NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie

LOL.410.017.11.2021

Sławomir Ambroziak
Wójt Gminy Jedwabno
Urząd Gminy w Jedwabnie
ul. Warmińska 2
12-122 Jedwabno

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 Gminy w Jedwabnie, ul. Warmińska 2, 12-122 Jedwabno (dalej: Urząd)
Kierownik jednostki kontrolowanej	Sławomir Ambroziak, Wójt Gminy Jedwabno, na stanowisku od 20 listopada 2018 r. (dalej: Wójt)
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 30 listopada) z uwzględnieniem zdarzeń wcześniejszych, jeżeli miały one wpływ na kontrolowane obszary działalności.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Olsztynie
Kontrolerzy	1. Justyna Lis, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LOL/108/2021 z 9 września 2021 r. 2. Joanna Łukasik, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/123/2021 z 11 października 2021 r. (akta kontroli str. 1-3)

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

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

W Urzędzie określono i przypisano odpowiedzialność za bezpieczeństwo informacji pracownikom oraz wyznaczono Inspektora Ochrony Danych (dalej: IOD). W obowiązującej w Urzędzie polityce dotyczącej bezpieczeństwa przetwarzania danych osobowych[3] określono zasady: postępowania z nośnikami i urządzeniami przenośnymi, wynoszenia aktywów z Urzędu, przesyłania informacji oraz zarządzania incydentami związanymi z bezpieczeństwem informacji. Zapoznano pracowników z zasadami bezpieczeństwa informacji przy przetwarzaniu danych osobowych.

Po przeprowadzonych analizach ryzyka bezpieczeństwa informacyjnego oraz pracy zdalnej wprowadzano regulacje doprecyzowujące obowiązujące procedury bezpieczeństwa informacji w Urzędzie. W marcu 2021 r. wprowadzono regulamin pracy zdalnej[4], w którym określono: warunki podjęcia pracy zdalnej, warunki jakie

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

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

[3] Zarządzenie Nr 80/2018 Wójta Gminy w Jedwabnie z 25 lipca 2018 r. w sprawie wprowadzenia "Polityki bezpieczeństwa w Urzędzie Gminy Jedwabno", Zarządzenie nr 116/2018 Wójta Gminy Jedwabno z 15 listopada 2018 r. w sprawie zmiany zarządzenia nr 80/2018 Wójta Gminy Jedwabno z dnia 25 lipca 2018 r. w sprawie wprowadzenia „Polityki Bezpieczeństwa w Urzędzie Gminy w Jedwabnie", Zarządzenie nr 99/2020 Wójta Gminy Jedwabno z 12 października 2020 r. w sprawie wprowadzenia zmian w "Polityce Bezpieczeństwa w Urzędzie Gminy w Jedwabnie"; dalej: PBDO lub Polityka bezpieczeństwa przetwarzania danych osobowych.

[4] Zarządzenie Nr 20/2021 Wójta Gminy w Jedwabnie z 15 marca 2021 r. w sprawie regulaminu pracy zdalnej w Urzędzie Gminy w Jedwabnie; dalej: Regulamin pracy zdalnej.

musi spełniać miejsce jej świadczenia oraz zasady ochrony informacji i danych osobowych.

Wdrożone rozwiązania organizacyjne i techniczne służyły zapewnieniu bezpieczeństwa danych osobowych w pracy zdalnej.

W toku kontroli stwierdzono jednak nieprawidłowości, które dotyczyły:

- nieopracowania, nieustanowienia i niewdrożenia w Urzędzie Systemu Zarządzania Bezpieczeństwem Informacji[5] (w tym Polityki Bezpieczeństwa Informacji[6]), 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[7], obejmujących swoim zakresem wszystkie kategorie przetwarzanych w Urzędzie informacji,
- nieprzestrzegania określonych w Urzędzie zasad bezpieczeństwa informacji w pracy zdalnej, tj. uregulowań w zakresie zasad postępowania z pamięciami przenośnymi[8] oraz obowiązków wynikających z Regulaminu pracy zdalnej.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[9] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. Do 30 listopada 2021 r., tj. dnia zakończenia kontroli, w Urzędzie nie opracowano i nie wdrożono SZBI (w tym nie wprowadzono PBI), spełniającego wymogi określone przepisami § 20 ust. 2 rozporządzenia KRI, do czego zobowiązywał § 20 ust. 1 ww. rozporządzenia. Zagadnienie to opisano w sekcji „Stwierdzone nieprawidłowości".

W okresie objętym kontrolą w Urzędzie funkcjonowały natomiast procedury będące elementami Polityki bezpieczeństwa informacji:

- Polityka bezpieczeństwa przetwarzania danych osobowych,
- Zasady postępowania z pamięciami przenośnymi,
- Procedury informatyczne[10],
- Zasady postępowania z informacją niejawną[11],
- System Elektronicznego Obiegu Dokumentów EDICTA[12],
- Regulamin pracy zdalnej.

(akta kontroli str. 4-415)

---

[5] Dalej: SZBI.

[6] Dalej: PBI.

[7] Dz.U. z 2017 r., poz. 2247, dalej: rozporządzenie KRI.

[8] Zarządzenie Nr 4/2019 Wójta Gminy w Jedwabnie z 16 stycznia 2019 r. w sprawie wprowadzenia w Urzędzie Gminy Jedwabno dokumentu wewnętrznego określającego zasady postępowania z pamięciami przenośnymi oraz procedura „Zasady postępowania z pamięciami przenośnymi" ujęta w załączniku nr 3 do Polityki bezpieczeństwa przetwarzania danych osobowych (dalej: Zasady postępowania z pamięciami przenośnymi).

[9] 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.

[10] Zarządzenie Nr 46/2019 Wójta Gminy Jedwabno z 20 maja 2019 r. w sprawie wprowadzenia procedur informatycznych.

[11] Zarządzenia Wójta dotyczące: powołania Pełnomocnika ds. Informacji Niejawnych, zatwierdzenia Planu Ochrony Informacji Niejawnych, sposobu i trybu przetwarzania informacji niejawnych, wyznaczenia Inspektora Bezpieczeństwa Teleinformatycznego, utworzenia Pionu Ochrony w Urzędzie.

[12] Zarządzenie nr 95/2019 Wójta Gminy Jedwabno z 30 września 2019 r. w sprawie wprowadzenia Systemu Elektronicznego Obiegu Dokumentów EDICTA w Urzędzie Gminy w Jedwabnie.

W toku przeprowadzonych 16 listopada 2021 r. oględzin ewidencji zasobów informatycznych Urzędu (dalej: zasoby IT) stwierdzono, że na komputerze Informatyka Urzędu prowadzona była w wersji elektronicznej aktualna inwentaryzacja zasobów IT Urzędu z wykorzystaniem specjalistycznego oprogramowania, która zawierała dane o komputerach, serwerach, urządzeniach sieciowych, drukarkach i oprogramowaniu będących na stanie Urzędu.

W Urzędzie prowadzono także ewidencję systemów teleinformatycznych używanych do realizacji zadań publicznych, w której dokonano oceny istotności oraz przypisano ważność zasobów informacyjnych Urzędu.

Urząd posiadał wykaz zasobów informacyjnych Urzędu zinwentaryzowanych wg stanu na 2019 r. Dokument zawierał pięć pozycji odnoszących się do różnych kategorii danych osobowych w następujących obszarach: obywatele[13], dziennik korespondencji[14], monitoring[15], pracownicy i byli pracownicy[16], kontrahenci i pracownicy kontrahentów[17]. Wykaz ten nie zawierał wszystkich rodzajów informacji przetwarzanych w Urzędzie, np.: danych o sytuacji ekonomiczno-finansowej Urzędu, informacji dotyczących umów oraz zamówień, wyników audytów i kontroli, informacji organizacyjnych związanych z bieżącym funkcjonowaniem Urzędu. W ww. wykazie odniesiono się tylko do rodzajów informacji związanych z ochroną danych osobowych.

Wójt wyjaśnił, że dokument ten nie był aktualizowany od 2019 roku, gdyż zawierał szeroki katalog informacyjny, ujmujący pełne spektrum informacji przetwarzanych w Urzędzie.

(akta kontroli str. 416-429)

W dokumencie PBDO określono politykę bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych oraz politykę bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych.

W ramach PBDO dedykowanej zbiorom papierowym określono m.in. następujące zasady:

- zakaz wynoszenia dokumentów zawierających dane osobowe poza obszar przetwarzania danych,
- fizycznego i organizacyjnego zabezpieczania dokumentów w formie papierowej przez nieuprawnionym dostępem, kradzieżą, zmianą, utratą lub zniszczeniem.

W ramach PBDO, w części dedykowanej systemom informatycznym, określono m.in. zasady:

- zarządzania uprawnieniami użytkowników[18],
- postępowania z nośnikami[19],
- wynoszenia aktywów i ich bezpieczeństwa poza siedzibą (sprzęt, nośniki)[20],

[13] Z następującymi kategoriami informacji: imię (imiona), nazwisko, PESEL, adres, adres e-mail, imiona rodziców, NIP, adres prowadzenia działalności, adres posesji, rodzaj gruntów, stan majątkowy.

[14] Z następującymi kategoriami informacji: imię (imiona), nazwisko, PESEL, adres, adres e-mail, adres prowadzenia działalności.

[15] Z następującymi kategoriami informacji: wizerunek.

[16] Z następującymi kategoriami informacji: dane określone w art. 22 Kodeksu pracy oraz w ustawie o pracownikach samorządowych.

[17] Z następującymi kategoriami informacji: dane kontaktowe.

[18] Procedura przygotowania stanowiska pracy, Procedura nadawania odbierania uprawnień, Procedura blokowania, odblokowania i usuwania kont użytkowników (załączniki 1-3 do Polityki bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych).

[19] Procedura zarzadzania nośnikami, Zasady postępowania z pamięciami przenośnymi (załączniki 8 i 17 do Polityki bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych)

- pozostawiania sprzętu bez opieki[21],
- zabezpieczenia przed szkodliwym oprogramowaniem[22],
- zabezpieczenia sieci[23],
- przesyłania informacji i zabezpieczenia wiadomości w formie elektronicznej[24],
- zarządzania incydentami związanymi z bezpieczeństwem informacji[25].

Powyższe zasady uregulowano poprzez 22 procedury zawarte w załączniku nr 3 do PBDO wskazując, że ww. załącznik to odpowiednik SZBI w Urzędzie opracowany w oparciu o wytyczne zawarte m.in. w rozporządzeniu KRI. Jednak we wstępie do ww. polityki zdefiniowano cel tejże polityki, jako ustanowienie jednolitych reguł postepowania w zakresie ochrony danych osobowych, tj. zasad bezpiecznego przetwarzania tych danych. Ponadto w PBDO określono także cel dla załącznika nr 3 (polityki bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych), jako zdefiniowanie zasad zarządzania i wskazanie środków zabezpieczających dla systemów informatycznych przetwarzających dane osobowe oraz spełnienie wymagań RODO oraz rozporządzenia KRI.

(akta kontroli str. 13-360)

1.2. Wójt w PBDO określił odpowiedzialność i uprawnienia osób pełniących istotną rolę w zapewnieniu bezpieczeństwa informacji w zakresie danych osobowych.

Zgodnie z ww. polityką, rolą Wójta, jako Administratora Danych Osobowych (dalej: ADO) było: decydowanie o celach i środkach przetwarzania danych osobowych, przyznawanie upoważnień do przetwarzania danych osobowych, szacowanie ryzyka dla bezpieczeństwa danych osobowych, monitorowanie i sprawdzanie przestrzegania przyjętych procedur ochrony danych osobowych.

Administratora Systemów Informatycznych (dalej: ASI) wskazano, jako upoważnionego do zarządzania systemem informatycznym i odpowiedzialnego za bezpieczeństwo tego systemu i jego ochronę przed zagrożeniami. Do jego zadań należało m.in.: przygotowanie stanowisk komputerowych do eksploatacji i przeprowadzanie szkoleń stanowiskowych dla pracowników Urzędu, nadawanie i odbieranie uprawnień użytkownikom systemów, tworzenie i przechowywanie kopii bezpieczeństwa systemów komputerowych, wdrożenie i zarządzanie oprogramowaniem antywirusowym w Urzędzie, zarządzanie komunikacją w lokalnych sieciach komputerowych oraz zapewnienie ciągłego, bezawaryjnego i bezpiecznego ich funkcjonowania, dokonywanie bieżących przeglądów i konserwacja systemów oraz nośników informacji służących do przetwarzania danych osobowych, analiza incydentów informatycznych, zarządzanie kluczami kryptograficznymi i certyfikatami, tworzenie instrukcji doprecyzowujących istotne czynności administracyjne w obszarze bezpieczeństwa przetwarzania danych.

---

[20] Zasady postepowania z pamięciami przenośnymi, Procedura bezpieczeństwa komputerów przenośnych (załączniki nr 17 i 12 do Polityki bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych).

[21] Procedura rozpoczynania, zawieszania i kończenia pracy w systemach informatycznych, Zasady postępowania z pamięciami przenośnymi, Procedura bezpieczeństwa komputerów przenośnych (załączniki nr do 6, 17 i 12 Polityki bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych).

[22] Procedura zabezpieczenia przed szkodliwym oprogramowaniem (załącznik nr 9 do Polityki bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych).

[23] Procedura bezpieczeństwa sieci teleinformatycznej (załącznik nr 10 do Polityki bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych).

[24] Procedura korzystania z Internetu i poczty elektronicznej, Animizacja, pseudoanonimizacja oraz szyfrowanie (załącznik nr 11 i 15 do Polityki bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych).

[25] Procedura zgłaszania incydentów informatycznych (załącznik nr 18 do Polityki bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych).

ASI posiadał także upoważnienie od ADO, w którym określono, że do jego obowiązków w zakresie ochrony danych osobowych należało wdrożenie i nadzór nad prawidłową realizacją w imieniu ADO Polityki bezpieczeństwa przetwarzania danych osobowych, a w szczególności: realizacja obowiązków wynikających z rozporządzenia KRI, przeprowadzanie i koordynowanie wykonania inwentaryzacji zasobów informatycznych oraz nadzór nad zasobami, pomoc przy wykonywaniu szacowania ryzyka poprzez identyfikację podatności elementów mających wpływ na działanie systemu informatycznego oraz zalecanie i sugerowanie stosowania odpowiednich zabezpieczeń, które te podatności mogą ograniczyć lub wyeliminować, nadawanie i odbieranie dostępów do konkretnych zasobów informatycznych.

Pracownicy Urzędu upoważnieni do przetwarzania danych osobowych zostali wskazani w PBDO, jako odpowiedzialni za bezpieczeństwo przetwarzanych danych osobowych oraz zgłaszanie propozycji do aktualizacji tego dokumentu.

(akta kontroli str. 16-360, 430)

W okresie objętym kontrolą 29 pracowników Urzędu posiadało pisemne upoważnienie od Wójta do przetwarzania danych osobowych. Pracownicy ci złożyli oświadczenia o:

- zapoznaniu się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Urzędzie,
- zobowiązaniu się do stosowania ww. przepisów i procedur,
- zobowiązaniu się do zachowania tajemnicy danych osobowych oraz sposobów ich zabezpieczania.

(akta kontroli str. 431-436)

1.3. Wójt, działając na podstawie art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[26], wyznaczył[27] w 2018 r. IOD oraz powierzył mu zadania do realizacji zgodnie z art. 39 ust. 1 Rozporządzenia 679/2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[28].

IOD spełniał wymagania określone w art. 37 ust. 5 RODO, tzn. posiadał kwalifikacje potwierdzające jego wiedzę i umiejętności na temat prawa i praktyk w dziedzinie ochrony danych osobowych.

Do głównych zadań IOD należało:

- identyfikacja i aktualizacja zbiorów danych osobowych,
- przeprowadzanie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych oraz monitorowanie jej wykonania,
- weryfikacja klauzul zgód na przetwarzanie danych osobowych oraz klauzul obowiązku informacyjnego,
- analiza stosowanych techniczno-organizacyjnych środków ochrony, bezpieczeństwa fizycznego oraz informatycznego, związanych z przetwarzaniem danych osobowych,
- prowadzenie rejestru czynności przetwarzania danych osobowych,
- zarządzanie upoważnieniami do przetwarzania danych osobowych i ewidencją osób upoważnionych,
- opiniowanie wzorów dokumentów dotyczących ochrony danych osobowych,

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

[27] Zarządzeniem Nr 54/2018 Wójta Gminy Jedwabno z dnia 29 maja 2018 r. w sprawie wyznaczenia Inspektora Ochrony Danych w Urzędzie Gminy w Jedwabnie.

[28] Dz.U.UE.L.2016.119.1; dalej: RODO.

- prowadzenie szkoleń dla pracowników z zakresu ochrony danych osobowych.

Osoba pełniąca funkcję IOD przejęła od 1 marca 2020 r. również zadania Informatyka Urzędu i ASI.

(akta kontroli str. 437-451)

1.4. Do PBDO z 12 października 2020 r.[29] dodano nowy załącznik nr 17 pn. „Zasady postępowania z pamięciami przenośnymi", w którym określono sposób przyznawania i używania pamięci przenośnych oraz zasady krótkotrwałego przenoszenia informacji, zawierających dane osobowe sporządzane na podstawie informacji zawartych w zbiorach osobowych prowadzonych w systemach informatycznych w Urzędzie. Wcześniej, tj. od 16 stycznia 2019 r. zasady te regulowało Zarządzenie Wójta nr 4/2019 w sprawie wprowadzenia w Urzędzie Gminy w Jedwabnie dokumentu wewnętrznego określającego zasady postępowania z pamięciami przenośnymi.

Oba dokumenty posiadały tożsame regulacje w następujących kwestiach:

- konieczność wnioskowania przez pracownika o przyznanie służbowej pamięci przenośnej,
- konieczność złożenia przez pracownika oświadczenia o otrzymaniu pamięci przenośnej i zapoznaniu się z zasadami postępowania z zewnętrznym nośnikiem danych,
- konieczność zaszyfrowania pamięci przenośnej,
- konieczność zdania pamięci przenośnej ASI w przypadku rozwiązania umowy o pracę, uszkodzenia pamięci,
- konieczność pisemnego powiadomienia ASI i IOD w przypadku utracenia pamięci przenośnej,
- konieczność nadania pamięciom przenośnym unikalnego numeru ewidencyjnego przez ASI,
- dedykowanie pamięci przenośnych do przechowywania i przenoszenia wyłącznie danych zawierających informacje służbowe, przechowywane wyłącznie w obszarze szyfrowanego dysku,
- zakaz stosowania pamięci przenośnych do wykonywania kopii zapasowych danych przetwarzanych na twardych dyskach komputerów służbowych,
- zakaz przenoszenia danych służbowych za pomocą pamięci przenośnych poza teren Urzędu, z wyjątkiem gdy posiadało się zgodę Administratora,
- obowiązek sprawdzania pamięci przenośnej oprogramowaniem antywirusowym,
- obowiązek usuwania danych z pamięci po ich wykorzystaniu,
- obowiązek ochrony pamięci przenośnej przed utratą i uszkodzeniem np. na skutek uderzenia, wystawienia na działanie wysokich temperatur, wilgoci, silnych pól magnetycznych.

(akta kontroli str. 178-367)

W PBDO w części dotyczącej przetwarzania danych w zbiorach papierowych określono zasady postępowania z dokumentami w formie papierowej, a mianowicie:

- określono środki fizyczne zabezpieczenia danych osobowych (systemy alarmowe, zamykane na klucz pokoje i szafy) oraz zasady zarządzania informacją (zasada zamkniętego pomieszczenia, zasada nadzorowanych dokumentów, zasada czystego biurka, zasada czystych drukarek, zasada czystego kosza),

[29] Zarządzenie Nr 99/2020 Wójta Gminy w Jedwabnie z 12 października 2020 r. w sprawie wprowadzenia zmian w „Polityce Bezpieczeństwa w Urzędzie Gminy w Jedwabnie".

- określono środki organizacyjne zabezpieczenia danych osobowych (ewidencja osób upoważnionych do przetwarzania danych osobowych, cykliczne szkolenia dotyczące wymogu ochrony danych osobowych);
- zakaz wynoszenia dokumentów zawierających dane osobowe poza obszar przetwarzania danych, za wyjątkiem uzyskania zgody ADO lub realizacji obowiązków służbowych,
- określono zasady aktualizacji, usuwania i niszczenia danych osobowych przetwarzanych w formie papierowej.

(akta kontroli str. 16-360)

W PBDO określono także procedurę bezpiecznej eksploatacji komputerów przenośnych (załącznik nr 12), tj.:

- wskazano użytkownika sprzętu, jako osobę odpowiedzialną za bezpieczeństwo komputera przenośnego przed zgubieniem, kradzieżą, zniszczeniem, uszkodzeniem, złośliwym oprogramowaniem,
- zakazano pozostawiania sprzętu komputerowego bez nadzoru w miejscach publicznych,
- zakazano udostępniania komputera osobom nieupoważnionym,
- zakazano jednoczesnego podłączania komputera przenośnego podłączonego do lokalnej sieci komputerowej z inną siecią zewnętrzną,
- wskazano ASI, jako jedyną osobą uprawnioną do instalowania dodatkowych urządzeń zewnętrznych na komputerze przenośnym,
- zobowiązano każdego użytkownika komputera przenośnego do pracy na własnym koncie w celu zachowania rozliczalności działań podejmowanych w systemie,
- wprowadzono obowiązek zapisywania danych osobowych przechowywanych na przenośnej stacji roboczej w zaszyfrowanym zasobie,
- wprowadzono zabezpieczenia programowe na poziomie BIOS-u (zaszyfrowane dyski, blokowanie opcji „BOOT") oraz automatyczny wygaszacz chroniony hasłem.

(akta kontroli str. 16-360)

1.5. Zasady dostępu i korzystania z zasobów Internetu oraz poczty elektronicznej ujęto w PBDO w systemach informatycznych - załącznik nr 11 pn. „Procedura korzystania z Internetu i poczty elektronicznej". Uregulowano w niej następujące kwestie:

- wykorzystanie Internetu i poczty elektronicznej tylko do celów służbowych i po uzyskaniu przez pracownika uprawnień do korzystania z systemów informatycznych Urzędu,
- przekazywanie informacji chronionych za pomocą poczty elektronicznej może odbywać się tylko po ich zabezpieczeniu (np. hasłem zabezpieczającym, szyfrowanie),
- wprowadzono zakaz udostępniania osobistego konta innym osobom w celu przeglądania Internetu lub przesyłania poczty,
- wprowadzono zakaz pobierania, uruchamiania i rozpowszechniania plików niezwiązanych z działalnością służbową oraz plików niewiadomego pochodzenia,
- zobowiązano użytkownika poczty elektronicznej do: codziennego kontrolowania poczty, wysyłania wyłącznie wiadomości podpisanych i z opisanym polem tematu, stosowania programów kompresujących w przypadku przesyłania dużych plików.

W „Procedurze przygotowania stanowiska pracy” (załącznik nr 1 do ww. polityki) określono, że ASI przygotowuje stanowisko komputerowe do pracy dla nowozatrudnionego pracownika i w razie potrzeby przeprowadza szkolenie stanowiskowe. Zabroniono użytkownikom stanowisk komputerowych do ingerowania w konfigurację sprzętową stacji roboczych, samodzielnego instalowania oprogramowania (w tym dodatków do przeglądarek) oraz używania aplikacji w wersji portable (programów niewymagających instalacji, przenoszonych na różnych nośnikach pamięci). Ponadto wskazano, że każda stacja robocza musi posiadać oprogramowanie antywirusowe. W celu zabezpieczenia wewnętrznej sieci Urzędu przed zagrożeniami pochodzącymi z sieci Internet wprowadzono także „Procedurę usuwania oprogramowania typu BOTNET” (załącznik nr 20 do ww. polityki).

(akta kontroli str. 16-360)

1.6. W PBDO w części dedykowanej systemom informatycznym uregulowano także kwestię zarządzania incydentami związanymi z bezpieczeństwem informacji. Zasady te ujęto w załączniku nr 18 do ww. polityki pn. „Procedura zgłaszania incydentów informatycznych”, tj.:

- zdefiniowano incydent bezpieczeństwa, jako niepożądane zdarzenie związane z dostępem do Internetu lub seria zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji,
- wskazano ASI, jako odpowiedzialnego za realizację tej procedury: prowadzenie ewidencji incydentów, ich klasyfikację oraz zgłaszanie do CSIRT NASK[30].

Do 19 listopada 2021 r. w Urzędzie nie prowadzono wpisów w ewidencji incydentów bezpieczeństwa.

Wójt wyjaśnił, że do 19 listopada 2021 r. nie zidentyfikowano incydentu, który klasyfikowałby się jako incydent informatyczny warunkujący wpis w tym rejestrze. W dniu 19 listopada 2021 r. nastąpiła eskalacja prób nieautoryzowanego dostępu do strony www.jedwabno.pl i ten incydent został zaewidencjonowany i zgłoszony do CSIRT NASK. Powyższy incydent wpisano do ewidencji incydentów w Urzędzie.

Ponadto PBDO zawierała również „Procedurę postępowania w przypadku naruszenia bezpieczeństwa danych” (załącznik nr 15). W Urzędzie prowadzono rejestr naruszeń ochrony danych osobowych zgodnie z ww. procedurą. Na dzień 17 listopada 2021 r. ww. rejestr posiadał jeden wpis dotyczący naruszenia ochrony danych osobowych w 2019 r.

(akta kontroli str. 16-360, 466-467, 537-546)

1.7. Od 15 marca 2021 r. w Urzędzie obowiązywał Regulamin pracy zdalnej, w którym określono:

- warunki podjęcia pracy zdalnej,
- warunki jakie musi spełniać miejsce jej świadczenia, w tym w zakresie BHP,
- zasady ochrony informacji i danych osobowych.

Obowiązki pracownika wykonującego pracę zdalną, związane z zasadami zapewnienia bezpieczeństwa informacji polegały na:

- zabezpieczeniu dostępu do sprzętu służbowego oraz posiadanych danych i informacji (w tym także znajdujących się na nośnikach papierowych) przed

[30] CSIRT NASK przyjmuje, analizuje i podejmuje działania i koordynuje reakcje na incydenty dotyczące bezpieczeństwa cywilnej cyberprzestrzeni RP zgłaszane przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny i osoby prywatne oraz na incydenty związane z nielegalnymi treściami publikowanymi w Internecie i zagrażającymi bezpieczeństwu dzieci oraz odpowiada za monitorowanie zagrożeń internetowych i stanu cyberbezpieczeństwa na poziomie sektorowym i krajowym.

osobami postronnymi, w tym wspólnie z nimi zamieszkującymi, oraz zniszczeniem,
- przestrzeganiu postanowień PBDO wraz z dokumentami powiązanymi,
- złożeniu oświadczenia o zapoznaniu się treścią ww. regulaminu i zasadami ochrony danych osobowych w trakcie pracy zdalnej.

Regulamin dopuszczał wykonywanie pracy zdalnej przy użyciu narzędzi lub materiałów niezapewnionych przez pracodawcę pod warunkiem poszanowania przez pracownika przetwarzanych przez niego informacji poufnych i innych tajemnic prawnie chronionych, w tym tajemnic zakładu pracy lub danych osobowych, a także informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. W przypadku kwestii nieujętych w ww. regulaminie zastosowanie miały regulacje PBDO wraz z dokumentami powiązanymi.

Wójt wyjaśnił, że nie wprowadzono regulacji dotyczących prywatnego sprzętu komputerowego używanego przez pracownika w trakcie pracy zdalnej, ponieważ w opinii radcy prawnego (opiniującego projekt przedmiotowych regulacji) nie było podstaw prawnych do stosowania wymogów w stosunku do sprzętu prywatnego. W ramach zorganizowanej w latach 2020-2021 pracy zdalnej przyjęto model dostępu do danych, z wykorzystywaniem zewnętrznego oprogramowania bazującego na zasadzie pulpitu zdalnego z zablokowanymi opcjami wydruku i kopiowania oraz szyfrowaniem łączności pomiędzy komputerami. Ponadto wszystkie urządzenia, które opuszczały teren Urzędu były szyfrowane. Pracownik wysyłając informację do interesanta, w przypadku zawarcia w nim danych osobowych, miał obowiązek zaszyfrowania pliku zawierającego informację, a hasło przesłać odbiorcy innym kanałem komunikacyjnym, zgodnie z przyjętą PBDO. W przypadku przesyłania informacji do firm zewnętrznych, z reguły stosowana była droga tradycyjna. W zakresie dokumentów w formie papierowej nie było i nie ma do dnia dzisiejszego pozwolenia na wynoszenie dokumentów z Urzędu, czy to w postaci kopii czy też oryginałów.

Ponadto Wójt wyjaśnił, że po wprowadzeniu przez ustawodawcę przepisów mających na celu przeciwdziałanie COVID-19[31], które dały możliwość wydawania przez pracodawcę poleceń pracy zdalnej i kierowania pracowników na pracę zdalną, wydał polecenie ustne o wykonywaniu pracy zdalnej przez pracowników Urzędu w systemie rotacyjnym. W związku z brakiem przepisów ustawowych, co do określenia zasad wykonywania pracy zdalnej oraz brakiem doświadczenia Urzędu, co do zaistniałej w wyniku pandemii sytuacji, polecenia ustne o wykonaniu pracy zdalnej wydawały się być najszybszym i najelastyczniejszym sposobem dostosowania się do sytuacji pandemicznej. Rok 2020 został potraktowany jako okres przejściowy, z nadzieją że w 2021 roku pandemii już nie będzie, a jednocześnie pojawią się nowe regulacje prawne w zakresie pracy zdalnej. W związku z tym, że pandemia trwa nadal, została podjęta decyzja o opracowaniu dokumentu zawierającego zasady pracy zdalnej i w marcu 2021 r. wydano zarządzenie w sprawie regulaminu pracy zdalnej.

(akta kontroli str. 408-415, 531-546)

1.8. Wszyscy pracownicy Urzędu, którzy w okresie 2020-2021 posiadali upoważnienie do przetwarzania danych osobowych, złożyli oświadczenia o zapoznaniu się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi.

[31] Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-10, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2020, poz.1842).

Większość pracowników Urzędu zapoznała się również z Regulaminem pracy zdalnej, co potwierdzono podpisami na liście pracowników, którzy zapoznali się z ww. regulacją (szerzej opisano w punkcie 2.2. wystąpienia).

W okresie objętym kontrolą w Urzędzie przeprowadzono także szkolenia z zakresu bezpieczeństwa informacji, tj.:

- w 2020 r.:
  - jeden nowozatrudniony pracownik administracyjny przeszkolony został do pracy na stacji roboczej w zakresie bezpiecznego posługiwania się komputerem, zasad tworzenia haseł, zasad korzystania z zewnętrznych nośników informacji, obsługi aplikacji PUMA,
  - 18 pracowników Urzędu, którzy kierowani byli do pracy zdalnej, zostało przeszkolonych z oprogramowania służącego do pracy przy użyciu pulpitu zdalnego oraz konfiguracji stanowiska do korzystania z aplikacji do obsługi pulpitu zdalnego;
- w 2021 r.:
  - 20 pracowników administracyjnych przeszkolono z zakresu zasad postępowania z hasłami, pocztą elektroniczną i korzystania z Internetu w obszarze ochrony danych osobowych,
  - 20 pracowników wykonujących pracę zdalną przeszkolono w zakresie zasad dostępu do sieci Urzędu oraz wykorzystywania udostępnionego oprogramowania.

(akta kontroli str. 408-415, 431-432, 452-465)

1.9. W okresie objętym kontrolą w Urzędzie dokonano aktualizacji procedur dotyczących ochrony danych osobowych. Zarządzeniem Nr 99/2020 Wójta Gminy w Jedwabnie z 12 października 2020 r. ws. wprowadzenia zmian w "Polityce bezpieczeństwa w Urzędzie Gminy w Jedwabnie" dokonano zmiany nazwy ww. polityki na „Polityka Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Jedwabnie”, dodano także zapisy dotyczące postępowania z pamięciami przenośnymi oraz doprecyzowano zapisy dotyczące procedur informatycznych (wcześniej kwestie te były uregulowane odrębnymi zarządzeniami Wójta).

„Raport z audytu bezpieczeństwa informacji w Urzędzie Gminy w Jedwabnie” został sporządzony 23 listopada 2020 r. przez Informatyka oraz Sekretarza Urzędu. Jednym z elementów ww. raportu była ocena ryzyka wykonana przez ASI, z której wynikała konieczność podjęcia następujących działań: opracowanie planu ciągłości działania, wytworzenie procedur wymiany danych i informacji, wytworzenie wymagań bezpieczeństwa na stanowisku pracy, przeszkolenie pracowników z zakresu bezpieczeństwa informacji.

Wójt wyjaśnił, że podjęto wszystkie działania, które zaplanowano w celu minimalizacji zidentyfikowanego ryzyka. Działania te implikowały wytworzenie dokumentów realizacyjnych do Polityki bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych, które dotyczyły: zarzadzania serwerami lokalnymi, komputerami w sieci lokalnej Urzędu, systemem informatycznym PUMA, EDICTA i EUSŁUGI, unormowania zasad zarządzania w przypadku awarii. Do końca 2021 r. zaplanowano przeprowadzenie kolejnego audytu bezpieczeństwa informacji w Urzędzie.

Ponadto w 2020 r. i 2021 r. ASI przygotował analizy ryzyka dla pracy zdalnej[32], w których wskazał potencjalne zagrożenia związane z pracą zdalną polegające na: nieupoważnionym dostępie do danych osobowych, niepożądanej modyfikacji danych osobowych oraz zniknięciu danych osobowych. Wskazano, iż działania minimalizujące wskazane ryzyko to szkolenia pracowników, za które odpowiadał ASI. Ponadto w ww. analizach ryzyka zaprezentowano także zasady organizacji pracy zdalnej i ich wpływ na bezpieczeństwo przetwarzania danych osobowych.

Wójt stwierdził, że przedstawione analizy ryzyka dla pracy zdalnej oraz wnioski z nich płynące wpłynęły na podejmowane przez niego decyzje w zakresie organizacji pracy Urzędu w warunkach pandemii, w tym organizacji pracy zdalnej w Urzędzie.

(akta kontroli str. 7-10, 468-530, 547-555)

Stwierdzone nieprawidłowości

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

W okresie od 1 stycznia 2020 r. do 30 listopada 2021 r. w Urzędzie nie opracowano, nie ustanowiono i nie wdrożono SZBI, o którym mowa w § 20 ust. 1 rozporządzenia KRI. Nie opracowano i nie wdrożono PBI, rozumianej jako zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa, według których dana organizacja zarządza i udostępnia swoje zasoby informacji.

Zgodnie z ww. przepisem jednostki realizujące zadania publiczne mają obowiązek opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia SZBI zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

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

W 2019 r. w Urzędzie dokonano[33] inwentaryzacji zasobów informacyjnych, ale tylko w odniesieniu do przetwarzanych danych osobowych, a nie w stosunku do wszystkich rodzajów informacji przetwarzanych w Urzędzie, wbrew wymaganiom Polskiej Normy PN-ISO/IEC 27001 (Załącznik nr 4: Wzorcowy wykaz celów stosowanych zabezpieczeń, pkt A.8.2. Klasyfikacja informacji), gdzie określono m.in., że „informacja powinna być klasyfikowana z uwzględnieniem wymogów prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.” Tym samym regulacje dotyczące bezpieczeństwa informacyjnego Urzędu odnosiły się tylko i wyłącznie do danych osobowych. Potwierdzeniem tego

[32] Analiza ryzyka dla pracy zdalnej, stan na dzień 15 kwietnia 2020 r. (dokument podpisany przez ASI, brak adnotacji ADO o zapoznaniu się z dokumentem), Mapowanie ryzyka i opinia IOD dla pracy zdalnej wg stanu na 12 kwietnia 2020 r. (dokument podpisany przez ASI i zaparafowany przez ADO z adnotacją „przedstawiono”), Analiza ryzyka dla pracy zdalnej, stan na dzień 15 marca 2021 r. (dokument podpisany przez ASI i zaparafowany przez ADO z adnotacją „przedstawiono”), Mapowanie ryzyka i opinia IOD dla pracy zdalnej wg stanu na 20 sierpnia 2021 r. (dokument podpisany przez ASI i zaparafowany przez ADO z adnotacją „przedstawiono”).

[33] Zgodnie z wzorem określonym w załączniku nr 5 do Polityki bezpieczeństwa przetwarzania danych osobowych.

jest także zdefiniowany cel i zakres przedmiotowy PBDO oraz załącznika nr 3 do tejże polityki, stanowiącego procedury bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych. Urząd określił, że celem ww. polityki i regulacji w niej zawartych jest ustanowienie zasad bezpiecznego przetwarzania danych osobowych.

Zdaniem Informatyka (pełniącego rolę ASI i IOD w Urzędzie), wprowadzanie kilku dokumentów precyzujących zadania związane z bezpieczeństwem informacji jest nieefektywne, a załącznik nr 3 pn. „Polityka bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych" do PBDO spełnia wszystkie wymogi literalnie zawarte w § 20 rozporządzenia KRI. Ponadto Informatyk oświadczył, że nie uważa za błędne ujęcie ochrony danych osobowych w jednym dokumencie z KRI, ponieważ zdecydowana większość informacji przetwarzanych przez pracowników (poza informacją niejawną) jest dostępna w trybie ustawy o dostępie do informacji publicznej. Po usunięciu danych osobowych obywateli i organizacji z podstawowej bazy danych Urzędu (PUMA), zakres pozostałych danych staje się publicznie dostępny (na wniosek). Poza tym o planach czy zamierzeniach obywatele są informowani na bieżąco.

Ponadto Wójt stwierdził, że dokumenty przyjęte w Urzędzie dotyczące polityki bezpieczeństwa informacji zawierają treści całościowo regulujące kwestie związane z systemem i polityką bezpieczeństwa informacji, jak również obejmują całość przetwarzanych danych w Urzędzie. Zdaniem Wójta struktura i zakres tych dokumentów była właściwa i zgodna z przepisami. Wójt podkreślił, że w PBDO wskazano, że załącznik nr 3 „Polityka bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych" jest odpowiednikiem SZBI.

Zdaniem NIK, rozporządzenie KRI określa minimalne wymagania dla rejestrów publicznych, wymiany informacji w postaci elektronicznej oraz minimalne wymagania dla systemów teleinformatycznych i odnosi się do ogółu informacji gromadzonych, przetwarzanych czy udostępnianych w Urzędzie. Zgodnie z § 20 ust. 1 rozporządzenia KRI utworzony i stosowany w Urzędzie SZBI powinien zapewnić poufność, dostępność i integralność wszystkich informacji z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Oznacza to, że nie tylko informacje dotyczące danych osobowych podlegają ww. zasadom i kryteriom. Podlegają im także inne dane chronione (tj. np.: objęte tajemnicą skarbową, tajemnicą przedsiębiorstwa, tajemnicą służbową, tajemnicą statystyczną, informacja niejawna), jak i dane publicznie dostępne. Mimo, iż procedury zawarte w załączniku nr 3 do PBDO odnosiły się do rozporządzenia KRI i wpisywały się w wymogi w nim określone, to jednak umieszczenie tych zasad bezpieczeństwa informacyjnego w dokumencie dedykowanym ochronie danych osobowych zawęża zakres ich stosowania do danych osobowych i systemów informatycznych przetwarzających dane osobowe. Należy też wskazać, że nawet dokumenty stanowiące informację publiczną wcześniej, jako projekty, podlegają obiegowi wewnętrznemu i jako takie, przed otrzymaniem ostatecznego kształtu, winny być chronione. Ponadto sporządzona w Urzędzie inwentaryzacja zasobów informacyjnych ograniczała się tylko do kategorii danych osobowych, co spowodowało, że stosowany w Urzędzie system zarządzania bezpieczeństwem informacji odnosił się tylko do danych osobowych.

(akta kontroli str. 7-12, 421, 547-554)

OCENA CZĄSTKOWA

W okresie objętym kontrolą w Urzędzie podejmowano działania w celu zorganizowania bezpieczeństwa informacji, w tym w ramach pracy na odległość

i mobilnym przetwarzaniu danych. Przyjęta w Urzędzie PBDO określała zasady: postępowania z nośnikami i urządzeniami przenośnymi, wynoszenia aktywów z Urzędu, przesyłania informacji oraz zarządzania incydentami związanymi z bezpieczeństwem informacji. W Urzędzie określono i przypisano odpowiedzialność za bezpieczeństwo informacji pracownikom. Wyznaczono także IOD, który posiadał odpowiednie kwalifikacje, a zakres jego obowiązków obejmował zadania określone w RODO. Przeprowadzono analizę ryzyka w ramach audytu bezpieczeństwa informacji w Urzędzie oraz analizy ryzyka dla pracy zdalnej. Działania podjęte w Urzędzie w wyniku tych analiz spowodowały wdrożenie dokumentów implementacyjnych do ww. polityki w zakresie zarządzania serwerami, komputerami i systemami informatycznymi oraz w zakresie zasad dotyczących ciągłości działania Urzędu. Wyniki tych analiz przyczyniły się także do organizacji bezpieczeństwa informacyjnego w ramach pracy zdalnej, w tym do przyjęcia Regulaminu pracy zdalnej w Urzędzie. W kontrolowanym okresie zapewniono także podnoszenie wiedzy pracowników w zakresie zagrożeń dla bezpieczeństwa informacji.

W toku kontroli stwierdzono jednak nieprawidłowość dotyczącą nieopracowania, nieustanowienia i niewdrożenia w Urzędzie SZBI oraz PBI, stosownie do przepisów rozporządzenia w sprawie KRI, obejmujących swoim zakresem wszystkie kategorie przetwarzanych w Urzędzie informacji.

OBSZAR

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

Opis stanu faktycznego

2.1. W Urzędzie zatrudnionych było 31 osób w 2020 r. i 32 - w 2021 r.[34] Spośród ww. pracowników, pracę zdalną na podstawie wniosku pracownika wykonywało odpowiednio 23 i 15 osób, w tym w czasie kwarantanny dwie osoby w 2020 r. i jedna w 2021 r. Wójt wprowadził możliwość świadczenia pracy zdalnej, zaś decyzję o dniu jej wykonywania pozostawił pracownikom.

(akta kontroli str. 531-536, 556)

2.2. W 2020 r. w Urzędzie nie wprowadzono żadnych pisemnych zasad regulujących pracę zdalną. W tym czasie w Urzędzie obowiązywały natomiast uregulowania wewnętrzne odnoszące się do bezpieczeństwa informacji obejmujących dane osobowe, których część regulacji miała zastosowanie także w pracy zdalnej (szerzej opisano w punkcie 1.1. wystąpienia).

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

Z dniem 19 marca 2020 r. wprowadzono obowiązek zgłaszania na skrzynkę mailową gotowości do pracy zdalnej.

[34] Wg stanu na 2 listopada 2021 r.

Kontrola wykazała, że 21, spośród 23 pracowników wykonujących obowiązki służbowe w ramach pracy zdalnej, potwierdziło gotowość do jej wykonywania zgodnie z przyjętą zasadą. Pozostałych dwóch pracowników nie dokonało ww. czynności. Zagadnienie to opisano w sekcji „Stwierdzone nieprawidłowości", w pozycji nr 1.

Zasady i tryb pracy zdalnej określono dopiero 15 marca 2021 r. w Regulaminie pracy zdalnej (szerzej opisano w punkcie 1.7. wystąpienia).

Kontrola wykazała, że spośród 12 pracowników wykonujących pracę zdalną po uchwaleniu ww. regulaminu tylko jeden złożył wszystkie wymagane oświadczenia[35] i wnioski[36].

Pozostałych 11 pracowników nie dopełniło wszystkich obowiązków wynikających z ww. regulaminu w zakresie wymaganych wniosków i oświadczeń:

- dwóch złożyło wymagane dokumenty, jednakże nie dotyczyły one wszystkich dni, w trakcie których wykonywane były obowiązki służbowe w ww. trybie. W jednym przypadku pracownik wykonywał pracę zdalnie łącznie przez 18 dni, spośród których udokumentował 15, a dla pozostałych trzech nie złożył wymaganej dokumentacji. W drugim przypadku wykonywał swoje obowiązki zdalnie przez cztery dni, udokumentował dwa, a dla pozostałych dwóch nie złożył wymaganych wniosków i oświadczeń,
- pozostałych dziewięciu pracowników nie złożyło wymaganych dokumentów.

Zagadnienie to opisano w sekcji „Stwierdzone nieprawidłowości", w pozycji nr 1.

Wszyscy pracownicy Urzędu skierowani do pracy zdalnej posiadali upoważnienie do przetwarzania danych osobowych oraz złożyli oświadczenia o zapoznaniu się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi.

Spośród 24 osób pracujących na odległość, 21 potwierdziło zapoznanie się z Regulaminem pracy zdalnej, dwóch nie miało takiego obowiązku[37], jedna zaś nie dokonała tej czynności.

Wójt wyjaśnił, że przez nieuwagę nie przedłożono pracownikowi ww. dokumentu do zapoznania się.

W dniu 12 listopada 2021 r. pracownica zapoznała się z treścią Regulaminu pracy zdalnej, co potwierdziła w złożonym oświadczeniu.

(akta kontroli str. 4-415, 433-436, 531-536, 557-639, 724-725)

2.3. Spośród 24 pracowników wykonujących pracę zdalną, w dwóch przypadkach zapewniono sprzęt teleinformatyczny będący własnością Urzędu, tj.:

- telefon, który przez cały okres objęty kontrolą wykorzystywany był przez Wójta do komunikacji głosowej,
- komputer przenośny, który wykorzystywany był przez pracownika odpowiedzialnego za obsługę Rady Gminy (przez łącznie pięć dni pracy zdalnej – cztery w 2020 r. i jeden w 2021 r.), na którym umożliwiono m.in. korzystanie z pakietu biurowego, przeglądarek internetowych oraz aplikacji do rozmów głosowych i połączeń wideo. Zainstalowano na nim również oprogramowanie

[35] Załącznik nr 3 do Regulaminu pracy zdalnej - Oświadczenie pracownika o zapoznaniu się z treścią Regulaminu pracy zdalnej w Urzędzie, znajomości zasad ochrony danych osobowych i zobowiązaniu się do przestrzegania ww. regulaminu.

[36] Załącznik nr 2 do Regulaminu pracy zdalnej – Wniosek pracownika o umożliwienie pracy zdalnej.

[37] W jednym przypadku pracownik rozwiązał umowę o pracę przed uchwaleniem ww. regulaminu, w drugim zaś – po zakończeniu urlopu bezpłatnego, tj. we wrześniu 2021 r.

antywirusowe i program służący do szyfrowania danych na dysku twardym. Komputer nie miał możliwości łączenia się z systemem informatycznym Urzędu, ani z komputerem stacjonarnym przez aplikację pulpitu zdalnego. Nie sporządzano również kopii bezpieczeństwa.

Zainstalowane oprogramowanie ww. komputera przydzielonego pracownikowi, do którego zadań należało m.in. przygotowywanie korespondencji oraz obsługa biurowa Przewodniczącego Rady i Przewodniczących Komisji, przygotowywanie materiałów pod obrady oraz prowadzenie dokumentacji i sprawozdawczości z zakresu ochrony zdrowia, umożliwiało ich realizację w trybie pracy zdalnej.

W pozostałych 23 przypadkach praca zdalna wykonywana była z użyciem sprzętu będącego własnością pracowników, co opisano w punkcie 2.5. wystąpienia.

(akta kontroli str. 640-650)

Pracownikom zapewniono również łącznie osiem nośników danych (7 pendrive i 1 dyktafon), spośród których do pracy zdalnej w latach 2020-2021 wykorzystano odpowiednio pięć i osiem takich urządzeń. Sposób korzystania z ww. urządzeń uregulowany został w Zasadach postępowania w pamięciami przenośnymi oraz w PBDO (szerzej opisano w punkcie 1.4 wystąpienia).

W Urzędzie prowadzono w formie elektronicznej wykaz urządzeń zewnętrznych dopuszczonych do pracy, w którym zaewidencjonowano osiem takich urządzeń. Wykaz ten zawierał ID urządzenia oraz nazwisko lub inicjały imienia i nazwiska pracownika, któremu je przydzielono, nie zawierał natomiast daty pobrania urządzenia.

ASI wyjaśnił, że PBDO nie narzuca obowiązku prowadzenia ewidencji pamięci przenośnych z uwzględnieniem daty przekazania urządzenia. Przyjęto, że data przekazania urządzenia to data złożenia przez pracownika wniosku o wyrażenie zgody na jego użytkowanie, tj. w sierpniu 2021 r.

W sześciu przypadkach pracownicy przedłożyli oświadczenia i wnioski dotyczące pobrania urządzeń przenośnych (wykazanych w ewidencji), w dwóch zaś ww. dokumentów nie przedłożono, pomimo obowiązku ich złożenia, wynikającego z uregulowań wewnętrznych. Zagadnienie to opisano w sekcji „Stwierdzone nieprawidłowości", w pozycji nr 2.

Stwierdzono również, że w wykazie urządzeń przenośnych ujęto urządzenie z błędnym numerem ID. Zagadnienie to opisano w sekcji „Stwierdzone nieprawidłowości", w pozycji nr 3.

(akta kontroli str. 674-696)

2.4. Oględziny komputera przenośnego (S/N:1FF51P2), wykorzystywanego przez pracownika odpowiedzialnego za obsługę Rady Gminy do pracy zdalnej, wykazały m.in., że użytkownik posiadał uprawnienia administratora (m.in. pozwalające na zainstalowanie dowolnego oprogramowania). Pracownik obsługiwał służbową pocztę elektroniczną, korzystając z prywatnego dostępu do Internetu.

ASI wyjaśnił, że zainstalowany na komputerze system Windows 10 Home umożliwiał instalowanie oprogramowania z poziomu użytkownika. Podał również, że system został zakupiony i zainstalowany w 2018 r., zanim został pracownikiem Urzędu. Instalacja systemu w wersji Pro zaplanowana jest na koniec 2021 r. ASI wyjaśnił również, że zainstalowane na laptopie oprogramowanie antywirusowe umożliwia blokowanie skryptów i stron wyłudzających informacje, a zainstalowane przeglądarki zapewniają ochronę przed niebezpiecznymi stronami internetowymi.

(akta kontroli str. 610-613, 651-673)

2.5. W Urzędzie dopuszczono możliwość wykonywania pracy zdalnej z wykorzystaniem prywatnych urządzeń komputerowych. Nie określono jednak

warunków, jakie powinien spełniać sprzęt i oprogramowanie, aby można go było wykorzystać w realizacji zadań służbowych.

Wójt wyjaśnił, że w 2020 r. opracowano projekt regulacji dotyczących używania sprzętu prywatnego, jednakże z uwagi na brak uregulowań prawnych dotyczących przetwarzania informacji na komputerach prywatnych oraz brak zgody pracowników na udzielenie informacji o posiadanym sprzęcie komputerowym[38] zrezygnowano z jego wdrożenia.

W badanym okresie nie weryfikowano również faktu usunięcia z komputerów prywatnych wszelkich informacji wykorzystywanych do celów służbowych w trakcie pracy zdalnej.

Wójt wyjaśnił, że ze względu na brak przepisów prawnych umożliwiających weryfikację sprzętu prywatnego, skorzystano z oprogramowania umożliwiającego dostęp do konta pracownika na komputerze lokalnym w trybie zdalnego pulpitu z wyłączonymi opcjami drukowania na drukarce lokalnej, używania schowka i używania managera plików. Zobowiązano również pracowników do wyłączania urządzeń po zakończeniu pracy, a weryfikacja włączonych urządzeń odbywała się z wykorzystaniem „Raportu statusu sieci", tworzonego z wykorzystaniem oprogramowania antywirusowego. Również ze względu na obowiązujące prawo nie weryfikowano usunięcia z komputerów prywatnych wszelkich informacji wykorzystywanych do celów służbowych.

W Urzędzie obowiązywały oświadczenia[39] dotyczące usunięcia wszystkich danych z nośników informatycznych, które złożyło jedynie sześciu pracowników. Kontrola wykazała, że po dniu złożenia ww. oświadczeń pracownicy wykonywali obowiązki służbowe w formie pracy zdalnej, jednakże nie złożyli ponownie ww. oświadczeń.

Wójt wyjaśnił, że wzór oświadczenia został wysłany do wszystkich pracowników, jednakże po wprowadzeniu aplikacji dostępowej, w której zablokowano możliwość przesyłania plików, używania schowka i wydruku dokumentów zdecydowano o nieobligatoryjności tego oświadczenia.

Od momentu wdrożenia pulpitu zdalnego, tj. od kwietnia 2020 r. pracownicy uzyskali możliwość używania wszystkich programów i usług, jakie były dostępne na ich komputerach osobistych znajdujących się w Urzędzie. Do oprogramowania umożliwiającego dostęp zdalny i kontrolowanie pulpitu komputerów i serwerów oraz zapory UTM dostęp miał wyłącznie ASI.

(akta kontroli str. 537-546, 636-638, 640, 697-722)

2.6. W Urzędzie określono zasady postępowania z dokumentacją tradycyjną, jednakże tylko zawierającą dane osobowe[40], w których zakazano wynoszenia dokumentów zawierających dane osobowe poza Urząd, z wyjątkiem sytuacji, w których uzyskano zgodę ADO na ich wyniesienie w celu realizacji obowiązków służbowych.

Stwierdzono, że w trakcie wykonywania pracy zdalnej pracownicy nie wynosili dokumentów, zarówno w wersji papierowej, jak i elektronicznej, poza siedzibę Urzędu.

(akta kontroli str. 16-360, 723)

2.7. Zasady dotyczące monitorowania i nadzoru nad wykonywaniem pracy zdalnej wynikały wyłącznie z Regulaminu pracy zdalnej i dotyczyły obowiązku sporządzenia

[38] Informacje dotyczące urządzeń prywatnych wykorzystywanych w celach służbowych złożyło tylko dwóch pracowników (Sekretarz i ASI).

[39] Nie zostały one wprowadzone do stosowania w postaci zarządzenia.

[40] Załącznik nr 2 do Polityki bezpieczeństwa przetwarzania danych osobowych.

przez pracownika wykonującego pracę zdalną ewidencji czynności pracy zdalnej wg wzoru określonego w załączniku nr 4 do ww. regulaminu.

Wójt wyjaśnił, że wykonywanie obowiązków służbowych monitorowano telefonicznie, jak również poprzez przyjmowanie efektów pracy zdalnej w postaci m.in. przygotowanych materiałów, analiz i opinii dostarczonych mailowo lub osobiście, po zakończeniu pacy zdalnej. Podał również, że niezbędnym elementem uzyskania dostępu do danych wewnątrz Urzędu była konieczność włączenia komputera pracownika wykonującego pracę zdalnie, co pozwalało zweryfikować, czy pracownik wykonuje swoje obowiązki. Monitorowanie w zakresie dostępu do sieci i danych Urzędu następowało poprzez mail z routera brzegowego, a na etapie dostępu do systemu dziedzinowego PUMA – poprzez weryfikację logów.

(akta kontroli str. 408-415, 537-546)

Stwierdzone nieprawidłowości

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

1. W okresie objętym kontrolą w Urzędzie nie przestrzegano ustalonych zasad w zakresie pracy zdalnej. Stwierdzono bowiem, że pracownicy Urzędu nie przedkładali wymaganych w związku z pracą zdalną dokumentów, tj.:

   - Dwóch pracowników wykonujących pracę zdalną w okresie od 28 października do 2 listopada 2020 r. (zanim uchwalono Regulamin pracy zdalnej) nie przesłało na skrzynkę mailową informacji z gotowością do wykonywania obowiązków służbowych w trybie pracy zdalnej, pomimo wprowadzenia takiego obowiązku z dniem 19 marca 2020 r.

     Pracownicy wyjaśnili, że uznali za wystarczające ustne powiadomienie pracodawcy o sposobie wykonywania pracy.

     Wójt wyjaśnił, że niewyegzekwowanie wysłania informacji mailowej wynikało z przeoczenia.

     (akta kontroli str. 572-573, 576-583, 587-588)

   - Dwóch pracowników wykonujących pracę zdalną w dniach 17 marca, 29 marca i 8 kwietnia 2021 r. (L.K.) oraz 16 marca i 19 marca 2021 r. (C.S.) nie złożyło wniosków o wyrażenie zgody na jej wykonywanie, oświadczeń o zapoznaniu się z zasadami jej wykonywania oraz wykazu zrealizowanych czynności, pomimo tego, iż obowiązek złożenia ww. dokumentów wynikał z §2 ust. 1 lit. b oraz §6 ust. 1 i 2 Regulaminu pracy zdalnej.

     Ponadto dziewięciu innych pracowników wykonujących w 2021 r. pracę zdalnie w ogóle nie złożyło żadnych dokumentów dotyczących zgody na pracę zdalną, pomimo tego, iż obowiązek ich złożenia wynikał z §2 ust. 1 lit. b oraz §6 ust. 1 i 2 Regulaminu pracy zdalnej.

     Pracownicy wyjaśnili, że wynikało to z uchybienia i niedopatrzenia.

     Wójt wyjaśnił, że pracownicy przesłali informację mailem, zgodnie z zasadami obowiązującymi przed uchwaleniem Regulaminu pracy zdalnej, którą uznał za wystarczającą.

     (akta kontroli str. 408-415, 589-613)

2. W okresie objętym kontrolą w Urzędzie nie przestrzegano zasad postępowania z nośnikami zewnętrznymi. Stwierdzono bowiem, że ASI wydał pracownikom pamięci przenośne nie egzekwując jednocześnie przedłożenia dokumentów określonych w §2 ust. 1 i 5 Zasad przyznawania pamięci przenośnych oraz w PBDO.

Pracownicy wyjaśnili, że nie wiedzieli o obowiązku złożenia takich dokumentów oraz że urządzenie dopuszczone jest do użytku wewnątrz Urzędu, więc nie ma takiego obowiązku.

(akta kontroli str. 361-367, 610-629, 675-693)

3. Nierzetelnie powadzono wykaz urządzeń przenośnych dopuszczonych do użytkowania, bowiem użytkownik posługiwał się urządzeniem, którego w tej ewidencji nie ujęto.

   Pracownik, który w ewidencji urządzeń przenośnych był użytkownikiem pamięci przenośnej wyjaśnił, że posiada tylko jedną pamięć przenośną i nie sprawdził numeru ID pamięci z ewidencją, bowiem w momencie odbioru urządzenia przydzielonego przez ASI był przekonany, że widnieje ona w ww. rejestrze.

   ASI wyjaśnił, że omyłkowo w ewidencji wpisano urządzenie z innym numerem ID.

   (akta kontroli str. 674-676, 683, 691-696)

OCENA CZĄSTKOWA

W Urzędzie wdrożono rozwiązania organizacyjne i techniczne mające na celu zapewnienie bezpieczeństwa informacji w pracy zdalnej, jednakże nie w pełni je egzekwowano. Nie przestrzegano uregulowań w zakresie zasad postępowania z pamięciami przenośnymi oraz nie w pełni rzetelnie prowadzono ich ewidencję. Nie wywiązywano się również z obowiązku składania wniosków i oświadczeń, wynikających z Regulaminu pracy zdalnej. Zapewniono możliwość wykonywania obowiązków służbowych z komputerów prywatnych poprzez dostęp do zdalnego pulpitu.

IV. Uwagi i wnioski

Najwyższa Izba 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 SZBI (w tym PBI) spełniającego wymogi określone w rozporządzeniu KRI.
2. Podjęcie działań zmierzających do przestrzegania przez pracowników zasad wynikających z Regulaminu pracy zdalnej.
3. Rzetelne prowadzenie wykazu urządzeń przenośnych dopuszczonych do użytkowania.

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, 30 listopada 2021 r.

Kontrolerzy

Justyna Lis

starszy inspektor kontroli państwowej

.....

podpis

Joanna Łukasik

główny specjalista kontroli państwowej

.....

podpis

Najwyższa Izba Kontroli

Delegatura w Olsztynie

Dyrektor

z up.

Piotr Wanic

Wicedyrektor

.....

podpis