. analizie ryzyka pracy zdalnej i stanowiły rekomendowane dla Urzędu rozwiązania organizacyjne i informatyczne mające na celu wyeliminowanie lub ograniczenie zidentyfikowanych ryzyk.

   Dotyczyło to stosowania zabezpieczeń przetwarzanych informacji z użyciem prywatnych komputerów i sieci w trakcie pracy zdalnej, w tym:
   - warunków, jakie powinien spełniać prywatny sprzęt (w tym jego oprogramowanie), aby można go było wykorzystywać w realizacji zadań służbowych w trakcie pracy zdalnej,
   - zasad postępowania z informacjami / dokumentami, które znalazły się w pamięci prywatnego sprzętu komputerowego wykorzystywanego do celów służbowych,
   - reguł korzystania z prywatnego punktu dostępowego do sieci Internet i prywatnych skrzynek e-mail do zadań służbowych.

   Wojewódzki Konserwator Zabytków wyjaśnił, że jego zdaniem, rozwiązania wskazane w analizie ryzyka były stosowane i nie wymagały dodatkowego implementowania w regulacjach Urzędu. Wskazał, że założono ograniczenie przetwarzania podczas pracy zdalnej (tj. poza siedzibą Urzędu) danych wymagających ochrony do niezbędnego minimum, zgodnie z zapisami obowiązującej już w Urzędzie Polityce ochrony danych osobowych z 2018 r. W wykonaniu powyższej reguły, pracownikom, którym polecano świadczenie pracy w sposób zdalny, powierzano do wykonania przede wszystkim takie zadania, które nie wiązały się z potrzebą przetwarzania danych prawnie chronionych. Podał także, że IOD w wiadomościach mailowych przekazywał pracownikom informacje na temat sposobu przetwarzania danych osobowych podczas pracy zdalnej.

   Zdaniem NIK, w przypadku dopuszczenia w jednostce wykorzystania sprzętu prywatnego celowe jest uregulowanie zasad korzystania z niego, zwłaszcza, że w Urzędzie nie dokonano klasyfikacji informacji, nie określono katalogu czynności dopuszczonych do wykonywania za pośrednictwem prywatnego

sprzętu komputerowego ani informacji, jakie mogą być przesyłane za pośrednictwem prywatnych skrzynek mailowych.

(akta kontroli str. 3-133, 197-205)

4. Nieprecyzyjnie określono w § 2 pkt 3 Regulaminu pracy zdalnej z 19 października 2020 r. obowiązki pracownika w przypadku udostępnienia mu w celu wykonywania pracy zdalnej dokumentacji w wersji papierowej. Wskazano bowiem, że pracownik w takiej sytuacji podpisuje oświadczenie, ale nie wyjaśniono, czego powinno dotyczyć to oświadczenie, ani komu powinno być przekazane. Nie opracowano także wzoru takiego oświadczenia.

   Powyższy zapis w ocenie NIK był zbyt ogólny, a w konsekwencji pracownicy nie stosowali go w praktyce.

   Zastępca Wojewódzkiego Konserwatora Zabytków wyjaśnił, że w założeniu oświadczenia pracowników miały wskazywać wprost, jaką sprawę pobiera do pracy zdalnej, dlatego też nie opracowano wzoru oświadczenia. Podał także, że oświadczenie to pracownik miał składać wówczas, gdy pobierał całość oryginalnej dokumentacji sprawy, a tego rodzaju okoliczności w Urzędzie nie występowały, wobec tego takie oświadczenia nie były składane.

   Zdaniem NIK, zapisy cz. II.C.17 standardów kontroli zarządczej dla sektora finansów publicznych[33] w zakresie komunikacji wewnętrznej, według których należy zapewnić efektywne mechanizmy przekazywania ważnych informacji w obrębie struktury organizacyjnej jednostki, wskazują na potrzebę doprecyzowania powyższych uregulowań.

   (akta kontroli str. 192-196, 249-257, 287-317)

OCENA CZĄSTKOWA

W okresie objętym kontrolą w Urzędzie podejmowano działania w celu zorganizowania bezpieczeństwa informacji w pracy na odległość i mobilnym przetwarzaniu danych. Określono i przypisano odpowiedzialność za bezpieczeństwo informacji pracownikom, powierzono pełnienie funkcji IOD podmiotowi, który posiadał odpowiednie kwalifikacje, a zakres jego obowiązków obejmował zadania określone w RODO. W odniesieniu do danych osobowych określono zasady postępowania z nośnikami i urządzeniami przenośnymi, wynoszenia aktywów z Urzędu oraz przesyłania informacji. Przeprowadzono analizę ryzyka pracy zdalnej, a w oparciu o jej wyniki wprowadzono regulamin pracy zdalnej. Zapewniono także podnoszenie wiedzy pracowników w zakresie zagrożeń dla bezpieczeństwa informacji.

Stwierdzone nieprawidłowości dotyczyły:

- nieopracowania, nieustanowienia i niewdrożenia w Urzędzie SZBI oraz Polityki Bezpieczeństwa Informacji, stosownie do przepisów rozporządzenia w sprawie KRI, obejmujących swoim zakresem wszystkie kategorie przetwarzanych w Urzędzie informacji,
- przyjęcia Instrukcji postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych po dwóch latach i ośmiu miesiącach od wprowadzenia obowiązku jej stosowania w Urzędzie,
- nieuwzględnienia zasad korzystania z prywatnych komputerów i prywatnych kont pocztowych do celów służbowych w uregulowaniach Urzędu, mimo że dopuszczono możliwość korzystania z ww. sprzętu podczas pracy zdalnej, a reguły takie zostały określone analizie ryzyka pracy zdalnej,

[33] Stanowiące załącznik do komunikatu 23 Ministra Finansów z dnia 16 grudnia 2009 r. *w sprawie standardów kontroli zarządczej dla sektora finansów publicznych* (Dz. Urz. MF Nr 15, poz. 84).

- nieprecyzyjnego określenia w Regulaminie pracy zdalnej obowiązków pracownika w przypadku udostępnienia mu w celu wykonywania pracy zdalnej dokumentacji w wersji papierowej.

OBSZAR

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

Opis stanu faktycznego

2.1 W latach 2020-2021 (do końca października) w Urzędzie dwukrotnie wprowadzono pracę zdalną, która była świadczona przez pracowników naprzemiennie z pracą w siedzibie Urzędu. Miało to miejsce w okresie od połowy marca do końca maja 2020 r. (przez 11 tygodni) oraz od połowy października 2020 r. do końca maja 2021 r. (przez 33 tygodnie).

W pierwszym z ww. okresów pracę zdalną zorganizowano w ten sposób, że pracownicy wykonywali powierzone im zadania w sposób zdalny co do zasady przez okres od 2 do 3 następujących po sobie dni w tygodniu. Natomiast w drugim, osoby zatrudnione w WUOZ w Olsztynie (wszystkie) pracowały zdalnie co drugi tydzień, pracownicy Delegatury w Elblągu - co drugi dzień, natomiast w Delegaturze w Ełku nie wprowadzono pracy zdalnej.

(akta kontroli str. 227-233)

W Urzędzie pracę w systemie zdalnym wykonywało w latach 2020-2021 łącznie 39 osób.

W 2020 r. było to 39 spośród 41 osób zatrudnionych w Urzędzie, z czego:
- na podstawie polecenia pracy zdalnej z inicjatywy pracodawcy – 32 osoby,
- na podstawie polecenia pracy zdalnej na wniosek pracownika – dwie osoby,
- zaś na podstawie obu ww. poleceń (zarówno z inicjatywy pracodawcy, jak i na wniosek pracownika) – pięć osób.

Natomiast w 2021 r. pracę w trybie zdalnym świadczyły 33 spośród 41 osób zatrudnionych w Urzędzie, z czego:
- na podstawie polecenia pracy zdalnej z inicjatywy pracodawcy – 22 osoby,
- na podstawie polecenia pracy zdalnej na wniosek pracownika – dwie osoby,
- zaś na podstawie obu ww. poleceń (zarówno z inicjatywy pracodawcy, jak i na wniosek pracownika) – dziewięć osób.

Pracę zdalną w czasie kwarantanny wykonywało trzech pracowników w 2020 r. i ośmiu w 2021 r., zaś w trakcie izolacji - dwie osoby w 2021 r.

Od połowy marca do końca maja 2020 r., w czasie tzw. pierwszej fali pandemii, polecenia pracy zdalnej przekazywano pracownikom w formie harmonogramów pracy zdalnej przygotowywanych przez kierowników wydziałów Urzędu i Delegatur, zatwierdzanych przez Wojewódzkiego Konserwatora Zabytków. Jak wyjaśnił Zastępca WKZ przesyłano je do wiadomości pracownikom mailowo, były one również wyłożone przy liście obecności.

Natomiast podczas tzw. drugiej fali pandemii, od połowy października 2020 r. do końca maja 2021 r., wydawano pisemne polecenia pracy zdalnej (z inicjatywy pracodawcy lub na wniosek pracownika), których wzory wprowadzono Regulaminem pracy zdalnej. Podobnie jak w pierwszym okresie, tworzono harmonogramy.

(akta kontroli str. 227-248)

Kierownicy Wydziałów wyjaśnili, że praca wykonywana zamiennie zdalnie i stacjonarnie nie zaburzyła działalności Urzędu, nie następował przestój realizacji zadań, ani przekraczanie terminów załatwienia spraw. Podali, że pracę zorganizowano tak, aby by na miejscu w Urzędzie były wykonywane wszystkie czynności formalno-prawne związane z procedowaniem postępowań administracyjnych, natomiast praca zdalna (w miejscu zamieszkania) miała charakter wspomagający, polegający na analizie merytorycznej danych dotyczących zabytków zawartych we wnioskach, koniecznych do poprawnego przeprowadzenia postępowania. Poinformowali także, że ograniczony został bezpośredni kontakt z klientem zewnętrznym i wyjazdy w teren, co nie miało jednakże wpływu na realizację zadań, bowiem kontakt z klientem urzędu zachowano poprzez maile i telefony służbowe.

Wojewódzki Konserwator Zabytków podał, że pracownikom, którym polecano świadczenie pracy w sposób zdalny, powierzano do wykonania przede wszystkim takie zadania, które nie wiązały się z potrzebą przetwarzania danych prawnie chronionych. Jednocześnie w Urzędzie stosowany był rotacyjny system polecania pracy zdalnej (pracownicy naprzemiennie z innymi pracownikami pracowali zdalnie lub w siedzibie Urzędu), który – ze względu na zapewnienie systematycznego wykonywania pracy także w siedzibie Urzędu – pozwalał na zapewnienie ciągłości wykonywania także tych zadań Urzędu, które wymagały przetwarzania ww. danych.

(akta kontroli str. 197-205, 249-257)

2.2 Pracownicy Urzędu skierowani do wykonywania pracy zdalnej w latach 2020-2021 zostali zapoznani z zasadami i procedurami dotyczącymi bezpieczeństwa informacji obowiązującymi przy jej wykonywaniu, określonymi w Regulaminie pracy zdalnej oraz wynikającymi z zasad określonych w Polityce ochrony danych osobowych.

Ponadto w okresie pracy zdalnej Inspektor Ochrony Danych rozsyłał mailowo pracownikom Urzędu informacje dotyczące:

- zaleceń Prezesa Urzędu Ochrony Danych Osobowych w zakresie ochrony danych osobowych podczas pracy zdalnej (wiadomość przesłano 19 marca 2020 r.),
- podstawowych zasad bezpieczeństwa informacji w trakcie wykonywania pracy za pośrednictwem elektronicznych środków komunikacji, w tym zaleceń dotyczących przygotowania sprzętu, sposobów komunikacji oraz zdalnego dostępu do danych pracodawcy (informacja przygotowana przez Państwowy Instytut Badawczy NASK we współpracy z Biurem do Walki z Cyberprzestępczością Komendy Głównej Policji oraz Europolem, przesłana 30 kwietnia 2020 r.).

(akta kontroli str. 148-149, 258-265)

2.3 W 2020 r. 8 spośród 39 pracowników wykonujących pracę zdalną korzystało z laptopów zapewnionych przez pracodawcę, a siedmiu z telefonów służbowych. Z prywatnego sprzętu komputerowego korzystało 31 osób, zaś jedna osoba świadczyła pracę bez wykorzystania urządzeń teleinformatycznych.

W 2021 r. spośród 33 pracowników wykonujących pracę zdalną, 12 osób korzystało z laptopów zapewnionych przez pracodawcę, a 5 z telefonów służbowych. Z prywatnego sprzętu komputerowego korzystało 20 osób, zaś jedna świadczyła pracę bez wykorzystania urządzeń teleinformatycznych.

W latach 2020-2021 (do 19 listopada) podczas pracy zdalnej nie użytkowano informatycznych nośników danych[34].

(akta kontroli str. 242-246)

Pełny dostęp do systemów teleinformatycznych Urzędu, realizowany za pośrednictwem kanałów sieci VPN i tzw. pulpitu zdalnego posiadało 5 spośród 8 pracowników wykonujących pracę zdalną z wykorzystaniem służbowych laptopów w 2020 r. i 9 spośród 12 - w 2021 r.

Analiza danych o oprogramowaniu zainstalowanym na pięciu laptopach[35] pozwalających na pełne korzystanie z zasobów Urzędu wykazała że, było to możliwe dzięki zapewnieniu połączenia z siecią Urzędu za pomocą kanału VPN. Pracownicy za pomocą pulpitu zdalnego mieli dostęp do stacji roboczej w Urzędzie i do wszystkich jej zasobów, funkcjonalności i programów, w tym do klienta poczty mailowej. Na ww. laptopach zainstalowano m.in. darmowy pakiet biurowy, oprogramowanie do pakowania i hasłowania plików, program do tworzenia PDF, przeglądarki internetowe, program do nagrywania płyt, a w przypadku sprzętu powierzonego Zastępcy Głównego Księgowego - także certyfikaty do banku.

Pozostali pracownicy korzystający ze sprzętu pracodawcy mieli możliwość korzystania m.in. z programów pakietu biurowego i dostępu do Internetu.

Natomiast osoby świadczące pracę z wykorzystaniem prywatnego sprzętu nie miały dostępu ani do systemu Urzędu, ani do służbowej skrzynki pocztowej. Jak wyjaśnił Informatyk, konfiguracja poczty i przyjęta praktyka uniemożliwiała korzystanie z służbowej poczty elektronicznej na urządzeniach prywatnych.

(akta kontroli str. 177-182, 266-269)

2.4 Oględziny sześciu urządzeń przenośnych[36], ustawień domeny i programów odpowiedzialnych za zarządzanie: programem antywirusowym, kopiami zapasowymi oraz zapisów na stronach internetowych zarządzających ustawieniami Firewalla i sieci Wi-Fi wykazały, że stosowano sprzętowe i programowe środki służące ochronie przetwarzanych informacji, zgodnie z wymogami określonymi w Polityce ochrony danych osobowych[37].

Jak wyjaśnił Informatyk, ww. polityka odnosiła się do danych osobowych, ale wdrożenie opisanych w niej procedur i rozwiązań technicznych zapewniało jednolitą ochronę wszystkich danych przetwarzanych w Urzędzie.

I tak, według stanu na dzień przeprowadzania oględzin stwierdzono, że:

- stosowano mechanizmy umożliwiające zapewnienie odpowiedniego poziomu bezpieczeństwa, zarówno systemów i oprogramowania, jak i przetwarzanych informacji, m.in.:
  - dostęp do systemu operacyjnego komputera zabezpieczano za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora użytkownika oraz hasła o wymaganej złożoności,
  - stosowano systemowe mechanizmy wymuszające okresową zmianę haseł w systemie operacyjnym komputera oraz automatyczną blokadę dostępu w przypadku dłuższej nieaktywności pracy użytkownika,

[34] Tj. płyt CD, DVD, pendrive, kart pamięci, dysków zewnętrznych i innych zewnętrznych nośników informacji.
[35] Numery inwentarzowe: PŚT/697/491, PŚT/788/491, PŚT/789/491, PŚT/790/491, PŚT/791/491.
[36] Były to urządzenia o numerach inwentarzowych PŚT/503/491, PŚT/696/491, PŚT/697/491, PŚT/788/491, PŚT/789/491 oraz PŚT/791/491.
[37] W tym w załącznikach do ww. polityki, w szczególności w zał. nr 10 do pn. *„Podstawowe, minimalne środki techniczne i organizacyjne”* i w zał. nr 7 pn. *„Zasady korzystania z urządzeń przenośnych oraz elektronicznych nośników informacji, na których są przetwarzane dane osobowe”.*

- zainstalowano oprogramowanie antywirusowe, a jego konfiguracja zapewniała ciągłość działania i bieżącą aktualizację,
- wdrożono system Firewall,
- stosowano środki ochrony kryptograficznej danych przesyłanych za pośrednictwem sieci Internet, tj. VPN i zewnętrzny certyfikat SSL,
- na urządzeniach zainstalowano program umożliwiający ustawienie hasła na plikach i folderach,
- wdrożono dwuskładnikowe uwierzytelnianie dostępu do VPN,

- przydzielono odpowiedni poziom uprawnień użytkownikom, tj. nie wyższy niż taki, który umożliwiał wykonanie przydzielonych zadań,
- wdrożono mechanizmy ochrony informacji w przypadku utraty sprzętu (włączono szyfrowanie dysków urządzeń przenośnych),
- zabezpieczano informacje przed utratą lub zniszczeniem (tworzono kopie zapasowe zbiorów danych i programów służących do przetwarzania danych).

(akta kontroli str. 177-182, 270-286)

2.5 Zapisami Regulaminu pracy zdalnej dopuszczono w Urzędzie możliwość wykorzystywania prywatnego sprzętu komputerowego do realizacji zadań służbowych podczas pracy zdalnej. W okresie objętym kontrolą z prywatnych komputerów korzystało: 31 spośród 39 pracowników wykonujących pracę zdalną w 2020 r. oraz 20 spośród 33 - w 2021 r. (do dnia zakończenia kontroli).

(akta kontroli str. 192-196, 242-246)

Nie dopuszczono łączenia się do sieci Urzędu, ani korzystania ze służbowego konta poczty elektronicznej za pomocą prywatnego sprzętu (komputerów przenośnych, stacjonarnych, tabletów lub smartfonów).

Analiza[38] sposobu wykorzystania przez sześciu pracowników prywatnego sprzętu komputerowego w trakcie pracy zdalnej wykazała, że na ww. komputerach:
- tworzono i edytowano dokumenty (np. projekty uzasadnień merytorycznych do pism),
- wysyłano i odbierano wiadomości z użyciem prywatnej skrzynki mailowej, najczęściej do kontaktu z kierownictwem Urzędu, w tym do przesyłania projektów rozstrzygnięć merytorycznych,
- tworzono raporty z wykonania pracy zdalnej,
- korzystano z ogólnodostępnych baz danych, np. Geoportalu, portalu mapowego Narodowego Instytutu Dziedzictwa, Miejskiego Systemu Informacji Przestrzennej Miasta Olsztyna oraz Wojewódzkiej ewidencji zabytków i Rejestru zabytków (zamieszczonych na stronie BIP Urzędu),
- przeglądano zdjęcia zabytków w Internecie.

(akta kontroli str. 177-182, 249-265, 287-314)

W uregulowaniach Urzędu, w tym w Regulaminie pracy zdanej nie określono warunków, jakie powinien spełniać prywatny sprzęt (w tym oprogramowanie), aby można go było wykorzystywać do realizacji zadań służbowych w trakcie pracy zdalnej, nie określono także procedur dotyczących bezpieczeństwa przetwarzanych informacji z użyciem komputerów prywatnych w trakcie pracy zdalnej, ani katalogu czynności dopuszczonych do wykonywania za pośrednictwem prywatnego sprzętu teleinformatycznego, co opisano w punkcie 1.6 niniejszego wystąpienia.

[38] Stwierdzono na podstawie wyjaśnień sześciu pracowników świadczących pracę zdalnie w okresie objętym kontrolą.

Pracownicy wykonujący pracę zdalną z wykorzystaniem prywatnego sprzętu komputerowego zostali zobowiązani do postępowania zgodnie z § 5 Regulaminu pracy zdalnej, tj. do zabezpieczenia dostępu do sprzętu oraz posiadanych danych i informacji przed zniszczeniem i osobami postronnymi.

Stosowano różne metody zapewnienia bezpieczeństwa i poufności danych i informacji służbowych podczas wykorzystywania sprzętu prywatnego w trakcie pracy zdalnej. Według informacji przekazanych przez sześciu pracowników obejmowały one m.in.:

- zabezpieczenia fizyczne (nieudostępnianie komputera innym osobom, zabezpieczenie komputera przed osobami postronnymi po skończonej pracy poprzez zamknięcie komputera w szafce, niewynoszenie laptopa z miejsca zamieszkania),
- zabezpieczanie komputera za pomocą hasła i stosowanie wygaszaczy ekranu,
- korzystanie z programów antywirusowych.

Ww. pracownicy, korzystający ze sprzętu prywatnego, nie zgłosili potrzeby wsparcia technicznego ze strony pracodawcy, do czego mieli prawo zgodnie z § 4 ust. 3 regulaminu.

(akta kontroli str. 3-46, 105-113, 192-196, 287-314)

2.6 W okresie objętym kontrolą pracownicy Urzędu pobierali[39] z jednostki oryginały, kserokopie, skany dokumentów niezbędnych do wykonywania przydzielonych zadań podczas świadczenia pracy w sposób zdalny.

Jak wyjaśnili Zastępca Wojewódzkiego Konserwatora Zabytków oraz pracownicy, z Urzędu w oryginale pobierano projektową dokumentację budowlaną lub programy badań, prac konserwatorskich przy zabytku, tj. załączniki do wniosków składanych do Urzędu. Podali także, że były to opracowania bardzo obszerne, nawet kilkusetstronicowe, zatem zupełnie niezasadne i nieekonomiczne było robienie ich kopii.

Pracownicy pobierający te dokumenty nie podpisywali oświadczeń, o których mowa w §2 pkt 3 Regulaminu pracy zdalnej. Jak wyjaśniła kierownik Wydziału IZNR, posiadano informacje o dokumentach pobieranych do analizy przez pracowników do pracy zdalnej ze sprawozdań tygodniowych składanych przez pracowników.

W Regulaminie pracy zdalnej zobowiązano pracowników do zabezpieczenia danych i informacji znajdujących się na nośnikach, w tym papierowych, przed dostępem osób postronnych oraz przed zniszczeniem. Według wyjaśnień pracowników[40], obowiązek ten realizowano poprzez m.in.: zabezpieczenie przed osobami postronnymi oryginałów / kopii dokumentów służbowych poprzez przechowywanie w jednym miejscu, najczęściej w zamkniętej szafce; odnoszenie ich po pracy zdalnej do Urzędu, niszczenie kopii w niszczarce Urzędu (po ich wykorzystaniu).

(akta kontroli str. 192-196, 287-314, 315-317)

Osoby korzystające ze sprzętu komputerowego zapewnionego przez pracodawcę pobierały skany dokumentów z sieci Urzędu lub przesyłały je na pocztę służbową. Natomiast pracownicy wykorzystujący sprzęt prywatny, przesyłali skany dokumentów na prywatne skrzynki pocztowe. W uregulowaniach Urzędu nie zawarto zasad dotyczących wykorzystania sprzętu prywatnego do celów służbowych, co opisano w punkcie 1.6 niniejszego wystąpienia.

(akta kontroli str. 3-96, 192-196, 287-314)

[39] Stwierdzono na podstawie wyjaśnień siedmiu pracowników świadczących pracę zdalną w okresie objętym kontrolą.
[40] J.w.

2.7 W okresie objętym kontrolą kierownicy Wydziałów i Delegatur Urzędu monitorowali i nadzorowali pracę zdalną podległych im pracowników.

Odbywało się to poprzez kontakt telefoniczny, drogą mailową oraz poprzez weryfikację wykonania zadań służbowych w systemie elektronicznego zarządzania dokumentacją. Kierownicy Wydziałów podali, że z uwagi na to, że wszystkie procedury formalno-prawne prowadzone były w Urzędzie, zapoznawali się z pracą wszystkich pracowników na miejscu poprzez akceptowanie pism wychodzących. Jak wyjaśniła kierownik Wydziału IZNR, pracownicy jej wydziału składali również cotygodniowe sprawozdania z pracy zdalnej.

Zastosowane metody monitorowania i nadzorowania pracy zdalnej obejmowały także zagadnienia dotyczące bezpieczeństwa informacji. Jak wyjaśnili Kierownicy Wydziałów, oprócz zapoznania pracowników z zasadami bezpieczeństwa i poufności podczas pracy zdalnej określonych w Regulaminie pracy zdalnej, część zasad określana była na bieżąco i bezpośrednio ustnie przekazywana pracownikom.

(akta kontroli str. 249-257, 287-314, 318-348)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

Wdrożone i stosowane rozwiązania organizacyjne i techniczne służyły zapewnieniu bezpieczeństwa danych osobowych w pracy zdalnej. Wprowadzona organizacja pracy (m.in. dostęp do sieci Urzędu wyłącznie za pomocą służbowego sprzętu komputerowego, założenie przekazywania pracownikom korzystającym ze sprzętu prywatnego zadań niewymagających przetwarzania danych chronionych) minimalizowała ryzyko naruszenia bezpieczeństwa danych osobowych. Stosowano sprzętowe i programowe środki służące ochronie informacji podnoszące poziom ich bezpieczeństwa, zgodnie z zasadami przyjętymi w Urzędzie. Monitorowano i nadzorowano pracę zdalną, a zastosowane metody obejmowały zagadnienia związane z bezpieczeństwem informacji.

Należy jednak zauważyć, że w Urzędzie nie ustalono, a w konsekwencji nie wdrożono, zasad dotyczących korzystania z komputerów prywatnych podczas pracy zdalnej.

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, ustanowienie i wdrożenie systemu zarządzania bezpieczeństwem informacji (w tym polityki bezpieczeństwa informacji) spełniającego wymogi określone w rozporządzeniu w sprawie KRI.
2. Opracowanie i wdrożenie zasad korzystania z komputerów prywatnych podczas pracy zdalnej.
3. Doprecyzowanie w Regulaminie pracy zdalnej zapisów dotyczących oświadczeń składanych przez pracownika w przypadku udostępnienia mu dokumentacji w wersji papierowej w celu wykonywania pracy zdalnej.

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 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.

Najwyższa Izba Kontroli
Delegatura w Olsztynie

Kontroler
Olga Ratkiewicz
Starszy inspektor kontroli państwowej

.....
podpis

Dyrektor
z up.
Piotr Wanic
Wicedyrektor

.....
podpis