NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

00565517

LBI.411.001.04.2017
R/17/001

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku
ul. Akademicka 4, 15-267 Białystok
T +48 85 874 81 00, F +48 85 874 81 33
lbi@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	R/17/001 – Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontrolerzy	Beata Palinowska – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/37/2017 z 27 lutego 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Urząd Gminy Jaświły, Jaświły 7, 19-124 Jaświły (dalej: „Urząd Gminy")
Kierownik jednostki kontrolowanej	Jan Joka – Wójt Gminy Jaświły[1] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

Urząd Gminy[3] nie podejmował wszystkich wymaganych przepisami prawa i regulacjami wewnętrznymi działań, mających na celu zapewnienie odpowiedniej ochrony posiadanych zasobów informacyjnych, które pozwoliłyby na całkowitą i skuteczną ochronę danych przez niego przetwarzanych.

Uzasadnienie oceny ogólnej

W Urzędzie Gminy do 16 marca 2017 r. nie wdrożono polityki bezpieczeństwa informacji, o której mowa w § 2 pkt 15 w związku § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[4].

Obowiązujące w Urzędzie Gminy uregulowania dotyczące bezpieczeństwa przetwarzania danych osobowych nie były w pełni przestrzegane oraz nie zawierały wszystkich elementów z wymienionych w § 4 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[5].

Pracownicy powołani przez Wójta Gminy na stanowiska Administratora Bezpieczeństwa Informacji (dalej: „ABI") oraz Administratora Systemu Informatycznego (dalej: „ASI") nie wywiązywali się z części obowiązków. ABI nie sporządzał planu sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, wymaganego § 3 ust. 5 rozporządzenia Ministra Administracji Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji[6]. ASI zaś nie podejmował działań niezbędnych do zapewnienia bezpieczeństwa systemom służącym przetwarzaniu danych osobowych (nie nadzorował sporządzania kopii zapasowych systemów i danych w sposób zgodny z określonym w wewnętrznych uregulowaniach Urzędu Gminy, nie przeprowadzał przeglądów i konserwacji systemów oraz dopuścił do posiadania przez wszystkich użytkowników uprawnień administratora

---

1 Funkcję Wójta Gminy Jaświły pełni od 20 czerwca 1990 r.

2 Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna. Jeżeli sformułowanie oceny ogólnej według proponowanej skali byłoby nadmiernie utrudnione albo taka ocena nie dawałaby prawdziwego obrazu funkcjonowania kontrolowanej jednostki w zakresie objętym kontrolą, stosuje się ocenę opisową bądź uzupełnia ocenę ogólną o dodatkowe objaśnienie.

3 Okres objęty kontrolą to od 1 stycznia 2016 r. do dnia zakończenia czynności kontrolnych oraz działania wcześniejsze mające wpływ na kontrolowaną działalność.

4 Dz. U. 2016 poz.113, ze zm. Rozporządzenie zwane dalej: „rozporządzeniem KRI".

5 Dz. U. Nr 100 poz. 1024. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie dokumentacji przetwarzania danych osobowych".

6 Dz. U. 2015 poz. 745. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie sposobu realizacji zadań ABI".

w systemach operacyjnych komputerów wykorzystywanych do przetwarzania danych osobowych).

Najwyższa Izba Kontroli zwraca uwagę, że kopie zapasowe nie były testowane, co stwarza zagrożenie utraty danych znajdujących się w systemach informatycznych Urzędu Gminy. Użytkowanie natomiast siedmiu komputerów z zainstalowanym systemem operacyjnym nieposiadającym wsparcia technicznego producenta może mieć wpływ na obniżenie skuteczności ochrony danych przetwarzanych z ich wykorzystaniem.

III. Opis ustalonego stanu faktycznego

1. Dokumentacja i procedury dotyczące ochrony danych

1.1. Dokumentacja dotycząca ochrony danych osobowych

Opis stanu faktycznego

Wójt Gminy skorzystał z możliwości jaką daje art. 36 a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[7] i wyznaczył ABI (zarządzeniem nr 11/15 z dnia 2 lutego 2015 r.[8]). W zarządzeniu wskazano, że zakres jego działania wynika z art. 36a ust. 2 ww. ustawy i obejmuje: [1] zapewnienie przestrzegania przepisów o ochronie danych osobowych, w tym m.in. sprawdzanie zgodności przetwarzania danych osobowych z tymi przepisami oraz opracowanie w tym zakresie sprawozdań dla administratora danych; [2] prowadzenie rejestru zbioru danych przetwarzanych przez administratora danych.

Zgłoszenia powołania ABI do Generalnego Inspektora Ochrony Danych Osobowych (dalej: „GIODO") dokonano 3 lutego 2015 r. (następnego dnia po powołaniu, tj. w terminie zgodnym ze wskazanym w art. 46b ust. 1 powołanej ustawy[9], na wzorze określonym w załączniku nr 1 do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji[10]. Zgłoszenie zawierało wszystkie elementy wymagane art. 46b ust. 2 ustawy o ochronie danych osobowych. (dowód: akta kontroli str. 4-7)

ABI nie opracował planu sprawdzeń z zakresu przestrzegania przepisów o ochronie danych osobowych w Urzędzie Gminy na rok 2016 i 2017. Było to niezgodne z § 3 ust. 5 rozporządzenia w sprawie sposobu realizacji zadań ABI (szerzej omówiono w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości").
(dowód: akta kontroli str. 282-284)

Od 1 stycznia 2016 r. ABI dwukrotnie[11] sprawdził zgodność przetwarzania danych osobowych z przepisami o ich ochronie. W wyniku czego ustalono, że w Urzędzie Gminy są realizowane procedury wynikające z przepisów ustawy o ochronie danych osobowych, a wszyscy pracownicy przetwarzający dane osobowe posiadają upoważnienia do ich przetwarzania. Zgodnie z art. 36a ust. 2 pkt 1 lit. a ustawy o ochronie danych osobowych, z przeprowadzonych czynności ABI sporządził sprawozdania dla ADO. Nie zawierały one jednak części elementów wymaganych art. 36c ustawy o ochronie danych osobowych (szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości"). (dowód: akta kontroli str. 71-72)

ABI, zgodnie z art. 36a ust. 2 pkt 1 lit. c) ww. ustawy, zapoznał osoby upoważnione do przetwarzania danych osobowych z przepisami o ich ochronie. W okresie objętym kontrolą zorganizował dwa wewnętrzne szkolenia z zakresu ochrony danych osobowych, w których uczestniczyło 10 – 12 pracowników, tj. wszyscy którzy zajmowali się przetwarzaniem danych osobowych. Zakres szkoleń obejmował m.in. zapoznanie pracowników z przepisami o ochronie danych osobowych, z obowiązującymi w Urzędzie Gminy regulacjami z zakresu ochrony danych osobowych, zakres obowiązków pracowników przetwarzających dane osobowe, przepisy karne.

ABI uczestniczył w szkoleniu zewnętrznym na temat stosowania przepisów ustawy o ochronie danych oraz zarządzania systemem ochrony danych osobowych (w 2016 roku).

---

[7] Dz. U. z 2016 r., poz. 922 ze zm.
[8] O powołaniu ABI w Urzędzie Gminy Jaświły.
[9] Dane dotyczące ABI zawarte w rejestrze prowadzonym przez GIODO były aktualne. Sprawdzono poprzez wyszukiwarkę http://egiodo.giodo.gov.pl/search_ado.dhtml.
[10] Dz. U. z 2014 r., poz. 1934.
[11] 11 stycznia 2016 r. i 9 stycznia 2017 r.

Zakres szkolenia obejmował m.in. wynikające z przepisów obowiązki ABI i ADO z zakresu ochrony danych osobowych, sprawozdawczość, prowadzenie rejestru zbiorów, opracowanie polityki bezpieczeństwa i instrukcji zarządzania, praktyczne stosowanie środków technicznych i organizacyjnych służących zabezpieczeniu danych osobowych.
(dowód: akta kontroli str. 57, 73-81)

ABI, w myśl art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych, prowadził rejestr zbiorów danych przetwarzanych w Urzędzie Gminy. Zawierał on nazwę zbioru, oznaczenie administratora danych, podstawę prawną upoważniającą do prowadzenia zbiorów, a także informacje wymienione w art. 41 ust. 1 pkt 3-4a i 7 ustawy o ochronie danych osobowych.
(dowód: akta kontroli str. 53-56)

W Urzędzie Gminy była prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych. Obejmowała ona wszystkich upoważnionych pracowników i zawierała wszystkie elementy określone w art. 39 ust. 1 ustawy o ochronie danych osobowych, za wyjątkiem identyfikatora użytkownika w systemie informatycznym, tj.: imię i nazwisko osoby upoważnionej, datę nadania i ustania upoważnienia oraz jego zakres (co szerzej opisano w dalszej części wystąpienia pokontrolnego w sekcji „Ustalone nieprawidłowości"). Analiza zakresów obowiązków pracowników wykazała, że posiadali oni upoważnienia do przetwarzania danych osobowych w systemach informatycznych lub prowadzonych w formie papierowej, adekwatne do powierzonych obowiązków.
(dowód: akta kontroli str. 243-248)

W Urzędzie nie zostały opracowane procedury / instrukcje w zakresie nadzoru oraz zapewnienia kontroli nad rodzajem danych osobowych i osobą wprowadzającą takie dane do danego zbioru, ani wskazaniem odbiorcy danych osobowych. Zastępca Wójta Gminy wyjaśnił, że: *„Nie zostały opracowane takie regulacje bowiem jest to mały Urząd i nie zachodziła potrzeba wprowadzenia takich regulacji. Nadzór w tym zakresie sprawują kierownicy referatów i jednostek w ramach swoich zakresów obowiązków"*.
(dowód: akta kontroli str. 282-284)

Urząd Gminy zgłosił GIODO do zarejestrowania 27[12] zbiorów danych osobowych. Cztery z nich nie były jednak faktycznie prowadzone, co szerzej opisano w dalszej części wystąpienia pokontrolnego w pkt 2, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 110-117, 282-284)

Wójt Gminy powołał, zarządzeniem z 27 listopada 2014 r. na stanowisko ASI osobę zatrudnioną w Urzędzie Gminy na stanowisku Inspektora ds. obsługi inwestycji. Zakres obowiązków ASI obejmował w szczególności tworzenie kont użytkowników w systemach informatycznych, przypisywanie do kont startowych haseł użytkowników, sprawdzanie częstotliwości założonych kont pod kątem jakości haseł i częstotliwości ich zmiany, czuwanie nad tworzeniem kopii bezpieczeństwa systemów i danych, automatyzacja zadań konserwacyjnych w systemach, w tym wykonywanie kopii zapasowych, monitorowanie stanu środowiska IT, monitorowanie legalności oprogramowania, prowadzenie szkoleń na temat bezpieczeństwa w środowisku systemów IT. (dowód: akta kontroli str. 132-133)

W Urzędzie Gminy, w myśl § 20 ust. 2 pkt 14 rozporządzenia w sprawie KRI, od 20 grudnia 2016 r. do 10 stycznia 2017 r. został przeprowadzony audyt wewnętrzny z zakresu bezpieczeństwa informacji za 2016 rok. Obejmował on: [1] stosowanie polityki bezpieczeństwa, [2] procedurę sporządzania kopii zapasowych, [3] monitoring sieci pod kątem zagrożenia wirusami, [4] przechowywanie nośników informacji, [5] postępowanie w sytuacji stwierdzenia naruszenia systemów ochrony danych osobowych, [6] sposób i miejsce przechowywania wydruków, elektronicznych nośników informacji oraz kopii zapasowych zawierających dane osobowe, a także zabezpieczenie systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu, [7] procedury wykonania przeglądów i konserwacji systemów oraz nośników informacji, [8] fizyczny nadzór nad bezpieczeństwem. Stwierdzono uchybienia, polegające na niewskazaniu osoby, która realizowałaby obowiązki

[12] W Urzędzie Gminy były prowadzone 24 zbiory, cztery były prowadzone w Gminnym Ośrodku Pomocy Społecznej w Jaświłach.

spoczywające na ABI na wypadek jego nieobecności oraz przechowywaniu kopii zapasowych w miejscu, w którym zostały wytworzone. (dowód: akta kontroli str. 58-70)

W okresie objętym kontrolą w Urzędzie Gminy nie były przeprowadzane zewnętrzne kontrole z zakresu bezpieczeństwa danych. Nie były składane pisemne skargi i wnioski związane z przypadkami ujawnienia danych osobowych. (dowód: akta kontroli str. 124)

Ustalone nieprawidłowości

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

1. ABI nie sporządził w latach 2016 i 2017 planu sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Było to niezgodne z § 3 ust. 5 rozporządzenia w sprawie sposobu realizacji zadań ABI. Zgodnie z tym przepisem plan sprawdzeń jest przygotowywany przez ABI na okres nie krótszy niż kwartał i nie dłuższy niż rok, następnie jest przedstawiany kierownikowi jednostki (Administrator Danych Osobowych, dalej „ADO") nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem i obejmuje, co najmniej jedno sprawdzenie.

   ABI wyjaśnił, że: *„Nie wiedziałem, że należy przygotować taki plan. W przyszłości takie plany będą przeze mnie opracowywane"*. (dowód: akta kontroli str. 282-284)

2. Sporządzone przez ABI dwa sprawozdania z czynności kontrolnych obejmujących sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ich ochronie nie zawierały elementów wymaganych art. 36c ustawy o ochronie danych osobowych:
   - wykazu podjętych w toku sprawdzenia czynności oraz imion, nazwisk i stanowisk osób w nich uczestniczących (pkt 3),
   - daty rozpoczęcia i zakończenia sprawdzenia, a także określenia przedmiotu i zakresu sprawdzenia (pkt 4 i 5),
   - stwierdzonych przypadków naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem (pkt 7).

   ABI wyjaśnił, że: *„W trakcie przeprowadzonych przeze mnie czynności nie stwierdzone zostały żadne uchybienia dlatego nie znalazło się to w sprawozdaniu. Brak innych elementów wynika z niewiedzy"*. (dowód: akta kontroli str. 71-72, 282-284)

3. Ewidencja osób upoważnionych do przetwarzania danych osobowych nie zawierała identyfikatora użytkownika w systemie informatycznym. Było to sprzeczne z art. 39 ust. 1 pkt 3 powołanej ustawy, zgodnie z którym w przypadku przetwarzania danych osobowych w systemie informatycznym, ewidencja osób upoważnionych do przetwarzania danych osobowych, powinna zawierać identyfikator użytkownika w systemie informatycznym.

   ABI wyjaśnił, że: *„Każdy z pracowników miał nadany indywidualny login i hasło do systemu operacyjnego oraz do systemu dziedzinowego. Natomiast nie było to ujęte w ewidencji z powodu przeoczenia"*.

   W trakcie kontroli ewidencję uzupełniono o ww. dane (w dniu 14 marca 2017 r.).
   (dowód: akta kontroli str. 243-255, 282-284)

1.2. Dokumentacja dotycząca warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne

Opis stanu faktycznego

Zarządzeniem Wójta Gminy z 3 kwietnia 2015 roku nr 20/15 wprowadzono Politykę bezpieczeństwa przetwarzania danych osobowych[13] i Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Jaświły[14]. (dowód: akta kontroli str. 8-52)

Polityka bezpieczeństwa zawierała jedynie elementy określone w § 4 pkt 5 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych. Nie zawierała natomiast elementów określonych w § 4 pkt 1, 3 i 4 ww. rozporządzenia, a wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania,

[13] Polityka bezpieczeństwa przetwarzania danych osobowych zwana dalej: Polityką bezpieczeństwa".
[14] Instrukcja Zarządzania Systemem Informatycznym zwana dalej: „Instrukcją zarządzania".

wymagany § 4 pkt 2 ww. rozporządzenia, był niepełny (co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości").

(dowód: akta kontroli str. 8-35)

Instrukcja zarządzania zawierała elementy wskazane w § 5 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, tj.: m.in. procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz osoby odpowiedzialne za te czynności, stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem, procedury rozpoczęcia i zakończenia pracy przeznaczone dla użytkowników systemu, procedury tworzenia kopii zapasowych zbiorów danych. Nie zawierała natomiast opisu procedury zawieszania pracy w systemie informatycznym, programów i narzędzi programowych służących do przetwarzania zbiorów danych, sposobu realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia w sprawie dokumentacji przetwarzania danych (szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości").

(dowód: akta kontroli str. 36-52)

W § 11 ust. 1 Instrukcji zarządzania wskazano, że kopie zapasowe nie powinny być przechowywane w tych samych pomieszczeniach, w których są przechowywane zbiory danych eksploatowane na bieżąco, zaś nośniki informacji oraz wydruki z danymi osobowymi nieprzeznaczonymi do udostępniania nie powinny być przechowywane w sposób umożliwiający do nich dostęp osobom uprawnionym. Nie wskazano natomiast okresu przechowywania kopii zapasowych i elektronicznych nośników informacji zawierających dane osobowe, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Zgodnie z § 11 ust. 4 Instrukcji zarządzania kopie awaryjne powinny być przeglądane okresowo w celu dokonania oceny przydatności do odtworzenia zasobów systemu w przypadku jego awarii. Stwierdzenie nieprzydatności kopii upoważnia ASI do jej zniszczenia. (dowód: akta kontroli str. 36-52)

Polityka bezpieczeństwa i Instrukcja zarządzania nie zawierały zapisów regulujących poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym[15]. W zgłoszeniach do GIODO wskazano, że dla 16 zbiorów danych zastosowano podstawowy poziom środków bezpieczeństwa, zaś dla czterech kolejnych poziom podwyższony[16] (szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości"). (dowód: akta kontroli str. 110-117)

Do 16 marca 2017 r. w Urzędzie Gminy nie opracowano Polityki bezpieczeństwa informacji wymaganej § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia w sprawie KRI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 197-234)

Spośród siedmiu systemów informatycznych służących do przetwarzania danych osobowych tylko jeden (SmartDoc) umożliwiał sporządzenie i wydrukowanie raportu o udostępnieniu danych, zawierającego w powszechnie zrozumiałej formie informacje określone w § 7 ust. 3 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, dotyczące m.in. daty pierwszego wprowadzenia danych osobowych i identyfikatora użytkownika wprowadzającego dane osobowe do systemu. Pozostałe sześć systemów informatycznych[17] nie pozwalało na wydrukowanie wymienionego raportu, umożliwiały natomiast wydruk listy operacji zawierającej elementy określone w § 7 ust. 3 pkt 1 i 2 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, tj. datę pierwszego wprowadzenia danych osobowych do systemu i identyfikator użytkownika wprowadzającego dane. (dowód: akta kontroli str. 258-259)

---

[15] Poziomy bezpieczeństwa były wskazane w zgłoszeniach rejestracji zbiorów danych przesłanych do GIODO.

[16] Pięć zbiorów danych było zgłoszonych do GIODO w 1999 roku.

[17] Fiskus, Cheops, Budżet/Płace, USCwin, Selwin, CEiDG, SmartDoc, Źródło. Administratorem danych dla systemu CEIDG i Źródło były podmioty zewnętrzne. W Urzędzie Gminy użytkowano również program Ewopis, którego Administratorem było Starostwo Powiatowe w Mońkach – program służył do przeglądania (pracownicy Urzędu Gminy nie wprowadzali danych do tego systemu).

Ustalone nieprawidłowości

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

1. Polityka bezpieczeństwa nie zawierała elementów wymaganych w § 4 pkt 1, 3 i 4 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, tj.: wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane były dane osobowe; opisu struktury zbiorów danych, wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposobu przepływu danych pomiędzy poszczególnymi systemami.

   ABI wyjaśnił, że *„Brak tych elementów wynika z przeoczenia. Zostanie to uzupełnione w najbliższym czasie"*. (dowód: akta kontroli str. 9-35, 282-284)

2. Instrukcja zarządzania nie zawierała następujących elementów wymienionych w § 5 rozporządzenia w sprawie dokumentacji przetwarzania danych:
   - procedury zawieszenia pracy przeznaczonej dla użytkowników systemu (§ 5 pkt 3 ww. rozporządzenia),
   - programów i narzędzi programowych służących do przetwarzania kopii zapasowych zbiorów danych (§ 5 pkt 4 ww. rozporządzenia),
   - opisu sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych (§ 5 pkt 5 ww. rozporządzenia),
   - sposobu realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 powołanego rozporządzenia, tj. dotyczących zapewnienia każdej osobie, której dane osobowe są przetwarzane w systemie informatycznym, informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia (§ 5 pkt 7 ww. rozporządzenia).

   ABI wyjaśnił, że brak tych elementów wynikał z przeoczenia i zostanie o nie uzupełniona Instrukcja zarządzania. (dowód: akta kontroli str. 8-52)

3. W Urzędzie Gminy do 16 marca 2017 r. nie była opracowana polityka bezpieczeństwa informacji, o której mowa w § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia w sprawie KRI, a obowiązujące procedury dotyczyły wyłącznie danych osobowych.

   ABI wyjaśnił, że: *„Byłem przekonany, że Polityka ochrony danych osobowych i Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych są dokumentami wystarczającymi. Podobne stanowisko było prezentowane na szkoleniach, w których uczestniczyłem. Dlatego nie został opracowany taki dokument. Dokument ten jest w trakcie wdrażania"*.
   (dowód: akta kontroli str. 157,197-234, 282-284)

Ocena cząstkowa

Urząd Gminy nie w pełni wywiązał się z obowiązku opracowania dokumentacji dotyczącej ochrony danych osobowych. Polityka bezpieczeństwa i Instrukcja zarządzania nie zawierały bowiem wszystkich elementów z określonych w rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych, a do 16 marca 2017 r. nie opracowano polityki bezpieczeństwa informacji, o której mowa w § 2 pkt 15 w związku § 20 ust. 1 rozporządzenia KRI. ABI nie wywiązał się zaś z obowiązku sporządzenia i przedłożenia ADO planów sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Przeprowadzone natomiast przez ABI w 2016 roku i 2017 roku sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ich ochronie zostały udokumentowane sprawozdaniami, które jednak nie zawierały niektórych elementów wymaganych przepisami.

2. Zakres przetwarzanych zasobów informacyjnych

Opis stanu faktycznego

W Urzędzie Gminy dane były przetwarzane w 24 zbiorach. Do GIODO, celem zarejestrowania, zgłoszono 28 zbiorów, w tym cztery, które były przetwarzane w gminnej jednostce organizacyjnej (co szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości"). Zarejestrowanych zostało 27 zbiorów. GIODO odmówił rejestracji zbioru „Kadry", zwolnionego z obowiązku rejestracji, zgodnie z art. 43 ust. 1 pkt 4 ustawy o ochronie danych osobowych. (dowód: akta kontroli str. 258-259, 285-289)

Zakres danych przetwarzanych w 10 (z 21) zbiorach był zgodny z zakresem objętym zgłoszeniem do GIODO. W 11 zbiorach gromadzone były dane osobowe wykraczające poza zakres objęty zgłoszeniem do GIODO, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". W okresie objętym kontrolą nie zgłaszano GIODO aktualizacji zakresu danych osobowych gromadzonych w zbiorach danych. Zakres danych osobowych gromadzonych we wszystkich zbiorach danych[18] był niezbędny do realizacji zadań przypisanych komórkom, w których je gromadzono. (dowód: akta kontroli str. 110-117)

W zgłoszeniu do rejestracji w rejestrze zbiorów prowadzonym przez GIODO zbioru danych pn. „Numeracja porządkowa nieruchomości", dokonanym 13 czerwca 2013 r. nie wskazano, że przetwarzanie danych osobowych w tym zbiorze powierzono innemu podmiotowi, na podstawie umowy zawartej 17 października 2012 r., co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 82-90)

Wójt Gminy pełnił funkcję ADO dla 21 zbiorów danych, do których dostęp posiadali pracownicy Urzędu Gminy, w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych. Dla trzech zbiorów danych administratorem były inne podmioty: CEIDG, Źródło i Ewopis[19]. Dostęp do zbioru danych CEIDG, prowadzonego przez Ministra Rozwoju i Finansów, posiadało dwóch pracowników Urzędu Gminy upoważnionych przez Wójta Gminy[20], na podstawie art. 26 ust 4a ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej[21]. Zbiór danych osobowych w systemie Ewopis był prowadzony przez Starostwo Powiatowe w Mońkach. Urząd Gminy uzyskał dostęp do tego systemu na podstawie umowy o dostępie do danych opisowych, zawartej 2 lutego 2017 r. Czterech pracowników Urzędu Gminy posiadało do niego dostęp na podstawie indywidualnie przydzielonego loginu i hasła. Z kolei dostęp do danych w systemie Źródło posiadali wyznaczeni pracownicy, którzy posługiwali się indywidualną kartą użytkownika zabezpieczoną kodem dostępowym. Stanowisko dostępowe do systemu Źródło nie miało dostępu do „otwartego" Internetu. (dowód: akta kontroli str. 125-131)

Ustalone nieprawidłowości

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

1. Urząd Gminy, mimo obowiązku wynikającego z art. 41 ust. 2 pkt 1 ustawy o ochronie danych osobowych, dopiero 10 czerwca 2013 r. zgłosił GIODO informację o powierzeniu innemu podmiotowi (na podstawie umowy zawartej 17 października 2012 r.) przetwarzania danych osobowych. Ponadto zakres danych osobowych powierzonych przetwarzającemu był szerszy niż zawarty w zgłoszeniu do GIODO.

   ABI wyjaśnił, że zajmował się tym pracownik, który obecnie nie pracuje w Urzędzie Gminy oraz, że nie potrafi wskazać powodu niezgłoszenia GIODO informacji o przedmiotowej umowie. (dowód: akta kontroli str. 82-90)

2. Zakres danych osobowych przetwarzanych przez Urząd Gminy w 11 zbiorach danych wykraczał poza określony w zgłoszeniach do rejestracji przez GIODO. Poza zgłoszenie wykraczały m.in. następujące dane: nr telefonu, nr rachunku bankowego, nr NIP, nr PESEL. Urząd Gminy nie wywiązał się zaś z obowiązku wynikającego z art. 41 ust. 2 ustawy o ochronie danych osobowych i nie zgłosił GIODO zwiększenia zakresu danych osobowych gromadzonych w tych zbiorach.

   ABI wyjaśnił, że: *„Wynikało to z przeoczenia kierowników komórek organizacyjnych, którzy przekazywali zakres przetwarzanych przez siebie danych celem ujęcia w zgłoszeniu do GIODO. W części zbiorów danych zakres mógł również z upływem czasu się zwiększyć. Zostanie to zaktualizowane"*.

   (dowód: akta kontroli str. 290-291, 282-284)

---

[18] Badaniem nie objęto czterech zbiorów danych osobowych.

[19] Centralna Ewidencja i Informacja o Działalności Gospodarczej.

[20] Zarządzeniem nr 15/12 z dnia 27 lutego 2012 r. o upoważnieniu do podpisywania dokumentów związanych z wprowadzaniem wniosków do CEIDG.

[21] Dz. U. z 2016 r. poz. 1829, ze zm.

3. Urząd Gminy nie zgłosił GIODO aktualizacji czterech zbiorów danych, które nie były prowadzone w Urzędzie, do czego był zobowiązany art. 41 ust. 4 ustawy o ochronie danych osobowych. Zbiory te były prowadzone w Gminnym Ośrodku Pomocy Społecznej (program 500+, świadczenia socjalne o charakterze materialnym, uzależnienia, świadczenia rodzinne).

   ABI wyjaśnił, że: *„Zdania związane z przetwarzaniem danych w tych zbiorach są realizowane przez jednostkę bezpośrednio podlegającą dla Wójta Gminy – Gminny Ośrodek Pomocy Społecznej. Dlatego dokonaliśmy zgłoszenia w ten sposób"*.
   (dowód: akta kontroli str. 110-117, 258-259, 282-284)

Ocena cząstkowa

Dane przetwarzane przez Urząd Gminy były niezbędne do realizacji zadań, w związku z którymi je prowadzono. Urząd Gminy nie wywiązał się z obowiązku poinformowania GIODO o powierzeniu przetwarzania danych osobowych na podstawie umowy zawartej z podmiotem zewnętrznym. W 11 (z 21) zbiorach przetwarzał zaś dane osobowe w zakresie większym niż określony w zgłoszeniu zbioru danych do ujęcia w rejestrze prowadzonym przez GIODO. Urząd Gminy nie przekazywał też GIODO aktualizacji prowadzonych zbiorów danych osobowych oraz zakresu danych osobowych przetwarzanych w zbiorach. Spełniono natomiast wymogi dostępu do zbiorów danych osobowych, których administratorami były podmioty zewnętrzne.

3. Sposób przechowywania oraz fizycznego zabezpieczenia danych

Opis stanu faktycznego

Spośród 24 zbiorów danych prowadzonych w Urzędzie Gminy, dziewięć było prowadzonych w formie elektronicznej, a pozostałe w formie papierowej. W regulacjach wewnętrznych nie określono sposobu fizycznego zabezpieczenia pomieszczeń, w których możliwy był dostęp do zbiorów danych osobowych (poza wskazaniem, że pomieszczenie powinno być chronione przed pożarem zgodnie z instrukcją p/poż, zaś w razie potrzeby należy zastosować dodatkowe zabezpieczenie fizyczne, tj. kraty i rolety antywłamaniowe – odpowiednio § 15 ust. 5 i 6 Polityki bezpieczeństwa). Brak uregulowań w tym zakresie szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

W zgłoszeniach zbiorów danych do rejestracji w rejestrze prowadzonym przez GIODO wskazano, że zastosowano środki fizycznej ochrony danych, w tym alarm przeciwwłamaniowy i monitoring przy użyciu kamer przemysłowych, zabezpieczenie pomieszczeń przed skutkami pożaru za pomocą gaśnicy wolnostojącej, zbiory danych w formie papierowej przechowywano w niemetalowych zamykanych szafach oraz zastosowano urządzenia UPS. Oględziny pomieszczeń, w których były gromadzone zbiory danych wykazały, że wszystkie środki fizycznej ochrony wymienione w zgłoszeniach do GIODO były stosowane. (dowód: akta kontroli str. 9-35, 266-267)

Urząd Gminy posiadał informacje z zakresu inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Było to zgodne z § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI. (dowód: akta kontroli str. 95-97)

W latach 2016 – 2017 (do 5 kwietnia) nie dokonywano likwidacji sprzętu będącego nośnikami danych (komputerów, pendrive). W 2017 roku zlecono podmiotowi zewnętrznemu, w ramach umowy serwisowej, naprawę serwera[22]. Umowa zawierała zapisy zobowiązujące wykonawcę do zachowania poufności informacji i danych nabytych w związku z realizacją przedmiotu umowy (zarówno w trakcie trwania umowy jaki i po jej ustaniu) oraz nakładała na wykonawcę obowiązek przetwarzania danych osobowych zgodnie z umową i ustawą o ochronie danych osobowych. Ponadto w umowie zobowiązano wykonawcę do: [1] zastosowania środków technicznych i organizacyjnych zapewniających ochronę danych osobowych; [2] dopuszczenia do przetwarzania danych osób posiadających upoważnienie; [3] prowadzenia rejestru osób upoważnionych; [4] zapewnienia, aby osoby które będą miały dostęp do danych zachowały je w tajemnicy.
(dowód: akta kontroli str. 98, 148-151, 265)

[22] Systemu Fiskus.

W § 15 ust. 3 Polityki bezpieczeństwa pracowników Urzędu Gminy zobowiązano do zamykania na klucz pomieszczeń, w których są przetwarzane dane osobowe podczas nieobecności osób upoważnionych. W § 24 Polityki bezpieczeństwa określony został sposób ochrony danych osobowych w zbiorach nieinformatycznych. Pracowników Urzędu Gminy zobowiązano do zabezpieczania dokumentów i wydruków w meblach biurowych zamykanych na klucz oraz niszczenia wydruków zawierających dane osobowe w sposób uniemożliwiający osobom nieuprawnionym zapoznanie się z ich treścią. W tym celu Urząd Gminy wyposażono w trzy niszczarki zlokalizowane w Urzędzie Stanu Cywilnego, Księgowości oraz Referacie Rolnictwa i Gospodarki Komunalnej.

(dowód: akta kontroli str. 9-35, 161)

Wg § 20 Instrukcji zarządzania nośniki informatyczne miały być przechowywane w miejscach, do których dostęp posiadały wyłącznie osoby upoważnione. Natomiast w § 21 Instrukcji użytkowników nośników przenośnych służących do przetwarzania danych osobowych zobowiązano do niezwłocznego informowania ABI o zakresie i rodzaju zbieranych danych osobowych oraz o celu ich przetwarzania. Nie ustanowiono zakazu wynoszenia nośników danych zawierających dane osobowe poza siedzibę Urzędu Gminy. Z kolei w § 22 Instrukcji zarządzania pracowników użytkujących przenośny komputer zobowiązano do zachowania szczególnej ostrożności podczas transportu i przechowywania komputera poza obszarem ochrony danych, w celu zapobieżenia dostępowi do danych osoby niepowołanej. Nie określono innych zasad korzystania ze służbowych urządzeń informatycznych poza siedzibą jednostki. W § 18 Instrukcji zarządzania wskazano, że do przesyłania danych przy połączeniach w sieci publicznej (Internet) powinny być wykorzystywane tylko kanały transmisji wykorzystywane przez autoryzowane programy. Nie określono również zasad użytkowania sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych.

ASI wyjaśnił, że: *„Pracownicy Urzędu Gminy nie mogą wykorzystywać sprzętu prywatnego do celów służbowych. Nie mają oni również możliwości podłączenia się do systemów informatycznych Urzędu Gminy poza jego siedzibą"*.

(dowód: akta kontroli str. 36-52, 283-285)

Sprzątanie pomieszczeń Urzędu Gminy powierzono pracownikowi zatrudnionemu w pełnym wymiarze czasu pracy. W obowiązujących w Urzędzie Gminy regulacjach pracowników zobowiązano do zabezpieczania dokumentów w zamykanych szafkach podczas nieobecności lub zakończeniu pracy (co opisano powyżej). Sprzątaniem pomieszczenia serwerowni zajmował się ASI, który wyjaśnił, że: *„Dostęp do pomieszczenia serwerowni powsiadam ja, jako Administrator Systemu Informatycznego, Administrator Bezpieczeństwa Informacji, a także Administrator Danych Osobowych – Wójt Gminy. Ja zajmuję się dbaniem o porządek w tym pomieszczeniu"*. (dowód: akta kontroli str. 283-285)

Zgodnie z § 15 ust. 1 Instrukcji zarządzania, przeglądy i konserwacje systemu miały być wykonywane przez ASI doraźnie. Wyjaśnił on, że: *„Przeglądy i konserwacje systemu są dokonywane doraźnie w zależności od zapotrzebowania"*. W § 15 ust. 2 Instrukcji zobowiązano użytkowników zbiorów danych zawierających dane osobowe do dokonywania, przy współudziale ASI, przeglądów i sprawdzania poprawności tych zbiorów, nie rzadziej niż raz na dwa tygodnie. W Urzędzie nie posiadano dokumentacji potwierdzającej przeprowadzenie przeglądów i sprawdzania poprawności zbiorów danych zawierających dane osobowe przy współudziale ASI, co szerzej opisano w dalszej części wystąpienia pokontrolnego w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 36-52)

W Urzędzie Gminy przyjęto regulacje dotyczące tworzenia kopii zapasowych w celu zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym. Częstotliwość tworzenia kopii zapasowych została określona w § 11 Instrukcji zarządzania. Wynosiła dwa razy w miesiącu dla systemu finansowo-księgowego oraz nie rzadziej niż raz na miesiąc dla pozostałych systemów. Stosownie do wymogów określonych w pkt IV załącznika do rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, w Urzędzie Gminy zabezpieczano przetwarzanie danych poprzez sporządzanie kopii zapasowych z sześciu systemów wykorzystywanych do gromadzenia danych

osobowych[23]. Kopie zapasowe systemu SmartDoc były sporządzane codziennie, a dla pozostałych pięciu systemów – z częstotliwością mniejszą niż określona w obowiązujących uregulowaniach. Nie wszystkie kopie były tworzone na oddzielnych nośnikach informatycznych oraz nie były testowane pod kątem ich przydatności do odtworzenia systemów informatycznych w przypadku awarii, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 36-52, 171-174)

W Urzędzie Gminy nie opracowano procedur postępowania w przypadku braku długotrwałego zasilania oraz niszczenia zbędnych kopii zapasowych, w sytuacji stwierdzenia utraty ich przydatności do odtworzenia systemu w przypadku awarii. Zgodnie z § 13 Instrukcji zarządzania system i urządzenia informatyczne służące do przetwarzania danych osobowych, które są zasilane energią elektryczną zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej. Minimalne zabezpieczenie systemu i urządzeń polegało na wyposażeniu serwerów i stacji roboczych w zasilacze awaryjne UPS. (dowód: akta kontroli str. 36- 52, 265)

W okresie objętym kontrolą nie wystąpiły przypadki fizycznej utraty danych. W Urzędzie nie opracowano procedur określających sposób postępowania w takiej sytuacji. ABI wyjaśnił, że: *„W Urzędzie nie występowały tego typu zdarzenia, dlatego nie opracowaliśmy takich procedur. Zostanie to w najbliższym czasie uzupełnione"*.

(dowód: akta kontroli str. 265, 282-284)

Ustalone nieprawidłowości

W działalności jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. W Urzędzie Gminy nie przeprowadzano przeglądów i konserwacji zbiorów danych zawierających dane osobowe, które – zgodnie z § 15 ust. 2 Instrukcji zarządzania – miały być przeprowadzane przez użytkowników tych zbiorów, przy udziale ASI, nie rzadziej niż raz na dwa tygodnie.

   ASI wyjaśnił, że przeglądy i konserwacje zbiorów danych zawierających dane osobowe prowadzonych w systemach informatycznych dokonywane są doraźnie, w zależności od zapotrzebowania. (dowód: akta kontroli str. 91-94, 282-284)

2. Kopie zapasowe z pięciu systemów były sporządzane z częstotliwością mniejszą niż określona w § 11 Instrukcji zarządzania. Zgodnie z tym zapisem kopie awaryjne dla systemu finansowo-księgowego powinny być tworzone dwa razy w miesiącu, dla pozostałych systemów nie rzadziej niż raz na miesiąc, a każda kopia powinna być zapisywana na oddzielnym nośniku informatycznym. Kopie zapasowe nie były również testowane pod kątem ich przydatności do odtworzenia systemu w przypadku awarii. I tak:
   - w 2016 roku sporządzono 22 kopie zapasowe systemu finansowo-księgowego Budżet / Płace, a do 27 marca 2017 r. dziesięć, z tego dwie zapisano na oddzielnym nośniku informatycznym,
   - kopie zapasowe systemu finansowo-księgowego FISKUS nie były w 2016 roku zapisywane na oddzielnych nośnikach informatycznych i na serwerze, a w 2017 roku jedną zapisano na oddzielnym nośniku informatycznym i dwie na serwerze,
   - w 2016 roku nie tworzono kopii zapasowych systemu Cheops, a w 2017 roku utworzono jedną kopię, która została zapisana na oddzielnym nośniku informatycznym,
   - w 2016 roku utworzono 10 kopii zapasowych systemu Selwin, zaś w 2017 roku trzy, z tego jedną zapisano na oddzielnym nośniku informatycznym,
   - w 2016 roku utworzono dwie kopie zapasowe systemu USCwin, a w 2017 roku jedną (żadna nie została zapisana na oddzielnym nośniku informatycznym).

[23] Nie były sporządzane kopie zapasowe z systemu Źródło, CEIDG oraz Ewopis. Serwery tych systemów nie znajdowały się w Urzędzie Gminy. Pracownicy posiadali dostęp zdalny do tych systemów.

ASI wyjaśnił, że: *„Kopie zapasowe były sporządzane przez pracowników merytorycznych. Mniejsza częstotliwość ich sporządzania oraz nietworzenie kopii na oddzielnych nośnikach wynika prawdopodobnie z przeoczenia"*. Wyjaśnił również, że kopie zapasowe nie były testowane, bowiem: *„Po zapisaniu kopii przeprowadzane jest sprawdzenie czy plik został zapisany. W przypadku systemu Cheops sprawdzam czy jest możliwość jego uruchomienia (czy kopia została sporządzona prawidłowo). W przypadku pozostałych systemów nie było do tej pory konieczności skorzystania z kopii zapasowych, dlatego nie wykonywaliśmy ich testowania. Prawdopodobnie w przypadku awarii musielibyśmy skorzystać z pomocy firmy obsługującej dany system"*. Wyjaśnił też, że przechowywanie nośników informatycznych z kopiami zapasowymi w tym samym pomieszczeniu w którym użytkowano system informatyczny służący do przetwarzania danych osobowych wynikało z tego, że: *„Kopie zapasowe były tworzone przez pracowników obsługujących systemy. Dostosujemy sposób postępowania z kopiami zapasowymi do uregulowań obowiązujących w Urzędzie. Kopie będą przechowywane w Skarbcu Urzędu"*.

(dowód: akta kontroli str. 36-52, 132-133, 171-174)

Ocena cząstkowa

W Urzędzie Gminy przyjęto regulacje określające zasady postępowania z dokumentami i wydrukami zawierającymi dane osobowe oraz zobowiązano pracowników do zabezpieczenia dokumentów podczas ich nieobecności. Wprawdzie w uregulowaniach tych nie określono form ochrony fizycznej zbiorów danych osobowych, jednak zastosowano, wszystkie środki fizycznej ochrony wskazane w zgłoszeniach zbiorów danych do rejestru prowadzonego przez GIODO. Nie przeprowadzano natomiast przeglądów i konserwacji systemów informatycznych wykorzystywanych do prowadzenia zbiorów danych zawierających dane osobowe, a kopie zapasowe wykonywano niezgodnie z przyjętymi uregulowaniami (z częstotliwością mniejszą niż wskazana w Instrukcji zarządzania oraz nie zapisywano ich na oddzielnych nośnikach informatycznych i nie testowano).

4. Skuteczność przyjętych rozwiązań dotyczących dostępu do poszczególnych systemów informatycznych i usług sieciowych przed nieuprawnionym dostępem, przejęciem lub niszczeniem danych

Opis stanu faktycznego

W Urzędzie Gminy[24] nie były przeprowadzane okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 265, 275)

Wszyscy pracownicy posiadali login i hasło do sprzętu informatycznego służącego do przetwarzania danych osobowych, a pracownicy, którzy obsługiwali systemy informatyczne służące do prowadzenia zbiorów danych także loginy i hasła do tych systemów. Długość i poziom skomplikowania hasła określone były w § 5 Instrukcji zarządzania. Przeprowadzone oględziny wykazały, że wymogi te zostały spełnione przez wszystkich pracowników. (dowód: akta kontroli str. 36-52, 260-264)

Oględziny wszystkich 21 stacji roboczych i laptopów wykorzystywanych do przetwarzania danych osobowych wykazały, że konfiguracja zabezpieczeń dostępu do pięciu systemów informatycznych służących do przetwarzania danych osobowych oraz systemu operacyjnego komputerów nie wymuszała okresowej zmiany hasła użytkowników (zmiana mogła nastąpić jedynie z inicjatywy użytkownika). W § 5 ust. 3 Instrukcji zarządzania wskazano, że zmiana hasła następuje nie rzadziej niż co 30 dni. Niezapewnienie tego wymogu opisano szerzej w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Ponadto stwierdzono, że wszyscy użytkownicy posiadali uprawnienia administratora, co umożliwiało instalację programów i konfigurację systemu (co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości"), 20 komputerów posiadało dostęp do „otwartego" Internetu, na wszystkich możliwe było odczytanie danych znajdujących się na zewnętrznym nośniku danych, w tym na 13 komputerach – po uprzednim wpisaniu hasła. (dowód: akta kontroli str. 260-264)

[24] Do 31 marca 2017 r.

W Urzędzie Gminy nie prowadzono rejestru dostępu do systemu. Dostęp do sieci Internet był obsługiwany przy użyciu routera CISCO, który został nabyty w ramach realizacji projektu pn. *„Wdrażanie elektronicznych usług dla ludności w województwie podlaskim"*. ASI nie dokonywał analizy logów usług sieciowych.

ASI wyjaśnił, że: *„Router jest obsługiwany przez Urząd Marszałkowski Województwa Podlaskiego. Został na nim zastosowany firewall systemowy. Nie posiadam dostępu do konfiguracji routera oraz do rejestru systemowego. W związku z tym nie dokonywałem analizy znajdujących się tam danych. Nie wiem ile czasu przechowywane są na nim logi oraz jakie dane są zawarte w rejestrze routera"*. (dowód: akta kontroli str.164-168, 282)

Sieć Wi-Fi, którą posiadał Urząd Gminy była zabezpieczona przed nieuprawnionym dostępem za pomocą klucza dostępowego. W obowiązujących w Urzędzie Gminy regulacjach nie opracowano procedur / uregulowań dotyczących dostępu do sieci Wi-Fi.
(dowód: akta kontroli str. 8-52, 260-264)

W Urzędzie Gminy w latach 2016 – 2017 (do 31 marca) nie stwierdzono przypadków wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji. Nie wystąpiła konieczność odtworzenia zbiorów danych z kopii bezpieczeństwa. W celu ochrony systemów, na każdym komputerze zainstalowano program antywirusowy, pełniący jednocześnie funkcję firewalla. Jego ustawienia nie pozwalały na odpowiedni nadzór nad dostępem użytkowników do „otwartego" Internetu (co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości"). Oprogramowania aktualizowały się automatycznie. (dowód: akta kontroli str. 260-264)

Serwer poczty Urzędu Gminy znajdował się na platformie regionalnej Wrota Podlasia, utworzonej w wyniku realizacji projektu pn. *„Wdrażanie elektronicznych usług dla ludności w województwie podlaskim"*. Ustawienia poczty pozwalały na zabezpieczenie przed wiadomościami typu SPAM, a programu antywirusowego chroniły przed przesyłaniem plików zawierających szkodliwe oprogramowanie.
(dowód: akta kontroli str. 118-123, 164-168)

Oględziny 21 komputerów (stacji roboczych i laptopów) wykazały, że na dwóch zainstalowano system Windows 8, na 12 – system Windows 7, a na siedmiu – Windows XP. Na żadnym nie stwierdzono zainstalowanego programu, na który Urząd Gminy nie posiadał licencji. (dowód: akta kontroli str. 260-264)

W Urzędzie Gminy nie opracowano procedur dotyczących płatności realizowanych drogą elektroniczną. Były one realizowane za pośrednictwem elektronicznego systemu zdalnej obsługi bankowej. Dane przekazywane między Urzędem Gminy a bankiem były przesyłane łączem szyfrowanym. Realizacja zleconych przez Urząd Gminy przelewów była wykonywana przez upoważnionych pracowników, którzy posiadali klucze autoryzujące, zabezpieczone kodami PIN. (dowód: akta kontroli str. 235-242)

Wydatki Urzędu Gminy poniesione na zakup programów związanych z bezpieczeństwem danych wynosiły w 2016 roku 1,5 tys. zł. Do 31 marca 2017 roku Urząd Gminy nie ponosił takich wydatków. (dowód: akta kontroli str. 108-109)

Ustalone nieprawidłowości

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

1. W Urzędzie Gminy w latach 2016 – 2017 (do 31 marca) nie były przeprowadzane okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji. Było to niezgodne z wymogiem określonym w § 20 ust. 2 pkt 3 rozporządzenia KRI.

   ASI wyjaśnił, że: *„ Nie były przeprowadzane takie analizy. Wynikało to z tego, że ryzyka w porównaniu do lat ubiegłych znacząco nie zmieniały się"*.
   (dowód: akta kontroli str. 265, 281)

2. W systemach operacyjnych wszystkich 21 stanowisk komputerowych nie wprowadzono rozwiązań wymuszających na użytkownikach okresową zmianę haseł, mimo takiego obowiązku określonego w § 5 ust. 3 Instrukcji zarządzania oraz wskazania w zgłoszeniach do rejestracji zbiorów danych w rejestrze zbiorów prowadzonym przez GIODO, iż wymóg ten jest spełniony w przypadku sześciu zbiorów danych. W pięciu

systemach informatycznych, w których były gromadzone dane osobowe również brak było ustawień wymuszających okresową zmianę haseł.

ASI wyjaśnił: „*W obowiązujących w Urzędzie Gminy uregulowaniach jest zawarty zapis zobowiązujący użytkowników do zmiany hasła co 30 dni. Użytkownicy są zobowiązani do stosowania tych uregulowań. W przypadku gdy będzie możliwe wprowadzenie takich ustawień zastosujemy takie rozwiązania*". (dowód: akta kontroli str. 271-272, 275-277)

3. Wszystkim użytkownikom komputerów, wykorzystywanych do przetwarzania zbiorów danych osobowych, zostały nadane uprawnienia administratora systemu operacyjnego. Ponadto urządzenia te posiadały dostęp do „otwartego" Internetu, zaś ustawienia firewalla nie umożliwiały kontroli dostępu do stron internetowych.

   Zgodnie z § 6 ust. 4 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną stosuje się wysoki poziom zabezpieczeń.

   W zgłoszeniach zbiorów danych do rejestracji w rejestrze prowadzonym przez GIODO wskazano, że w przypadku 14 zbiorów zastosowano środki bezpieczeństwa na poziomie podstawowym, a w pięciu na poziomie podwyższonym[25] oraz, że dane osobowe są przetwarzane bez użycia żadnego z urządzeń służącego do przetwarzania danych osobowych połączonego z siecią publiczną.

   ASI wyjaśnił, że: „*Nadanie uprawnień administratora każdemu z pracowników wynikało z uproszczenia dostępu i zostanie zmienione. Program antywirusowy został zainstalowany z ustawieniami domyślnymi. Ustawienia programu antywirusowego umożliwiające kontrolę dostępu do stron internetowych również zostaną zmienione*".
   (dowód: akta kontroli str. 110-117, 164-168, 260-264, 275-277)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że z dniem 8 kwietnia 2014 r. producent oprogramowania zakończył udzielanie wsparcia dla systemu operacyjnego Windows XP, a w konsekwencji oprogramowanie to, zainstalowane na siedmiu komputerach, może nie dość skutecznie chronić dane przetwarzane na tych urządzeniach.

ASI wyjaśnił, że: „*Ze względów finansowych wykorzystujemy ten system na komputerach zakupionych w 2007 i 2009 roku. System ten będzie przez nas w miarę możliwości finansowych Urzędu Gminy stopniowo wycofywany z użytkowania*".
(dowód: akta kontroli str. 260-264, 276-278)

Ocena cząstkowa

Przyjęte w Urzędzie Gminy rozwiązania nie w pełni zabezpieczały przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych. Na komputerach wykorzystywanych do przetwarzania danych osobowych, zastosowano zabezpieczenia w postaci programu antywirusowego z funkcją firewalla, którego konfiguracja nie umożliwiała pełnej ochrony, ze względu na posiadanie uprawnień administratora przez użytkowników tych urządzeń. Wprawdzie wprowadzono zabezpieczenia dostępu, w postaci indywidualnego loginu i hasła, do systemów informatycznych oraz poszczególnych programów wykorzystywanych do przetwarzania danych osobowych, jednak konfiguracja zabezpieczeń dostępu do systemu operacyjnego nie wymuszała okresowej zmiany hasła użytkownika. Nie prowadzono okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji. Ponadto NIK zwraca uwagę, że na siedmiu (z 21) komputerach zainstalowano systemem operacyjny, którego producent zakończył udzielanie wsparcia, co wpływa na obniżenie skuteczności ochrony danych przetwarzanych przy jego wykorzystaniu.

[25] W czterech zgłoszeniach z 1999 roku nie wskazano zastosowanego poziomu zabezpieczeń.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[26] wnosi o:

1. Terminowe zgłaszanie do GIODO zmian zakresu danych gromadzonych w zarejestrowanych zbiorach danych osobowych przetwarzanych w Urzędzie Gminy oraz zaktualizowanie pozostałych informacji przekazanych do GIODO.
2. Przygotowywanie okresowych planów sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ich ochronie oraz sporządzanie kompletnych sprawozdań z przeprowadzenia czynności kontrolnych obejmujących sprawdzanie zgodności przetwarzania danych osobowych z przepisami.
3. Dostosowanie zapisów Polityki bezpieczeństwa i Instrukcji zarządzania do wymogów § 4 i § 5 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz ujęcie w wykazie zbiorów danych osobowych wszystkich wykorzystywanych zbiorów.
4. Stosowanie obowiązujących w Urzędzie Gminy regulacji dotyczących okresowej zmiany haseł.
5. Dostosowanie środków bezpieczeństwa do poziomów bezpieczeństwa przetwarzania danych osobowych, o których mowa w § 6 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych.
6. Wykonywanie, zgodnie z obowiązującymi regulacjami wewnętrznymi, kopii bezpieczeństwa danych przetwarzanych z wykorzystaniem programów.
7. Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, a także przeglądów i konserwacji systemów informatycznych.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

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 Białymstoku.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK, proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i 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.

Białystok, dnia 20 kwietnia 2017 r.

Kontroler
Beata Palinowska
starszy inspektor kontroli państwowej

Palinowska Beata
podpis

DYREKTOR DELEGATURY
Najwyższej Izby Kontroli w Białymstoku
z up. WICEDYREKTOR
Robert Skwarko

podpis

[26] Dz. U. z 2017 r. poz. 524, ze zm. Ustawa zwana dalej „ustawą o NIK".