NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.411.001.06.2017
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
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontroler	Piotr Jurkin – starszy inspektor k. p., upoważnienie do kontroli nr LBI/41/2017 z 7 marca 2017 r. Maciej Brzosko – starszy inspektor k. p., upoważnienie do kontroli nr LBI/42/2017 z 14 marca 2017 r. (dowód: akta kontroli str. 1-4)
Jednostka kontrolowana	Starostwo Powiatowe w Kolnie, ul. 11 Listopada 1, 18-500 Kolno[1]
Kierownik jednostki kontrolowanej	Stanisław Wiszowaty – Starosta Kolneński[2] (dowód: akta kontroli str. 5)

II. Ocena kontrolowanej działalności[3]

Ocena ogólna

Starostwo nie podejmowało wszystkich działań wymaganych przepisami prawa oraz regulacjami wewnętrznymi, w celu zapewnienia ochrony posiadanych zasobów informacyjnych, co obniżało poziom ich bezpieczeństwa. Nie wywiązano się również z obowiązku zgłoszenia Generalnemu Inspektorowi Ochrony Danych Osobowych (dalej: „GIODO") do zarejestrowania 10 z 58 przetwarzanych zbiorów danych osobowych. W trzech zaś zbiorach (z 29 objętych analizą) przetwarzano dane osobowe, które nie były wykorzystywane do realizacji zadań, w związku z którymi Starostwo je prowadziło.

Uzasadnienie oceny ogólnej

W Starostwie nie opracowano polityki bezpieczeństwa informacji, mimo takiego wymogu określonego 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]. Wprowadzone regulacje wewnętrzne[5] dotyczyły jedynie danych osobowych i nie zawierały elementów wymaganych w § 4 pkt 4 i § 5 pkt 5 i 7 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[6]. Regulacje te nie były też w pełni przestrzegane.

W Starostwie nie dokonywano sprawdzenia zgodności przetwarzania danych osobowych z przepisami prawa, stosownie do obowiązku wynikającego z art. 36a ust. 2 pkt 1a w związku z art. 36b ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[7] oraz nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, mimo takiego wymogu zawartego w § 20 ust. 2 pkt 3 rozporządzenia KRI.

---

[1] Dalej: „Starostwo".

[2] Pełnił funkcję od 1 grudnia 2014 r. do dnia zakończenia kontroli.

[3] 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. Okres objęty kontrolą: od 1 stycznia 2016 r. do dnia zakończenia czynności kontrolnych.

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

[5] Opisane w Polityce bezpieczeństwa przetwarzania i ochrony danych osobowych (dalej: „polityka bezpieczeństwa") oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych (dalej: „instrukcja zarządzania").

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

[7] Dz. U. 2016 poz. 922.

III. Opis ustalonego stanu faktycznego

1. Dokumentacja i procedury dotyczące ochrony danych

1.1. Dokumentacja dotycząca ochrony danych osobowych

Opis stanu faktycznego

W okresie objętym kontrolą Starosta nie powołał Administratora Bezpieczeństwa Informacji (dalej: „ABI"). W związku z tym, na podstawie art. 36b ustawy o ochronie danych osobowych, zadania mu przypisane wykonywał administrator danych osobowych, czyli Starosta. Wyjaśnił on: *„Do dnia 25 czerwca 2015 r. na ABI wyznaczony był pracownik zatrudniony na stanowisku Informatyka w Starostwie. W związku ze zmianą w 2015 roku przepisów o ochronie danych osobowych polegających na określeniu zakresu zadań dla ABI oraz wymogów jakie powinna spełniać osoba powołana do pełnienia tej funkcji (art. 36a) ABI został odwołany (...)*". Obowiązująca w Starostwie polityka bezpieczeństwa przewidywała funkcjonowanie stanowiska ABI oraz określała dla niego zakres zadań. W Starostwie w 2016 roku nie przeprowadzano kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Analiza zakresów obowiązków 15 pracowników upoważnionych do przetwarzania danych wykazała, że we wszystkich przypadkach osoby te zobowiązano do znajomości m.in. treści ustawy o ochronie danych osobowych. (dowód: akta kontroli str. 6-28, 177-192)

W Starostwie prowadzono ewidencję osób upoważnionych do przewarzania danych osobowych zawierającą wszystkie elementy określone w art. 39 ust. 1 ustawy o ochronie danych osobowych i obejmującą wszystkich pracowników (46), którym udzielono upoważnień. Analiza zakresów obowiązków 20 losowo wybranych pracowników merytorycznych jednostki wykazała, że 17 posiadało upoważnienia do przetwarzania zbiorów danych osobowych w wersji papierowej lub w systemach informatycznych, adekwatne do przypisanych im obowiązków. Jeden z pracowników od 5 maja 2011 r. do 18 stycznia 2017 r. nie posiadał takiego upoważnienia w stosunku do części realizowanych zadań, a dwóm pozostałym nie przypisano w zakresach czynności zadań wynikających z nadanych upoważnień, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 29-50)

W Starostwie nie opracowano procedur (instrukcji) dotyczących nadzoru nad rodzajem przetwarzanych danych osobowych i osób wprowadzających takie dane do danego zbioru, ani wskazaniem odbiorcy takich danych. Starosta wyjaśnił, że: *„Bezpośrednią kontrolą nad przekazywaniem danych ze zbiorów osobowych sprawują Naczelnicy Wydziałów w uzgodnieniu z Radcą Prawnym i Starostą. Regulację wynikają z ogólnych zapisów w zakresach czynności naczelników w ramach prowadzonego nadzoru nad wydziałem – „Bieżące nadzorowanie i kontrola realizacji zadań na poszczególnych stanowiskach pracy utworzonych w Wydziale oraz zapewnienie wykonywania wszystkich zadań określonych w regulaminie organizacyjnym Starostwa jako zadania wspólne wydziałów"*.

Do 15 marca 2017 r. Starostwo zgłosiło GIODO do zarejestrowania 36 (z 58) prowadzonych zbiorów danych osobowych. Wszystkie zgłoszenia zawierały elementy wymagane art. 41 ust. 1 ustawy o ochronie danych osobowych. Nie stwierdzono przypadku odmowy rejestracji zgłoszonego zbioru danych oraz nie występowano do GIODO o wykreślenie z rejestru zbiorów danych osobowych. W związku ze zmianami przepisów prawa dotyczących ośmiu zgłoszonych / zarejestrowanych zbiorów danych osobowych, dokonano ich aktualizacji[8], polegającej m.in. na rozszerzeniu zakresu przetwarzania danych. Dwanaście z pozostałych 22 niezgłoszonych do rejestracji zbiorów danych osobowych, na podstawie art. 43 ust. 1 pkt 4, 8 i 9 ustawy o ochronie danych osobowych, nie podlegało temu obowiązkowi[9].

[8] Po jednej w 2010 roku i 2015 roku oraz sześć w 2014 roku.

[9] Dotyczyło to: [1] akt osobowych pracowników Starostwa, [2] akt osobowych zatrudnionych na stanowiskach kierowników jednostek administracyjnych, [3] ewidencji i danych osobowych pracowników Starostwa, [4] ewidencji zapotrzebowania i naboru kandydatów do pracy, [5] ewidencji księgowo-finansowej, [6] dane płacowe, [7] ewidencji środków trwałych i pozostałych środków trwałych, [8] sprawozdań finansowych, bilansów [9] danych osób ubezpieczonych, [10] ewidencji kontrahentów, [11] ewidencji podatkowej zatrudnionych oraz [12] rejestru stowarzyszeń i fundacji.

Niezgłoszenie zaś do rejestracji 10[10] kolejnych zbiorów danych osobowych szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 10, 22, 51-53, 97-102, 163)

Obowiązki związane z administrowaniem systemami, w których gromadzono i przetwarzano dane osobowe powierzono informatykowi, do zadań którego należało m.in.: zabezpieczenie zbiorów danych prowadzonych w systemach informatycznych, administrowanie i zarządzanie serwerami i przeciwdziałanie dostępowi osób niepowołanych do systemów, w których przetwarzane są takie dane. Informatyk posiadał stosowne upoważnienia do przetwarzania danych osobowych we wszystkich systemach, dla których administratorem danych był Starosta Kolneński. (dowód: akta kontroli str. 103-113)

W Starostwie nie przeprowadzano corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, wynikających z § 20 ust. 2 pkt 14 rozporządzenia KRI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 102)

W okresie objętym kontrolą pracownicy Starostwa nie uczestniczyli w szkoleniach z zakresu bezpieczeństwa przetwarzania danych / informacji. Starosta wyjaśnił, że spowodowane to było brakiem środków finansowych. Dodał, że *„W bieżącym roku planuje się przeszkolenie pracowników w zakresie ochrony danych osobowych podczas przeprowadzenia audytu wewnętrznego"*. W 2016 roku Starostwo nie było kontrolowane przez podmioty zewnętrzne w zakresie bezpieczeństwa danych. W okresie tym nie wpływały również do jednostki skargi związane z przypadkami ujawnienia danych osobowych. (dowód: akta kontroli str. 22, 51-53)

Ustalone nieprawidłowości

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

1. W Starostwie w 2016 roku nie przeprowadzano kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, mimo takiego obowiązku wynikającego z art. 36a ust. 2 w związku z art. 36b ustawy o ochronie danych osobowych. Starosta wyjaśnił, że powodem tego było przeoczenie i nadmiar innych obowiązków. (dowód: akta kontroli str. 22, 51-53)

2. Trzech pracowników Starostwa (z 20 objętych badaniem) posiadało upoważnienia do przetwarzania danych osobowych i prowadzenia zbiorów takich danych nieadekwatne do zakresu ich obowiązków. Osoba zatrudniona w Wydziale Budżetu i Finansów od 5 maja 2011 do 18 stycznia 2017 r. nie posiadała upoważnienia do dostępu i przetwarzania danych osobowych w stosunku do części realizowanych zadań. Natomiast dwóm pracownikom Wydziału Komunikacji i Transportu nie przypisano w zakresach czynności zadań wynikających z nadanych upoważnień. Było to niezgodne z art. 37 ustawy o ochronie danych osobowych oraz § 20 ust. 2 pkt 4 rozporządzenia KRI, przewidujących, że do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie, zaś osoby zaangażowane w proces przetwarzania informacji powinny posiadać stosowne uprawnienia i uczestniczyć w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań i obowiązków. Skarbnik Powiatu wyjaśniła, że: *„(...) było to zwykłe przeoczenie związane ze zmianą programu finansowo-księgowego Quorum."* Natomiast Naczelnik Wydziału Komunikacji i Transportu wyjaśnił, że: *(...) powodem nieprzypisania w zakresach czynności dwóm pracownikom Wydziału zadań określonych w upoważnieniach do dostępu i przetwarzania danych osobowych była nieuwaga. Określając zakres zadań dla pracowników do przetwarzania danych, nie zwróciłem dostatecznej uwagi na rozbieżności wynikające z zakresu czynności oraz upoważnień".*

   W trakcie kontroli (7 kwietnia 2017 r.) dostosowano zakresy czynności pracowników do wykonywanych zadań. (dowód: akta kontroli str. 23, 35-38, 40-50, 116-119)

[10] Dotyczyło to: [1] książki orzeczeń lekarskich wraz z listami stawiennictwa osób do kwalifikacji wojskowej, [2] planu obrony cywilnej, [3] planu operacyjnego ochrony przed powodzią, [4] planu organizacji wczesnego ostrzegania, [5] planu organizacji systemu wykrywania i alarmowania, [6] planu działania stałego dyżuru, [7] planu działania powiatowego ośrodka analiz danych i alarmowania, [8] planu działania powiatowej drużyny pobierania próbek, [9] planu zarządzania kryzysowego, [10] rejestru klubów sportowych.

3. Nie zgłoszono GIODO do rejestracji 10 z 58 zbiorów danych prowadzonych w Starostwie, co naruszało wymogi art. 40 ustawy o ochronie danych osobowych. Starosta wyjaśnił, że było to wynikiem przeoczenia. Przedmiotowe zbiory danych zgłoszono GIODO w trakcie kontroli. (dowód: akta kontroli str. 51-93, 102)

4. W Starostwie nie przeprowadzano corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, mimo obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI. W konsekwencji niemożliwa była rzetelna ocena skuteczności przyjętych rozwiązań w zakresie ochrony danych osobowych. Starosta wyjaśnił, że spowodowane to było: *„(...) brakiem środków finansowych w budżecie powiatu. W projekcie budżetu na 2017 rok w Wydziale Spraw Społecznych i Promocji Powiatu zostały zaplanowane środki finansowe na wykonanie audytu wewnętrznego z zakresu bezpieczeństwa informacji w wysokości 8.000 zł".* (dowód: akta kontroli str. 22, 51-56)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że obowiązująca w Starostwie polityka bezpieczeństwa przewidywała wyznaczenie ABI, jako osoby odpowiedzialnej za bezpieczeństwo danych, będącej jednym z elementów zabezpieczenia organizacyjnego danych osobowych. Pomimo to w okresie objętym kontrolą nie wyznaczono osoby na to stanowisko. Starostwa wyjaśnił, że: *„(...) nie powołano Administratora Bezpieczeństwa Informacji mimo tego, że w Polityce bezpieczeństwa przetwarzania i ochrony danych osobowych przewidziano takie stanowisko, ponieważ do pełnienia tej funkcji należałoby zatrudnić osobę posiadającą odpowiednie kwalifikacje i fachową wiedzę z zakresu ochrony danych osobowych, natomiast z uwagi na ograniczone środki finansowe w budżecie powiatu, decyzja o zatrudnieniu została odłożona w czasie. Informuję jednocześnie, że planowane jest powołanie (jeszcze w tym roku) Administratora Bezpieczeństwa Informacji w Starostwie, prawdopodobnie pełnienie tej funkcji zostanie zlecone firmie zewnętrznej specjalizującej się w zakresie ochrony danych osobowych".* (dowód: akta kontroli str. 6-10, 114-115, 177-192)

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

Opis stanu faktycznego

W Starostwie, zarządzeniem Nr 8/11 Starosty Kolneńskiego z 5 kwietnia 2011 r., wprowadzono politykę bezpieczeństwa oraz instrukcję zarządzania.
(dowód: akta kontroli str. 177-200)

Poza ww. dokumentami nie wprowadzano innych regulacji, procedur, instrukcji dotyczących gromadzenia i przetwarzania zasobów informatycznych oraz danych osobowych.

Wprowadzona polityka bezpieczeństwa nie zawierała kompletu elementów określonych w § 4 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, zaś w wykazie zbiorów danych osobowych ujęto 42 z 58 prowadzonych przez Starostwo zbiorów danych. Ponadto przyjęta instrukcja zarządzania nie zawierała elementów wymaganych § 5 pkt 5 i 7 ww. rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". W pkt 5 ust. 2 części IV polityki bezpieczeństwa wskazano, że w systemie informatycznym obowiązują zabezpieczenia na poziomie wysokim, co szerzej opisano w pkt 4 niniejszego wystąpienia.
(dowód: akta kontroli str. 10, 102, 177-200)

Starostwo nie opracowało polityki bezpieczeństwa informacji, o której mowa w § 2 pkt 15 w związku § 20 ust. 1 rozporządzenia KRI, zaś przyjęte rozwiązania opisane w instrukcji zarządzania i w polityce bezpieczeństwa dotyczyły ochrony danych osobowych. Nie aktualizowano przyjętych regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 10, 22, 177-200)

Spośród 14 systemów informatycznych wykorzystywanych do przetwarzania danych osobowych[11], 10 zapewniało realizację wymogów określonych w § 7 ust. 3 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, tj. możliwość sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące m.in. daty pierwszego wprowadzenia danych osobowych czy identyfikatora użytkownika wprowadzającego dane osobowe do systemu. Niezrealizowanie wymogów określonych w § 7 ust. 3 ww. rozporządzenia w odniesieniu do czterech pozostałych systemów szerzej opisano poniżej, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 120-162)

Ustalone nieprawidłowości

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

1. Wykaz zbioru danych osobowych zawarty w polityce bezpieczeństwa był niepełny. Nie zawierał bowiem 16 z 58 posiadanych przez Starostwo zbiorów danych. Starosta wyjaśnił, że: *„Spowodowane to było nieaktualizowaniem Polityki bezpieczeństwa"*.
(dowód: akta kontroli str. 51-53, 102, 177-192)

2. Przyjęta w Starostwie polityka bezpieczeństwa i instrukcja zarządzania nie zawierały elementów wymaganych odpowiednio w § 4 pkt 4 oraz § 5 pkt 5 i 7 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, tj.: sposobu przepływu danych pomiędzy systemami, miejsca i czasu przechowywania kopii zapasowych, a także sposobu realizacji wymogów określonych w § 7 ust. 1 pkt 4 ww. rozporządzenia. Starosta wyjaśnił, że: *„W trakcie tworzenia Polityki bezpieczeństwa przetwarzania i ochrony danych osobowych, było brak wiedzy na temat przepływu tych informacji pomiędzy systemami. W Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych przeoczono konieczność zawarcia zapisów wymaganych § 5 pkt 5 i 7 rozporządzenia Ministra"*.
(dowód: akta kontroli str. 51-53, 102, 177-200)

3. W Starostwie nie opracowano polityki bezpieczeństwa informacji, o której mowa w § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI oraz nie aktualizowano regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia, mimo takiego wymogu określonego w § 20 ust. 2 pkt 1 ww. rozporządzenia. Starosta wyjaśnił, że powodem było przeoczenie i nadmiar innych obowiązków. Dodał, że: *„W związku z nadmiernym obciążeniem pracownika na stanowisku „Informatyk" nie przeprowadzono aktualizacji dokumentacji. Po otrzymaniu wyników kontroli zostanie dokonana aktualizacja dokumentacji"*. (dowód: akta kontroli str. 10, 22, 51-53)

4. Cztery z 14 programów wykorzystywanych do przetwarzania danych osobowych nie spełniało wymogów określonych w § 7 ust. 3 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych. Nie umożliwiało bowiem sporządzenia każdej osobie, której dane przetwarzano, raportu zawierającego – w powszechnie zrozumiałej formie – informacje dotyczące m.in. daty pierwszego wprowadzenia danych osobowych oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu. Starosta wyjaśnił, że: *„Do dnia rozpoczęcia kontroli nie miałem świadomości o istnieniu takiego obowiązku. Nie mieliśmy też wiedzy, że programy informatyczne nie posiadają takiej opcji w swoich strukturach. Pierwszy raport został wydrukowany podczas kontroli. Niezwłocznie podejmiemy działania w celu dostosowania pozostałych programów do wymogów określonych w § 7 ust. 3 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych"*.
(dowód: akta kontroli str. 51-53, 120-162)

Ocena cząstkowa

Starostwo nie w pełni wywiązało się z obowiązku opracowania wymaganej dokumentacji i procedur dotyczących ochrony danych. Przyjęte dokumenty: polityka bezpieczeństwa i instrukcja zarządzania nie zawierały wszystkich elementów określonych w rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych. Ponadto, mimo wymogu określonego w § 20 ust. 1 i 2 pkt 1 rozporządzenia KRI, nie opracowano polityki

[11] QuorumFK, Quorum Płace, Płatnik, Home Banking, Qdeklaracje, RWD-2, CEPIK, Portal Starosty, Foris, EWID2007, EKSMOoN, Quoru Kadry, Resto, Smart Doc. Administratorem danych dla systemu CEPIK, EKSMOoN i RWD-2 były podmioty zewnętrzne.

bezpieczeństwa informacji i nie aktualizowano regulacji wewnętrznych, a wbrew przepisom § 20 ust. 2 pkt 14 ww. rozporządzenia nie przeprowadzano corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji. GIODO nie zgłoszono zaś w celu zarejestrowania 10 z 58 przetwarzanych zbiorów danych osobowych. Z kolei w czterech z 14 programów, w których przetwarzano dane osobowe, wbrew przepisom § 7 ust. 3 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, nie umożliwiono każdej osobie, której dane przetwarzano, sporządzenia raportu zawierającego informacje dotyczące m.in.: daty pierwszego wprowadzenia danych osobowych i identyfikatora użytkownika wprowadzającego dane osobowe do systemu. Starosta nie wywiązał się także z obowiązku przeprowadzania sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

2. Zakres przetwarzanych zasobów informatycznych

Opis stanu faktycznego

W Starostwie przetwarzano dane w 58 zbiorach danych, z których cztery prowadzono wyłącznie w wersji elektronicznej[12], 19 w formie papierowej i elektronicznej, a pozostałe tylko w formie papierowej. GIODO zgłoszono 36 zbiorów danych, co szerzej opisano w pkt 1 niniejszego wystąpienia.

Spośród zgłoszonych GIODO zbiorów danych, w 35 przypadkach zakres przetwarzanych danych był zgodny ze zgłoszeniem do GIODO. W jednym przypadku gromadzono dane nie objęte zgłoszeniem, co szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

Analiza 29 zbiorów[13] danych prowadzonych w poszczególnych komórkach organizacyjnych Starostwa wykazała, że w 26 przypadkach zakres przetwarzanych danych był niezbędny do realizacji zadań przypisanych tym komórkom. W trzech kolejnych zbiorach gromadzono dane, które nie były wykorzystywane przy realizacji zadań, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Dla wszystkich zbiorów danych (do których dostęp posiadali pracownicy Starostwa), z wyjątkiem CEPIK, EKSMOoN i RWD-2[14], administratorem danych, w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych, był Starosta Kolneński. Starostwo uzyskało dostęp do zbioru danych CEPIK na podstawie umowy DMD/0004/99 z 6 czerwca 1999 r., zawartej z Polską Wytwórnią Papierów Wartościowych S.A. Starostwo spełniło wymogi dostępu do tego zbioru danych, które zawarte zostały w załączniku nr 5, dotyczącym wymagań techniczno-organizacyjnych pomieszczeń, w których zlokalizowano sprzęt komputerowy systemów teleinformatycznych. Pomieszczenia te zabezpieczono bowiem alarmem przeciwwłamaniowym, w oknach zainstalowano kraty, zaś sześć użytkowanych komputerów wyposażono w UPS oraz zablokowano możliwość połączenia z Internetem. Pracownicy Starostwa obsługujący ww. system posługiwali się indywidualną kartą użytkownika zabezpieczoną kodem PIN.

Certyfikaty, loginy i hasła dostępu do systemów EKSMOoN i RWD-2 dla pracowników Starostwa nadawały podmioty zewnętrzne.

(dowód: akta kontroli str. 23, 39, 97-101, 164-167, 170, 202-209, 217-221, 308)

Ustalone nieprawidłowości

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

1. Starostwo nie zrealizowało wymogu, wynikającego z art. 41 ust. 2 ustawy o ochronie danych osobowych i nie zgłosiło GIODO informacji o rozszerzeniu zakresu przetwarzanych danych w jednym ze zbiorów danych osobowych (rejestr sprzętu pływającego i kart wędkarskich). Starosta wyjaśnił, że powodem niezgłoszenia było przeoczenie. (dowód: akta kontroli str. 97-101, 170-172)

[12] EWID 2007, Cepik, Hom Banking oraz SmartDoc.

[13] 14 prowadzonych w formie elektronicznej i 15 w formie papierowej.

[14] Centralna Ewidencja Pojazdów i Kierowców, Elektroniczny Krajowy System Monitoringu Orzekania o Niepełnosprawności, Rejestr wniosków i decyzji o pozwoleniu na budowę i rejestr zgłoszeń budowy.

2. W trzech poniżej wymienionych zbiorach gromadzono i przetwarzano dane osobowe, które nie były wykorzystywane przy realizacji zadań, w związku z którymi je prowadzono.
   - W Wydziale Budownictwa i Ochrony Środowiska w formie papierowej prowadzono zbiór danych dotyczący sprzętu pływającego i kart wędkarskich. Analiza 10 (ze 112 spraw) wykazała, że w ośmiu przypadkach, oprócz danych zgłoszonych GIODO, dodatkowo przetwarzano serię i nr dowodu osobistego. Jak wyjaśniła naczelnik Wydziału: *„W celu prawidłowego prowadzenia postępowań związanych z wydawaniem kart wędkarskich wystarczające są dane wskazane w zgłoszeniu do GIODO, tj. imię i nazwisko, data urodzenia i miejsce urodzenia oraz adres zamieszkania. Całkowicie zbędne są pozostałe dane dotyczące serii nr dowodu osobistego dostarczanego organowi wraz z innymi dokumentami (...)".*
   - W Wydziale Spraw Społecznych i Promocji Powiatu w formie elektronicznej oraz papierowej (teczki spraw) prowadzono dwa rejestry: stowarzyszeń i klubów sportowych. Analiza akt 10 (z 84) zarejestrowanych stowarzyszeń wykazała, że we wszystkich przypadkach rejestr zawierał oprócz imion i nazwisk członków zarządu i organu kontroli wewnętrznej, także daty urodzenia tych osób i nr Pesel. Zgodnie z art. 40b ust. 1 ustawy z dnia 7 kwietnia 1989 r. Prawo o stowarzyszeniach[15], w rejestrze tym zamieszcza się jedynie imiona i nazwiska członków zarządu oraz organu kontroli wewnętrznej jeśli jest przewidziany. Ustawa nie przewidywała przetwarzania dat urodzenia. Natomiast analiza wpisów i akt 10 spraw (z 15 ujętych w rejestrze klubów sportowych) wykazała, że w sześciu przypadkach ewidencja zawierała imiona i nazwiska oraz daty urodzenia członków zarządu i organu kontroli wewnętrznej, zaś w pozostałych czterech dodatkowo nr Pesel ww. osób. Przepisy § 5 rozporządzenia Ministra Sportu i Turystyki z dnia 18 października 2011 r. w sprawie ewidencji klubów sportowych[16] nie przewidują gromadzenia nr Pesel przez organ prowadzący rejestr.

   Gromadzenie danych osobowych niewykorzystywanych do realizacji zadań narusza przepis art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, zgodnie z którym przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest to niezbędne dla zrealizowania obowiązku wynikającego z przepisu prawa. Naczelnik Wydziału Budownictwa i Ochrony Środowiska wyjaśniła, że: *„Nie zdawaliśmy sobie sprawy, że nie możemy przetwarzać danych innych niż zgłoszonych do GIODO i wyłącznie niezbędnych do realizacji przypisanych nam zadań".* Natomiast Naczelnik Wydziału Spraw Społecznych i Promocji Powiatu wyjaśnił: *„Nie mieliśmy świadomości, że nie możemy przetwarzać danych innych niż niezbędne do realizacji przypisanych nam zadań. Petenci składający dokumenty do wydziału dołączali do nich także dane niewymagane przepisami prawa, tj. datę urodzenia czy nr Pesel, a my nieświadomie je przetwarzaliśmy. Zwrócę uwagę podległym pracownikom, aby przetwarzano wyłącznie dane niezbędne do realizowanych zadań".* (dowód: akta kontroli str. 164-169)

Ocena cząstkowa

Starostwo przetwarzając dane osobowe wykroczyło poza uprawnienia wynikające z przepisów oraz realizowanych zadań. Nie wywiązano się z obowiązku poinformowania GIODO o rozszerzeniu zakresu przetwarzania danych w jednym zbiorze danych osobowych. W kolejnych trzech z 29 analizowanych zakres gromadzonych informacji wykraczał zaś poza dane niezbędne do realizacji zadań, w związku z którymi Starostwo prowadziło przedmiotowe zbiory danych. Spełniono natomiast wymogi dotyczące dostępu do zbioru danych osobowych, których administratorem były podmioty zewnętrzne.

[15] Dz. U. z 2017 r. poz. 210.
[16] Dz. U. Nr 243 poz. 1449.

3. Sposób przechowywania oraz fizycznego zabezpieczenia danych

Opis stanu faktycznego

W Starostwie 19 z 58 zbiorów danych, w których przetwarzane były dane osobowe prowadzono w wersji papierowej i elektronicznej, a cztery w formie elektronicznej. Do tego celu wykorzystywano 13 różnych aplikacji / programów informatycznych[17]. W Starostwie wdrożono elektroniczny obieg dokumentów prowadzony w systemie Elektroniczne Zarządzanie Dokumentacją. Zbiory danych prowadzone w formie papierowej przechowywane były w szafach zamykanych na klucz (za wyjątkiem przypadku przechowywania części dokumentacji księgowej w Wydziale Budżetu i Finansów w szafach niezabezpieczonych przed nieuprawnionym dostępem, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości").

(dowód: akta kontroli str. 201-222)

W części IV pkt 1 ppkt 1 polityki bezpieczeństwa wskazano zabezpieczenia fizyczne danych osobowych w postaci zainstalowanego systemu alarmowego w budynku Starostwa, zamykanych na klucz wszystkich pomieszczeń, w których prowadzi się zbiory i przetwarza dane osobowe oraz wyposażenie pomieszczeń w szafy z zamkami. Przeprowadzone 17 marca 2017 r. oględziny pomieszczeń Starostwa wykazały spełnienie tych wymagań. Główna serwerownia Starostwa wyposażona była w drzwi antywłamaniowe i przeciwpożarowe (klucze do tego pomieszczenia posiadały jedynie trzy osoby w Starostwie[18]), redundantną klimatyzację, czujnik ruchu oraz czujnik przeciwpożarowy. Pomieszczenie zasilane było odrębnym węzłem zasilającym.

(dowód: akta kontroli str. 177-192, 201-225)

Informatyk Starostwa na bieżąco gromadził dane, o których mowa w § 20 ust. 2 pkt 2 rozporządzenia KRI, tj. prowadził aktualną inwentaryzację sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującą ich rodzaj i konfigurację. Każde urządzenie komputerowe Starostwa posiadało tzw. „metrykę komputera". Ponadto Informatyk Starostwa prowadził listę komputerów i drukarek sieciowych, która zawierała informacje dotyczące: IP urządzenia, adres Mac, nazwę urządzenia w sieci, imię i nazwisko posiadacza sprzętu, numer pokoju w których urządzenie się znajduje, nr inwentarzowy i ewentualne uwagi dotyczące rodzaju sprzętu (laptop, drukarka, ksero, serwer, itp.).

(dowód: akta kontroli str. 226-229)

W okresie objętym kontrolą, tj. od 1 stycznia 2016 r. nie dokonywano likwidacji sprzętu będącego nośnikiem danych w postaci komputerów, dysków lub pendrive. Ostatnia taka utylizacja miała miejsce 29 września 2015 r. Obejmowała ona osiem komputerów, jeden zestaw komputerowy (stacja robocza i monitor), cztery monitory, trzy zasilacze UPS, jedno urządzenie sieciowe switch, oraz jedną kserokopiarkę. Utylizacji dokonał podmiot zewnętrzny. Na pytanie dotyczące przygotowania nośników danych do utylizacji, Informatyk wyjaśnił: *„Każdy dysk twardy jest permanentnie kasowany z jakichkolwiek danych. Wykonuje się tzw. zerowanie dysku. Dla pewności przy najbliższej utylizacji sprzętu komputerowego, dyski, na których przetwarzane były wrażliwe dane osobowe pozostaną na stanie Starostwa w pokoju 219."* (dowód: akta kontroli str. 226-228, 289-305)

Za prowadzenie archiwum zakładowego odpowiedzialny był Wydział Organizacyjny Starostwa. Analiza dokumentacji brakowania dokumentacji niearchiwalnej za 2016 rok wykazała, że w tym okresie nie przekazywano do utylizacji płyt CD/DVD. Brakowanie dokumentacji papierowej w 2016 roku następowało w oparciu o przepisy rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej[19] – na wniosek Starosty Kolneńskiego, za zgodą Archiwum Państwowego. Brakowania dokumentów dokonał podmiot zewnętrzny 29 grudnia 2016 r.

---

[17] Quorum: Kadry, Płace, F-K, QDeklaracje; ZUS Płatnik, Home Banking, RWD-2, RESTO, CEPIK, Portal Starosty, FORIS, EWID, EKSMOoN.

[18] Informatyk, Naczelnik Wydziału Spraw Społecznych i Promocji Powiatu oraz pracownik Wydziału Geodezji, Kartografii, Katastru i Gospodarki Nieruchomościami Starostwa.

[19] Dz. U. z 2015 r. poz. 1743.

Do niszczenia bieżących dokumentów, niewymagających archiwizacji, np. w przypadku błędów w piśmie, nieprawidłowego wydruku, itp. wykorzystywano 15 niszczarek znajdujących się na wyposażeniu Starostwa, jednak nie opracowano w tym zakresie żadnych wytycznych lub procedur. (dowód: akta kontroli str. 226-228)

Zgodnie z obowiązującym w Starostwie regulaminem pracy[20], pracownikom zabroniono wynoszenia z miejsca pracy, bez zgody przełożonego, rzeczy będących własnością pracodawcy, wykorzystywania, bez zgody przełożonego sprzętu i materiałów należących do pracodawcy do celów niezwiązanych z wykonywaną pracą bądź niezgodnie z przeznaczeniem. Wyniesienie poza teren zakładu pracy dokumentów i przydzielonego wyposażenia, z wyjątkiem telefonu komórkowego, wymagało zgody bezpośredniego przełożonego. Starosta wyjaśnił, że nie wydawał zgody na wykorzystywanie laptopów służbowych poza siedzibą Starostwa. W regulacjach wewnętrznych Starostwa nie określono zasad wykorzystywania urządzeń prywatnych do celów służbowych. Starosta wyjaśnił: *„Pracownicy nie mogą używać swojego sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych. Nie mogą podłączać swojego sprzętu do infrastruktury Starostwa".* (dowód: akta kontroli str. 230-238, 285-286)

Sprzątaniem pomieszczeń Starostwa zajmowały się dwie pracownice oraz jedna stażystka. Sprzątanie odbywało się w godzinach między 10:30 a 18:30 (w przypadku stażystki) oraz od 14:00 lub 15:00 w przypadku dwóch pracownic Starostwa. Z wyjaśnień Naczelnika Wydziału Spraw Społecznych i Promocji Powiatu Starostwa wynika, że pomieszczenia serwerowni sprzątane były pod nadzorem jednej z trzech osób posiadających klucze i upoważnienie do dostępu do tego pomieszczenia. (dowód: akta kontroli. str. 240-254)

Zgodnie z obowiązującym regulaminem pracy, każdy pracownik obowiązany był do uporządkowania swego stanowiska i zabezpieczenia po zakończeniu pracy powierzonych mu pomieszczeń i ich wyposażenia, tj.: urządzeń, sprzętu, dokumentów, pieczęci, walorów pieniężnych. (dowód: akta kontroli str. 232-237)

Zgodnie z pkt 10 ust. 2 instrukcji zarządzania systemami informatycznymi, przeglądu i konserwacji systemów informatycznych dokonywał informatyk, na wniosek naczelnika wydziału. Z wyjaśnień Informatyka wynika, że w okresie objętym kontrolą naczelnicy wydziałów nie zgłaszali mu potrzeby przeprowadzenia takich konserwacji, jednakże regularnie dokonywał sprawdzenia administrowanych systemów, używając do tego celu dedykowanego oprogramowania. (dowód: akta kontroli str. 17-24, 111-127)

Zgodnie pkt 7 ust. 1 ppkt 1 instrukcji zarządzania systemami informatycznymi, kopie zapasowe miały być wykonywane codziennie i sprawdzane raz w miesiącu pod kątem ich przydatności do odtworzenia danych. Na dzień 22 marca 2017 r. w Starostwie zabezpieczano przetwarzanie danych poprzez sporządzanie kopii zapasowych 10 z 14 systemów wykorzystywanych do przetwarzania danych. Kopie bezpieczeństwa programów QNT F-K, Kadry, Płace, Qdeklaracje oraz EWID i EZD wykonywane były automatycznie raz dziennie i zapisywane na dwóch serwerach Starostwa. Ponadto w przypadku EWID doraźnie zgrywano kopie bezpieczeństwa na płyty CD i przechowywano je w sejfie. Kopie bezpieczeństwa Home Banking, ZUS Płatnik oraz RESTO wykonywano raz w tygodniu ręcznie. W przypadku programu FORIS kopie bezpieczeństwa wykonywane były automatycznie przy aktualizacjach programu (około raz w miesiącu). Zagadnienie szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Kopie bezpieczeństwa przechowywano w serwerowni na serwerze głównym, na serwerze NAS (mieszczącym się w głównej serwerowni) oraz na komputerach stacjonarnych w pokojach 106, 205, 206, 219, 308. Kopie bezpieczeństwa przechowywane były na dwóch różnych urządzeniach za wyjątkiem kopii bezpieczeństwa FORIS i RESTO, które przechowywane były na jednym urządzeniu. W przypadku systemów RWD-2, CEPiK i EKSMOoN danymi zarządzały podmioty zewnętrzne i one były odpowiedzialne za tworzenie kopii bezpieczeństwa. Testowanie kopii sporządzonych przez Starostwo odbywało się doraźnie przy aktualizacjach systemów / programów.

(dowód: akta kontroli str. 193-200, 223-225)

[20] Zarządzenie Nr 30/11 Starosty Kolneńskiego z dnia 1 grudnia 2011 r. w sprawie ustalenia regulaminu pracy w Starostwie Powiatowym w Kolnie.

W Starostwie nie określono procedur na wypadek wystąpienia sytuacji nadzwyczajnej (np. awaria, długotrwały brak zasilania). Starostwo posiadało dostęp do agregatu prądotwórczego (John Deer 700 TSS, o mocy 48 kW), stanowiącego własność Podlaskiego Urzędu Wojewódzkiego w Białymstoku, który został użyczony Starostwu 27 czerwca 2007 r. Urządzenie to nie było na stałe zainstalowane w budynku Starostwa. Na dzień rozpoczęcia kontroli agregat znajdował się w Urzędzie Miasta Kolno. Z 27 komputerów stacjonarnych poddanych oględzinom 17 marca 2017 r., 24 posiadały zasilacze awaryjne UPS.
(dowód: akta kontroli str. 201-222, 226-228)

Ustalone nieprawidłowości

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

1. Przeprowadzone 17 marca 2017 r. oględziny pomieszczeń Starostwa, w których przetwarzano dane osobowe, wykazały m.in., że w Wydziale Budżetu i Finansów część dokumentacji księgowej za 2015 rok, znajdującej się w pokoju 205, przechowywano w szafach, które nie były wyposażone w zamki, co naruszało wymogi ustalone w pkt 2 ust. 1 części IV polityki bezpieczeństwa przetwarzania i ochrony danych. Skarbnik Powiatu wyjaśniła: *„(...)dokumenty zostały omyłkowo wstawione do niezamykanych szaf i już zostały zabezpieczone w zamykanej na klucz szafie. Ponadto, w celu poprawy warunków zabezpieczenia przechowywanej dokumentacji w Wydziale Budżetu i Finansów planuje się zakup szaf i regałów biurowych".*
(dowód: akta kontroli str. 201-222, 254-256)

   Przeprowadzone w dniu 10 kwietnia 2017 r. oględziny wykazały przeniesienie tych dokumentów do szaf wyposażonych w zamek. (dowód: akta kontroli str. 176)

2. Kopie bezpieczeństwa systemów Home Banking, ZUS Płatnik oraz RESTO wykonywano raz w tygodniu ręcznie, zaś programu FORIS – automatycznie przy aktualizacjach programu (około raz w miesiącu), podczas gdy zgodnie pkt 7 ust. 1 ppkt 1 Instrukcji zarządzania systemami informatycznymi, powinny być one wykonywane codziennie. Informatyk wyjaśnił: *„Programy Resto, Foris czy ZUS Płatnik są wykorzystywane raz, dwa razy w tygodniu, także ich codzienne archiwizowanie jest nielogiczne i zajmuje niepotrzebnie dodatkowe miejsce na serwerze. Wystarczy w tym przypadku kopia tygodniowa. W przypadku Home Bankingu została wdrożona codzienna archiwizacja bazy danych. Polityka bezpieczeństwa i Instrukcja zarządzania systemami informatycznymi wymagają uaktualnienia. Po kontroli NIK zgłoszony zostanie problem Staroście".* (dowód: akta kontroli str. 223-225, 289-305)

Ocena cząstkowa

Sposób przechowywania i fizycznego zabezpieczenia danych osobowych nie w pełni odpowiadał regulacjom określonym w polityce bezpieczeństwa i instrukcji zarządzania systemami informatycznymi (w polityce bezpieczeństwa poziom zabezpieczenia danych określono jako wysoki). Część dokumentacji księgowej Wydziału Budżetu i Finansów przechowywano w szafach, które nie były wyposażone w zamki, a kopie bezpieczeństwa danych systemu Home Banking, ZUS Płatnik, RESTO i FORIS wykonywano rzadziej niż przewidywała to instrukcja zarządzania systemami informatycznymi. W Starostwie prowadzono inwentaryzację sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującą ich rodzaj i konfigurację, a Informatyk na bieżąco prowadził przeglądy i konserwację tych urządzeń. W regulaminie pracy zobowiązano m.in. pracowników do zabezpieczania dokumentów przed dostępem osób nieupoważnionych po zakończeniu pracy.

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

Opis stanu faktycznego

W Starostwie nie opracowywano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 226-228)

Analiza wszystkich 58 kont użytkowników korzystających z 13 systemów / programów informatycznych (badaniem nie objęto systemu EZD), w których były przetwarzane dane osobowe, wykazała, że 55 użytkowników posiadało upoważnienie Starosty do przetwarzania danych w tych systemach / programach oraz indywidualne loginy i hasła do systemów operacyjnych i poszczególnych systemów / programów. Wyjątek stanowiły trzy osoby, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Zakres nadanych upoważnień do przetwarzania danych osobowych 20 z 46 pracowników Starostwa w odniesieniu do ich zakresów czynności opisano w pkt 1 niniejszego wystąpienia pokontrolnego.

Osobom, które zaprzestały świadczenia pracy w 2016 roku niezwłocznie usunięto konta użytkowników w systemach informatycznych, do których miały dostęp[21].

(dowód: akta kontroli str. 226-228, 257-262, 173)

Logi usług, ruchu sieciowego i danych wychodzących z sieci lokalnej Starostwa do sieci publicznej archiwizowane były na serwerze Starostwa. Dostęp do tych danych odbywał się przez usługę serwera FTP, do której miał dostęp Naczelnik Wydziału Spraw Społecznych i Promocji Powiatu oraz Informatyk. W przypadku logów aplikacji, w których przetwarzane były dane osobowe (QNT, RESTO, EWID, Płatnik, Home Banking, EZD) zapisywane były one w tych programach i kopiach bezpieczeństwa. Z wyjaśnień Informatyka wynika, że dane w logach analizowane były ręcznie doraźnie, w przypadku awarii, błędu programu lub systemu. (dowód: akta kontroli str. 289-305)

Zgodnie z pkt 4.1. Instrukcji zarządzania systemem informatycznym, każdorazowe uwierzytelnienie użytkownika w systemie następowało po podaniu identyfikatora i hasła. Ponadto polityka bezpieczeństwa przetwarzania i ochrony danych osobowych, w pkt 5 ust. 2 części IV wskazywała, że w systemie informatycznym obowiązują zabezpieczenia na poziomie wysokim, zaś najważniejszymi zastosowanymi środkami zabezpieczenia danych w systemach informatycznych w Starostwie są hasła dostępu do systemu i hasła dostępu do aplikacji (zgodnie z pkt 5 ust. 3 polityki). Powyższe dokumenty nie wskazywały wymagań dotyczących haseł dla systemów i aplikacji. Przeprowadzone 17 marca 2017 r. oględziny 30 z 62 komputerów wykorzystywanych w Starostwie oraz 14 systemów informatycznych, w których przetwarzano dane osobowe wykazały, że na żadnym urządzeniu hasła dostępowe do systemu operacyjnego nie spełniały wymagań przewidzianych dla środków bezpieczeństwa na poziomie wysokim, określonych w rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych. System nie wymuszał bowiem zmiany hasła nie rzadziej niż co 30 dni, jego odpowiedniej długości (minimum osiem znaków) oraz jakości (powinno się składać z małych i wielkich liter, cyfr lub znaków specjalnych). W trzech z 14 systemów informatycznych, w których przetwarzano dane osobowe hasła dostępowe nie spełniały tych wymagań. Zagadnienie szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 177-222)

W okresie objętym kontrolą Starostwo nie korzystało z usług naprawy komputerów lub laptopów, świadczonych przez firmy zewnętrzne. Informatyk wyjaśnił: *„Jeżeli uszkodzona jest część komputera stacjonarnego i naprawa jest opłacalna, to zostaje ta część wymieniona ręcznie przeze informatyka. Wszelkie awarie sprzętu serwerowego, komputerowego i dotyczące laptopów z projektu EZD Urzędu Marszałkowskiego są wpierw zgłaszane przez System Obsługi Zgłoszeń. Na podstawie zgłoszenia serwisant z Urzędu Marszałkowskiego Województwa Podlaskiego przyjeżdża, wykonuje demontaż dysków twardych, które zostają w Starostwie i zabiera awaryjny sprzęt do naprawy. Do tej pory nie korzystaliśmy z naprawy gwarancyjnej tych urządzeń".*

(dowód: akta kontroli str. 226-228, 289-305)

Starostwo posiadało jeden router Wi-Fi zlokalizowany w sekretariacie Starostwa. Dostęp do sieci bezprzewodowej zabezpieczony był hasłem. Oględziny 30 z 62 komputerów wykorzystywanych w Starostwie wykazały, że żadne urządzenie nie posiadało dostępu do tej sieci. (dowód: akta kontroli str. 201-222)

---

[21] W 2016 roku z czterema osobami rozwiązano umowy o pracę. W czasie zatrudnienia dwie osoby miały dostęp do CEPiK i dwie do EWID i QNT Kadry.

Między 1 stycznia 2016 r. a 31 marca 2017 r. nie stwierdzono w Starostwie przypadków wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, fizycznej utraty danych i konieczności odtwarzania zbioru danych ze sporządzonych kopii bezpieczeństwa. W celu ochrony systemów zastosowano zabezpieczenia w postaci firewalla sprzętowego o nazwie Mikrotik RB2011UiAS-RM, który uniemożliwiał osobom nieuprawnionym dostęp do sieci wewnętrznej Starostwa (LAN). Firewall zainstalowany był na styku łącza głównego internetowego (WAN) i sieci wewnętrznej Starostwa. Ponadto oględziny 30 z 62 użytkowanych w Starostwie komputerów wykazały, że na czterech urządzeniach nie był zainstalowany program antywirusowy[22], a na kolejnych trzech aktualizacja oprogramowania antywirusowego odbywała się ręcznie. Zagadnienie szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 201-222, 226-228, 263-264)

Starostwo miało wykupioną usługę hostingu strony internetowej i domenę internetową w podmiocie zewnętrznym (home.pl). Dane przechowywano na serwerach wykonawcy usługi, który był również administratorem danych. Zgodnie z pkt 7 regulaminu sieci home.pl, podmiot realizujący usługę przetwarzał dane zgodnie z zasadami wskazanymi w ustawie o ochronie danych osobowych oraz w ustawie o świadczeniu usług drogą elektroniczną i zapewniał bezpieczeństwo zgromadzonych danych. (dowód: akta kontroli str. 263-264)

Oględziny 30 z 62 użytkowanych w Starostwie komputerów wykazały, że 23 miały zainstalowany system operacyjny Windows 7, pięć Windows 10, a dwa Windows XP i nie stwierdzono przy tym instalacji programów, na które Starostwo nie posiadało licencji. Na pięciu komputerach zainstalowane były natomiast różnego rodzaju komunikatory, a na siedmiu oprogramowanie służące do rozliczeń podatkowych. Informatyk wyjaśnił: *„Komunikatory czy programy do wysyłania Pitów były zainstalowane za zgodą Informatyka. Powyższe programy nie są zakazane".* (dowód: akta kontroli str. 201-222, 174-175)

W Starostwie nie opracowano pisemnych procedur związanych z płatnościami realizowanymi drogą elektroniczną. W obowiązującej w Starostwie polityce rachunkowości[23] wskazano osoby z Wydziału Budżetu i Finansów odpowiedzialne za dokonywanie płatności drogą elektroniczną. Skarbnik Powiatu wyjaśniła: *„Zgodnie z przyjętą w Starostwie polityką rachunkowości dotyczącą obiegu i terminarzu spływu dokumentów finansowo-księgowych wszystkie rachunki i faktury oraz inne dowody księgowe podlegające zapłacie wpływają do Skarbnika Powiatu. Dokumenty poddane są wstępnej kontroli merytorycznej i formalno-rachunkowej oraz zatwierdzane do wypłaty poprzez postawienie pieczęci i złożenie podpisu zatwierdzającego przez Skarbnika Powiatu i Starostę. Dokumenty w dalszej części są przekazywane na stanowisko podinspektora Marianny L., która zgodnie z zakresem czynności sporządza przelewy i wypłaty z rachunków bankowych za pomocą programu Home Banking, oraz sprawdza poprawność danych kontrahenta i numery rachunków bankowych z którego dokonywany jest przelew i na jaki numer bankowy mają wpłynąć środki pieniężne. Następnie pracownik drukuje listę wszystkich sporządzonych przelewów, składa podpis „sporządził" i przedkłada Skarbnikowi i Staroście do dokonania autoryzacji przelewów (złożenie podpisu). Przed autoryzacją przelewu Skarbnik dokonuje sprawdzenia poprawności wykonanych przelewów.* (dowód: akta kontroli str. 267-280)

W 2016 roku wydatki Starostwa na zakup programów związanych z zapewnieniem bezpieczeństwa przetwarzania danych wyniosły 4,4 tys. zł[24].
(dowód: akta kontroli str. 281-282)

Ustalone nieprawidłowości

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

1. W okresie objętym kontrolą, w Starostwie nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, mimo takiego wymogu zawartego w § 20 ust. 2 pkt 3 rozporządzenia KRI. Starosta wyjaśnił: *„W Starostwie*

[22] Na pozostałych urządzeń zainstalowany był program antywirusowy „G Data Security" w wersji 14.01.122 z 31 października 2016 r.
[23] Zarządzenie Nr 32/2016 Starosty Powiatu Kolneńskiego z dnia 29 grudnia 2016 r. Zmieniające zarządzenie w sprawie wprowadzenia zasad (polityki) rachunkowości).
[24] Faktura VAT Nr 1138/12/2014 z 23 grudnia 2014 r. na przedłużenie licencji programu antywirusowego na okres trzech lat.

nie było przeprowadzanych okresowych analiz ryzyka. Nie było powołanego ABI, a Informatyk z powodu natłoku obowiązków nie przeprowadzał okresowych analiz ryzyka. W 2017 roku zostanie przeprowadzona analiza ryzyka protokolarnie".

(dowód: akta kontroli str. 226-228, 285-286)

2. Trzech z 58 użytkowników kont systemów / programów informatycznych, w których były przetwarzane dane osobowe, nie posiadało stosownych upoważnień Starosty do przetwarzania tych danych. Dotyczyło to Iwony P., Justyny F. i Roberta W. N., którzy nie posiadali upoważnień do przetwarzania danych osobowych odpowiednio w programach: Resto, QNT Płace i Home Banking. Starosta wyjaśnił, że w przypadku Iwony P. i Roberta W. N. brak upoważnień był wynikiem przeoczenia. Dostęp do aplikacji QNT Płace jest zaś Justynie F. niezbędny do korzystania z aplikacji QNT Zakupy i F-K. W toku kontroli uzupełniono upoważnienia, za wyjątkiem Pani Iwony P. z uwagi na jej długoterminową nieobecność w pracy.

(dowód: akta kontroli str. 226-228, 257-262, 283-288)

3. Przeprowadzone 17 marca 2017 r. oględziny 30 komputerów (27 stacjonarnych i trzy laptopy) wykorzystywanych w Starostwie wykazały, że dostęp do systemów operacyjnych był zabezpieczony indywidualnym loginem i hasłem użytkownika, jednakże system nie wymuszał zmiany tych haseł co 30 dni oraz ich odpowiedniej jakości (brak wymogu ośmioznakowego hasła, składającego się z małych i wielkich liter, cyfr lub znaków specjalnych). Zgodnie zaś z pkt 5 ust. 2 części IV polityki bezpieczeństwa przetwarzania i ochrony danych osobowych, w systemie informatycznym obowiązywały zabezpieczenia na poziomie wysokim. Ponadto oględziny 14 systemów informatycznych, w których przetwarzano dane osobowe wykazały, że w przypadku Home Banking i FORIS systemy nie wymuszały okresowej zmiany hasła, zaś w system RWD-2 nie wymuszał długości i jakości hasła na poziomie wysokim. Informatyk wyjaśnił: *„Planowane jest wdrożenie poziomu wysokiego (czyli wymuszanie hasła co 30 dni, 8 znakowego, duże, małe litery, znaki specjalne) przy uwierzytelnianiu użytkowników do systemów operacyjnych, w których przetwarzane są dane osobowe".*

(dowód: akta kontroli str. 201-222, 289-305)

4. Przeprowadzone 17 marca 2017 r. oględziny 30 z 62 użytkowanych w Starostwie komputerów wykazały, że na czterech urządzeniach nie był zainstalowany program antywirusowy, a na kolejnych trzech aktualizacja oprogramowania antywirusowego odbywała się ręcznie. Informatyk wyjaśnił: *„W komputerach, w których doszło do usterki programu antywirusowego zostanie wdrożony program naprawczy, a aktualizacja baz danych wirusów zostanie ustawiona w tryb automatyczny".*

(dowód: akta kontroli str. 201-222, 289-305)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na niżej wymienione zagadnienia.

1. W Starostwie wykorzystywano dwa komputery z zainstalowanym systemem operacyjnym Windows XP, mimo że z dniem 8 kwietnia 2014 r. producent oprogramowania zakończył udzielanie wsparcia technicznego dla tego systemu. Zdaniem NIK, użytkowanie tego oprogramowania, może mieć wpływ na obniżenie skuteczności ochrony danych przetwarzanych na urządzeniach działających z jego wykorzystaniem. (dowód: akta kontroli str. 201-222)

2. Na pięciu komputerach (z 30 analizowanych) zainstalowane były komunikatory, co do zasady przeznaczone do użytku prywatnego, podczas gdy zgodnie z odpowiednio pkt 11 ust. 1 i 5 Instrukcji zarządzania systemami informatycznymi pracownicy nie są uprawnieni do instalacji jakiegokolwiek prywatnego oprogramowania, a połączenia z Internetem mogą używać jedynie w celach służbowych.

(dowód: akta kontroli str. 193-222)

Ocena cząstkowa

W Starostwie nie wywiązano się z obowiązku przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. W celu ochrony systemów przed nieuprawnionym dostępem, zastosowało zabezpieczenia w postaci firewalla zainstalowanego na głównym łączu internetowym. Wprowadziło również zabezpieczenia dostępu w postaci indywidualnego loginu i hasła do systemów informatycznych oraz poszczególnych programów wykorzystywanych do przetwarzania danych osobowych.

Przyjęte rozwiązania jednak nie w pełni zabezpieczały przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych. Na czterech urządzeniach (z 30 analizowanych) nie był zainstalowany program antywirusowy, a na kolejnych trzech aktualizacja oprogramowania antywirusowego odbywała się ręcznie. Konfiguracja zabezpieczeń dostępu do systemu operacyjnego objętych analizą 30 z 62 komputerów oraz trzech z 14 systemów informatycznych, w których przetwarzano dane osobowe, nie odpowiadała zabezpieczeniom na poziomie wysokim. Systemy operacyjne stacji roboczych oraz oprogramowanie Home Banking, RESTO i RWD-2 nie wymuszały bowiem okresowej zmiany hasła lub / i jego jakości oraz długości. Trzech z 58 użytkowników kont systemów / programów informatycznych, w których były przetwarzane dane osobowe, nie posiadało do tego celu stosownych upoważnień Starosty.

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[25], wnosi o:

1. Dostosowanie zapisów polityki bezpieczeństwa i instrukcji zarządzania do wymogów odpowiednio § 4 pkt 4 oraz § 5 pkt 5 i 7 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych.
2. Opracowanie i wdrożenie Polityki bezpieczeństwa informacji oraz podjęcie działań, wynikających z § 20 ust. 1 i ust. 2 pkt 1, 3 i 14 rozporządzenia KRI, w zakresie aktualizacji przyjętych regulacji wewnętrznych, prowadzenia okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz audytów wewnętrznych z zakresu bezpieczeństwa informacji.
3. Ujęcie wszystkich zbiorów wykorzystywanych w Starostwie w wykazie zbiorów danych osobowych, stanowiącym element polityki bezpieczeństwa.
4. Dostosowanie programów wykorzystywanych w Starostwie do przetwarzania danych osobowych do wymogów określonych w § 7 ust. 3 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych.
5. Przetwarzanie w zbiorach wyłącznie danych niezbędnych do realizacji obowiązków wynikających z przepisów prawa.
6. Uzupełnienie upoważnienia pracownika do przetwarzania danych osobowych w systemie RESTO.
7. Podjęcie działań w celu zabezpieczenia dostępu do systemów operacyjnych stacji roboczych i systemów wykorzystywanych do przetwarzania danych osobowych na poziomie wysokim, zgodnie z polityką bezpieczeństwa przetwarzania i ochrony danych osobowych.
8. Instalację oprogramowania antywirusowego na wszystkich urządzeniach służących do przetwarzania danych osobowych oraz zapewnienie jego automatycznej aktualizacji.

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.

[25] Dz. U. z 2017 r. poz. 524. Ustawa zwana dalej „ustawą o NIK".

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.

Kontrolerzy:

Piotr Jurkin
starszy inspektor kontroli państwowej

.....
podpis

Maciej Brzosko
starszy inspektor kontroli państwowej

.....
podpis

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

.....
podpis