NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.411.001.01.2017
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	Piotr Jurkin – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/9/2017 z 9 stycznia 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Starostwo Powiatowe w Hajnówce, ul. Aleksandra Zina 1, 17-200 Hajnówka (dalej: „Starostwo")
Kierownik jednostki kontrolowanej	Mirosław Romaniuk – Starosta Hajnowski[1] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

Starostwo nie podejmowało ogółu działań, wymaganych przepisami prawa oraz regulacjami wewnętrznymi, zmierzających do 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 sześciu z 37 przetwarzanych zbiorów danych osobowych. W trzech zaś zbiorach (z 21 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[3]. Wprowadzone regulacje wewnętrzne[4] dotyczyły jedynie danych osobowych i nie zawierały elementów wymaganych w § 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[5]. Regulacje te nie były też przestrzegane.

Ze swoich obowiązków nie wywiązywały się osoby powołane przez Starostę na stanowisko Administratora Bezpieczeństwa Informacji (dalej: „ABI") oraz Administratora Systemów Informatycznych (dalej: „ASI"). ABI nie sprawdzał bowiem zgodności przetwarzania danych osobowych z przepisami prawa oraz nie prowadził rejestru zbiorów danych przetwarzanych w Starostwie, wymaganego art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych[6]. ASI natomiast nie przeprowadzał corocznych przeglądów i konserwacji systemów informatycznych, przewidzianego w § 14 ust. 1 pkt 2 Instrukcji zarządzania, oraz nie sporządzał kopii bezpieczeństwa danych gromadzonych przy wykorzystaniu dwóch z dziewięciu systemów użytkowanych w Starostwie.

---

[1] Pełniący obowiązki od 1 grudnia 2014 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] Dz. U. 2016 poz.113, ze zm. Rozporządzenie zwane dalej: „rozporządzeniem KRI".

[4] Opisane w Instrukcji zarządzania systemem informatycznym Ochrony Danych Osobowych (dalej: „Instrukcja zarządzania") oraz Polityce Bezpieczeństwa Ochrony Danych Osobowych (dalej: „Polityka bezpieczeństwa").

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

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

Najwyższa Izba Kontroli zwraca również uwagę, że nieprzeprowadzanie testowania kopii zapasowych może narazić Starostwo na utratę danych w przypadku ich uszkodzenia, a użytkowanie sześciu komputerów z system operacyjnym nieposiadającym wsparcia technicznego producenta może mieć wpływ na skuteczność ochrony danych przetwarzanych z ich wykorzystaniem.

III. Opis ustalonego stanu faktycznego

1. Dokumentacja i procedury dotyczące ochrony danych osobowych

1.1. Dokumentacja dotycząca ochrony danych osobowych

Opis stanu faktycznego

Starostwa Hajnowski, w myśl art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[7], 4 lutego 2015 r. powołał ABI, który pełnił tą funkcję do 31 lipca 2016 r. Kolejną osobę na to stanowisko powołano 29 sierpnia 2016 r. Byli to pracownicy Starostwa, z których pierwszy był informatykiem, a drugi głównym specjalistą, zatrudnionym w Biurze Rady Powiatu Hajnowskiego. Zgłoszenia ABI do zarejestrowania przez GIODO dokonano odpowiednio 23 lutego 2015 r. i 20 września 2016 r. (19 i 22 dni po powołaniu), tj. w terminie wynikającym z art. 46b ust. 1 ustawy o ochronie danych osobowych. Przedmiotowe zgłoszenia zawierały wszystkie elementy wymagane w art. 46b ust. 2 tej ustawy. Dokonano ich na wzorach, będących załącznikami do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji[8]. W rejestrze prowadzonym przez GIODO dane ABI zgłoszone 23 lutego 2015 r. odzwierciedlały informacje wymienione w wniosku. Do 6 lutego 2017 r. natomiast nie odnotowano w nim zmian na tym stanowisku, wynikających ze zgłoszenia skierowanego 20 września 2016 r. Zawiadomienie o odwołaniu osoby pełniącej obowiązki ABI do 31 lipca 2016 r. nastąpiło z naruszeniem terminu określonego w art. 46b ust. 1 powołanej ustawy, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 4-16)

W dniu 14 marca 2016 r. Starosta zatwierdził, przygotowany przez ABI, Plan sprawdzeń na 2016 rok, o którym mowa w § 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[9]. Przewidziano w nim przeprowadzenie ośmiu przeglądów/kontroli dotyczących m.in. zgodności przetwarzania danych osobowych oraz ich zabezpieczeń z przepisami o ochronie danych osobowych w poszczególnych komórkach organizacyjnych Starostwa. Z zaplanowanych ośmiu działań przeprowadzono cztery, lecz z jednego przeglądu nie sporządzono sprawozdania[10] (przegląd ten przeprowadził ABI pełniącego obowiązki do końca lipca 2016 roku). Pozostałe trzy sprawdzenia sporządził obecny ABI. Zawierały elementy wymienione w art. 36 c ustawy o ochronie danych osobowych. Sprawozdania nie były jednak przekazywane Staroście, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 17-27, 151)

W dniu 14 lipca 2016 r., w celu zapoznania pracowników z przepisami o ochronie danych osobowych, ABI (pełniący obowiązki do końca lipca 2016 roku) przesłał do 51 osób (z 62 zatrudnionych) Instrukcję zarządzania, Politykę bezpieczeństwa oraz tekst ustawy o ochronie danych osobowych. Wyjaśnił on: *„Nie wiem dlaczego nie przekazano tych materiałów dla wszystkich pracowników Starostwa"*. Dodał, że: *„Nie podejmowałam żadnych działań w tym kierunku, nie organizowałam również żadnych szkoleń z tego zakresu dla pracowników Starostwa z powodu dużej ilości innych obowiązków"*.

(dowód: akta kontroli str. 32-35)

---

[7] Dz. U. 2016 poz. 922.
[8] Dz. U. 2014 poz. 1934. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie wzorów zgłoszeń".
[9] Dz. U. 2015 poz. 745. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie sposobu realizacji zadań ABI".
[10] Przeprowadzenie przeglądu odnotowano w książce kontroli wewnętrznych.

ABI nie prowadził rejestru zbiorów danych przetwarzanych przez administratora danych (Starostę), o którym mowa w art. 36 a ust. 2 pkt 2 ustawy o ochronie danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 36-37, 52)

W Starostwie prowadzono ewidencję osób upoważnionych do przewarzania danych osobowych zawierającą wszystkie elementy określone w art. 39 ust. 1 ustawy o ochronie danych osobowych, obejmującą wszystkich pracowników (61), którym udzielono upoważnień. Analiza zakresów obowiązków 20 losowo wybranych pracowników merytorycznych jednostki wykazała, że 18 posiadało upoważnienia do przetwarzania zbiorów danych osobowych w wersji papierowej lub w systemie informatycznym, adekwatne do przypisanych im obowiązków. Dwóch pozostałych pracowników nie posiadało upoważnień uprawniających do realizacji niektórych z przypisanych im obowiązków, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 38-51)

W Starostwie nie opracowano procedur, instrukcji dotyczących nadzoru oraz zapewnienia kontroli nad rodzajem danych osobowych i osobą wprowadzającą takie dane do danego zbioru, ani wskazaniem odbiorcy danych osobowych. Starosta wyjaśnił, że wymóg dotyczący zapewnienia kontroli w tym zakresie realizowano „(...) *poprzez ogólny zapis w zakresach czynności naczelników wydziałów Starostwa Powiatowego dotyczący nadzoru na realizacją ustawy o ochronie danych osobowych przez podległych pracowników*".

W § 4 Instrukcji zarządzania[11] określono, że dane osobowe udostępnia się podmiotom zewnętrznym w oparciu o umowę poufności. Starosta wyjaśnił, że należy przez to rozumieć powierzenie przetwarzania danych osobowych stosownie do zapisów wynikających z art. 31 ustawy o ochronie danych osobowych. W związku z tymi uregulowaniami, podpisanie przez Starostwo umowy z podmiotem zewnętrznym w zakresie udostępnienia i serwisu systemów obsługujących rozrachunki oraz kadry i płace[12], skutkowało zawarciem z wykonawcą umowy w sprawie powierzenia przetwarzania danych osobowych[13]. Umowy powierzenia przetwarzania danych osobowych nie podpisano zaś z wykonawcą kolejnej umowy z tego zakresu (z terminem obowiązywania do 31 grudnia 2018 r.), co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 52-66, 87-101)

Do 6 lutego 2017 r. Starostwo zgłosiło GIODO do zarejestrowania 32 (z 37) prowadzonych zbiorów danych osobowych, w tym dwukrotnie[14] rejestr legitymacji osób niepełnosprawnych. ABI wyjaśniła: „*Nie potrafię odpowiedzieć (...) dlaczego rejestry „Legitymacji osób niepełnosprawnych" zgłoszono dwukrotnie do GIODO. Osoby odpowiedzialne za ten fakt już nie pracują w Starostwie*". Wszystkie zgłoszenia zawierały elementy wymagane art. 41 ust. 1 ustawy o ochronie danych osobowych. Nie stwierdzono przypadku odmowy rejestracji przez GIODO zgłoszonego zbioru danych, ani aktualizacji zgłoszonych zbiorów danych/rejestrów. Niezgłoszenie od rejestracji sześciu prowadzonych zbiorów danych osobowych szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 34-35, 102-120)

Starostwo 9 września 2013 r.[15], wystąpiło o wykreślenie z rejestru zbiorów danych osobowych prowadzonego przez GIODO następujących zbiorów: „Rejestr zmian imion i nazwisk", „Ewidencja osób kierowanych do zakładu pielęgnacyjno-opiekuńczego SP ZOZ", „Rejestr wniosków uczniów szkół ponadgimnazjalnych ubiegających się o przyznanie stypendium", „Rejestr wniosków studentów ubiegających się o przyznanie stypendium" oraz „Rejestr osób skierowanych do zakładu opiekuńczo-leczniczego". Starostwo 17 września 2013 r. zostało poproszone przez GIODO o wyjaśnienie, czy ww. zbiorach zaprzestano przetwarzania danych, tj. m.in. utrwalania, zbierania i ich przechowywania, np. w celu archiwalnym. W odpowiedzi z 30 września 2013 r. Starosta wyjaśnił, że ww. zbiory są w rzeczywistości nadal przetwarzane w celach archiwalnych, a w związku z powyższym

[11] Przyjęta zarządzeniem wewnętrznym nr 21/2012 Starosty Hajnowskiego z 20 listopada 2012 r.
[12] Umowa Nr 109/GA/2013 z 1 stycznia 2013 r., obowiązująca od 1 stycznia 2013 do 31 grudnia 2015 r.
[13] Umowę zawarto 15 lutego 2013 r. na czas obowiązywania umowy nr 109/GA/2013.
[14] 15 lutego 2008 r. i 3 lutego 2012 r.
[15] Pisma nr: OA.142.1.2103, OA.142.2.2103, OA.142.3.2103, OA.142.4.2103 oraz OA.142.5.2103

wycofuje wnioski o ich wykreślenie. Decyzją nr DRZDO-DEC/172/15/14253 z 24 lutego 2015 r. GIODO umorzył postępowania o wykreślenie przedmiotowych zbiorów z rejestru.
(dowód: akta kontroli str. 121-131)

Obowiązki ASI[16] powierzono osobie zatrudnionej na stanowisku informatyka. Do jej obowiązków należało m.in. administrowanie systemami, w których gromadzono i przetwarzano dane. ASI posiadał upoważnienie do przetwarzania danych osobowych we wszystkich systemach wykorzystywanych w Starostwie.
(dowód: akta kontroli str. 132-134, 163-164, 169-170)

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. 99-101)

W okresie objętym kontrolą pracownicy Starostwa nie uczestniczyli w szkoleniach z zakresu bezpieczeństwa przetwarzania danych / informacji. Starosta wyjaśnił: „*W 2017 roku planujemy przeprowadzić szkolenia dla osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem bezpieczeństwa danych osobowych. Zakres i termin zostanie określony po szczegółowym rozeznaniu rynku oraz uzależniony od posiadanych środków finansowych*". 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. 99-101, 140-142,159-160)

Ustalone nieprawidłowości

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

1. W dniu 31 lipca 2016 r. rozwiązano umowę o pracę z osobą pełniącą obowiązki ABI, zaś zgłoszenie tego faktu do GIODO nastąpiło 20 września 2016 r., tj. 51 dni później. Było to niezgodne z art. 46b ustawy o ochronie danych osobowych, zgodnie z którym administrator danych jest zobowiązany zgłosić GIODO odwołanie ABI w terminie 30 dni od dnia jego odwołania. Starosta wyjaśnił, że: „*Niezgłoszenie tego faktu w terminie do GIODO spowodowane było przeoczeniem*". (dowód: akta kontroli str. 9-10, 135)

2. W Starostwie nie zrealizowano czterech z ośmiu przeglądów/kontroli dotyczących m.in. zgodności przetwarzania danych osobowych oraz ich zabezpieczeń z przepisami o ochronie danych osobowych w poszczególnych komórkach organizacyjnych, zaplanowanych na 2016 rok. Z jednego przeglądu nie sporządzono zaś sprawozdania (powinien je przygotować ABI pełniący swe obowiązki do końca lipca 2016 roku), czym naruszono § 6 ust. 1 rozporządzenia w sprawie sposobu realizacji zadań ABI, zgodnie z którym po zakończeniu sprawdzenia ABI przygotowuje przedmiotowe sprawozdanie. Z kolei pozostałych trzech sprawozdań, sporządzonych przez aktualnego ABI, nie przekazano Staroście, co było niezgodne z § 6 ust. 3 pkt. 1 ww. rozporządzenia. ABI wyjaśniła, że: „*Nie potrafię wytłumaczyć dlaczego osoba pełniąca przede mną tą funkcję nie realizowała sukcesywnie zadań wymienionych w planie sprawdzeń na 2016 rok i dlaczego nie sporządziła sprawozdania z jedynego działania jakie zrealizowała. Natomiast nieprzekazanie Staroście sprawozdań z trzech przeprowadzonych przez mnie sprawdzeń spowodowane było przeoczeniem oraz faktem, że nie stwierdziłam w ich trakcie żadnych uchybień*".
(dowód: akta kontroli str. 17-27, 34-35, 151)

3. W Starostwie nie prowadzono rejestru zbiorów danych przetwarzanych przez administratora, mimo takiego obowiązku wynikającego z art. 36 a ust. 2 pkt 2 ustawy o ochronie danych osobowych. ABI wyjaśniła, że: „*(...) z dniem 29 sierpnia 2016 r. Zarządzeniem Nr 24/2016 Starosta Hajnowski powołał mnie na Administratora Bezpieczeństwa Informacji (...). Powyższe zadanie zostało włączone do zakresu czynności, które wykonuję na stanowisku głównego specjalisty w Biurze Rady Powiatu. W związku z tym, że obowiązków Administratora (...) nie przejęłam bezpośrednio od osoby, która była w Starostwie powołana na to stanowisko (...), przeoczyłam*

[16] Powołany na to stanowisko zarządzeniem Starosty Hajnowskiego Nr 4/2015 z 4 lutego 2015 r.

obowiązek prowadzenia rejestru zbioru danych (...). Po zakończeniu kontroli, braki wynikające z niewypełniania obowiązku prowadzenia rejestru zbioru danych zostaną niezwłocznie uzupełnione". (dowód: akta kontroli str. 36-37, 52)

4. Wystawione przez Starostę dla dwóch pracowników upoważnienia do przetwarzania danych osobowych i prowadzenia zbiorów takich danych (z 20 objętych badaniem) nie były adekwatne do zakresu obowiązków tych pracowników, związanych z przetwarzaniem takich informacji. 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. ABI wyjaśniła, że: „*Przedmiotowe upoważnienia weryfikował poprzedni Administrator Bezpieczeństwa Informacji, a nadawał je administrator danych osobowych (Starosta). Nie potrafię wytłumaczyć dlaczego zakres wydanych upoważnień nie odpowiadał zakresom czynności tych pracowników.*"

   W trakcie kontroli (15 i 16 lutego 2017 r.) wydano upoważnienia do przetwarzania danych osobowych dostosowane do zadań przewidzianych w zakresach czynności obu pracowników . (dowód: akta kontroli str. 34-35, 41-51)

5. Z wykonawcą umowy w sprawie udostępnienia i serwisu systemów obsługujących rozrachunki oraz kadry i płace (obowiązującej do 31 grudnia 2018 r.) nie podpisano umowy powierzenia przetwarzania danych osobowych, mimo takiego wymogu określonego § 4 ust. 1 Instrukcji zarządzania, zgodnie z którym administrator danych udostępnia dane osobowe podmiotom zewnętrznym w oparciu o umowę poufności. Starosta wyjaśnił, że: „(...) *spowodowane to było przeoczeniem. Niezwłocznie podejmiemy działania w celu zawarcia takiej umowy*".
   (dowód: akta kontroli str. 57-66, 95-101,135)

6. Nie zgłoszono GIODO do zarejestrowania sześciu z 37 zbiorów danych prowadzonych w Starostwie, co naruszało wymogi art. 40 ustawy o ochronie danych osobowych. Dane osobowe w tych zbiorach były przetwarzane przed powołaniem ABI[17]. Starosta wyjaśnił, że: „*Spowodowane to było zaniedbaniem pracownika, który w tamtym okresie był odpowiedzialny za dokonywanie takich zgłoszeń. Osoba ta już nie pracuje w Starostwie*". (dowód: akta kontroli str. 102-103, 119-120,135)

7. W Starostwie nie przeprowadzano corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, wynikających 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: „*W związku z brakiem środków finansowych w budżecie powiatu nie przeprowadzano okresowych audytów wewnętrznych w zakresie bezpieczeństwa informacji*".
   (dowód: akta kontroli str. 99-101, 159-160)

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

Opis stanu faktycznego

Starostwo Zarządzeniem Nr 21/2012 Starosty Hajnowskiego z 20 listopada 2012 r. wprowadzono Instrukcję zarządzania systemem informatycznym ochrony danych osobowych oraz Politykę Bezpieczeństwa ochrony danych osobowych, którą zmieniono zarządzeniem Nr 13/2013 z 7 marca 2013 r[18]. (dowód: akta kontroli str. 57-86)

W Starostwie poza ww. dokumentami nie wydawano innych regulacji, procedur, instrukcji dotyczących gromadzenia i przetwarzania zasobów informatycznych oraz danych osobowych.

[17] Zgodnie z art. 43 ust. 1a ustawy o ochronie danych osobowych obowiązkowi rejestracji zbiorów danych nie podlega administrator danych, który powołał ABI i zgłosił go do rejestracji GIODO.

[18] Zarządzenie w sprawie zmiany zarządzenia Nr 21/2012 Starosty Hajnowskiego z 20 listopada 2012 r.

Wprowadzona Polityka bezpieczeństwa zawierała elementy określone w § 4 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych. Wykaz zbiorów danych osobowych (stanowiący załącznik Nr 2 do Polityki bezpieczeństwa) zawierał 26 z 37 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. W żadnym z ww. dokumentów nie określono poziomów bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 52, 57-86, 99-101, 115-118)

Starostwo nie opracowało i nie wdrożyło 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 aktualizowało 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. 52)

Spośród ośmiu systemów informatycznych przetwarzających dane osobowe[19], tylko jeden (Smart Doc) zapewniał 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 siedmiu pozostałych systemów, szerzej opisano poniżej, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 99-101,136-137)

Ustalone nieprawidłowości

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

1. Wykaz zbioru danych osobowych, będący załącznikiem Nr 2 do Polityki bezpieczeństwa, był nierzetelny. Zawierał bowiem jedynie 26 z 37 posiadanych przez Starostwo zbiorów danych. Starosta wyjaśnił, że: „*Polityka bezpieczeństwa w Starostwie Powiatowym w Hajnówce została wprowadzona Zarządzeniem nr 21/2012 Starosty Hajnowskiego z dnia 20 listopada 2012 r. (...) Wykaz zbioru danych zbioru danych osobowych w postaci dokumentacji papierowej i elektronicznej zawiera załącznik Nr 2 (...). Pracownik, który opracował powyższe zarządzenie odszedł na emeryturę. Nieujęcie wszystkich zbiorów danych w Polityce bezpieczeństwa wynikało najprawdopodobniej z nienależytego wykonania obowiązków służbowych przez tego pracownika. Aktualnie polityka bezpieczeństwa wraz z załącznikami jest aktualizowania*".
(dowód: akta kontroli str. 53-54, 67-86, 115-118)

2. Przyjęta w Starostwie Instrukcja zarządzania nie zawierała elementów wymaganych przepisem § 5 pkt. 5 i 7 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, tj.: sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także sposobu realizacji wymogów określonych w § 7 ust. 1 pkt 4 ww. rozporządzenia. W Starostwie, mimo wymogu wynikającego z § 6 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, nie określono poziomów bezpieczeństwa przetwarzania danych osobowych dla poszczególnych systemów informatycznych. Starosta wyjaśnił, że: „*Przeoczono zamieszczenie w instrukcji informacji o sposobie i okresie przechowywania elektronicznych nośników informacji oraz kopii zapasowych, a także odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostepnienia*". Przeoczeniem również tłumaczono brak zapisów określających poziomy bezpieczeństwa przy przetwarzaniu danych osobowych w systemach informatycznych.
(dowód: akta kontroli str. 52-66, 99-101)

[19] Kadry i Płace, Płatnik, Resto, EwOpis, Ośrodek, Smart Doc. Administratorem danych dla systemu CEPIK i RWD-2 były podmioty zewnętrzne. W Starostwie użytkowano również program EwMapa, w który gromadzono dane graficzne dotyczące nieruchomości bez danych osobowych.

3. W Starostwie nie opracowano i nie wdrożono polityki bezpieczeństwa informacji, o której mowa w § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI oraz nie aktualizowało regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia, mimo takiego wymogu wynikającego z § 20 ust. 2 pkt 1 ww. rozporządzenia. Starostwa wyjaśnił, że: „(...) *nie opracowano i nie wdrożono Polityki bezpieczeństwa informacji ze względu na zmiany organizacyjne w Starostwie i braki kadrowe. Obecnie trwają prace związane z opracowaniem Polityki Bezpieczeństwa Informacji. (...) Osoby, które były odpowiedzialne za aktualizację Polityki Bezpieczeństwa Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym Ochrony Danych Osobowych od ubiegłego roku nie pracują już w Starostwie (...). Nie potrafię odpowiedzieć dlaczego powyższe dokumenty nie były aktualizowane*". (dowód: akta kontroli str. 52-54, 159-160)

4. Siedem z ośmiu programów wykorzystywanych do przetwarzania danych osobowych, których administratorem był Starosta, nie spełniało wymogów określonych w § 7 ust. 3 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych. Nie umożliwiało bowiem dla każdej osoby, której dane przetwarzano, sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące m.in. daty pierwszego wprowadzenia danych osobowych oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu. ASI wyjaśnił, że: „*Do dnia rozpoczęcia kontroli nie miałem świadomości o istnieniu takiego obowiązku. Nikt z petentów wcześniej nie występował do pracowników Starostwa zajmujących się przetwarzaniem danych osobowych o sporządzenie takiego raportu. Pierwszy został wydrukowany dopiero w trakcie 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. 99-101, 136-139)

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 § 2 pkt 15 w związku § 20 ust. 1 rozporządzenia KRI, nie opracowano polityki bezpieczeństwa informacji oraz nie aktualizowano regulacji wewnętrznych. Nie określono też poziomów bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych oraz nie przeprowadzano corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji. Do GIODO nie zgłoszono zaś, w celu zarejestrowania, sześciu z 37 przetwarzanych zbiorów danych osobowych. Tylko jeden z ośmiu programów, w którym przetwarzano dane osobowe, stosownie do § 7 ust. 3 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, umożliwiał każdej osobie, której dane przetwarzano, sporządzenie i wydrukowanie raportu zawierającego informacje dotyczące m.in.: daty pierwszego wprowadzenia danych osobowych, identyfikatora użytkownika wprowadzającego dane osobowe do systemu. Osoby powołane na stanowisko ABI nie wywiązywały się zaś z obowiązków dotyczących przeprowadzania sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i opracowania sprawozdań w tym zakresie. Ponadto wbrew art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych, nie powadziły one rejestru zbiorów danych przetwarzanych w Starostwie.

2. Zakres przetwarzanych zasobów informatycznych

Opis stanu faktycznego

W Starostwie przetwarzano dane w 37 zbiorach danych, z których dziewięć prowadzono w wersji elektronicznej[20], a pozostałe w papierowej. Do GIODO zgłoszono 32 zbiory danych, z tego jeden dwukrotnie, co szerzej opisano w pkt 1 niniejszego wystąpienia.

Wg. stanu na 16 lutego 2017 r. w Starostwie nie prowadzono czterech zbiorów danych: dwóch „rejestrów legitymacji osób niepełnosprawnych", „rejestru poborowych" oraz „ewidencji osób korzystających z środków PFRON". ABI wyjasnił, że: „*Oba rejestry legitymacji osób niepełnosprawnych oraz wykaz osób korzystających ze środków PFRON*

[20] Do tego celu wykorzystywano dziewięć programów informatycznych: Ewopis, EwMapa, Ośrodek, Cepik, Resto, Smart Doc, Kadry i Płace, Płatnik oraz RWD-2.

przekazano w 2013 roku wraz z archiwum do PCPR w Hajnówce, niestety bez żadnego oficjalnego poświadczenia. Natomiast w Starostwie nie prowadzono rejestru poborowych. Nie potrafię wyjaśnić dlaczego zgłoszono ten zbiór do GIODO i potem nie był on prowadzony. Osoby, które były odpowiedzialne za te zdarzenia nie pracują już w Starostwie".

Spośród pozostałych 28 zbiorów danych zgłoszonych do GIODO, zakres przetwarzanych danych w 25 był zgodny ze zgłoszeniem do GIODO. W kolejnych trzech gromadzono zaś informacje nie objęte zgłoszeniem, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". W okresie objętym kontrolą, nie aktualizowano zakresu danych gromadzonych w zbiorach zgłoszonych do GIODO.

Analiza 21 zbiorów danych prowadzonych w poszczególnych komórkach organizacyjnych Starostwa wykazała, że w 18 przypadkach zakres przetwarzanych danych był niezbędny do realizacji zadań przypisanych tym komórkom. W trzech kolejnych zbiorach gromadzono dane, które nie były wykorzystywane przy realizacji wykonywanych 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 i RWD-2[21], administratorem danych, w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych, był Starosta. Starostwo uzyskało dostęp do zbioru danych CEPIK na podstawie umowy DMD/003/99 z 1 lipca 1999 r.[22], zawartej z Polską Wytwórnia 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. Natomiast certyfikaty, loginy i hasła dostępu do systemu RWD-2 dla pracowników Starostwa nadawał podmiot zewnętrzny.

(dowód: akta kontroli str. 34-35, 102-118, 140-146, 157-158, 162)

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 do GIODO rozszerzenia zakresu przetwarzanych danych w trzech niżej wymienionych zbiorach danych osobowych oraz przekazania kolejnych trzech innej jednostce. Starosta wyjaśnił: „*Spowodowane to było niedopełnieniem swoich obowiązków przez odpowiedzialnych pracowników Starostwa. Niezwłocznie zostanie to uzupełnione* ". (dowód: akta kontroli str. 135,151)

2. W trzech zbiorach przetwarzających dane osobowe w jednostce gromadzono dane osobowe, które nie były wykorzystywane przy realizacji zadań.

   W Wydziale Geodezji Katastru i Nieruchomości w formie papierowej prowadzono zbiór danych dotyczący „nadawania na własność działek"[23]. Analiza 10 (z 27 spraw) wykazała, że we wszystkich aktach poszczególnych spraw, oprócz danych zgłoszonych do GIODO, dodatkowo przetwarzano: Nr Pesel, datę urodzenia i miejsce urodzenia oraz serię i nr dowodu osobistego. Ponadto w trzech przypadkach stwierdzono kopie dowodów osobistych. Jak wyjaśniła p.o. naczelnika Wydziału Geodezji Katastru i Nieruchomości: „*W celu prawidłowego prowadzenia postępowań związanych z nadawaniem na własność działek wystarczające są dane wskazane w zgłoszeniu do GIODO, tj., imię i nazwisko, imiona rodziców oraz adres zamieszkania. Całkowicie zbędne są pozostałe dane (Pesel, data urodzenia i miejsce urodzenia oraz nr dowodu osobistego)*".

---

[21] Centralna Ewidencja Pojazdów i Kierowców, Rejestr wniosków i decyzji o pozwoleniu na budowę i rejestr zgłoszeń budowy.

[22] Zmienionej na umowę Nr 65/167 z 14 maja 2009 r.

[23] Zbiór danych dotyczących postępowań w sprawie zwrotu działek w oparciu o art. 6 ustawy z 24 lutego 1989 r. o zmianie ustawy o ubezpieczeniu społecznym rolników indywidualnych i członków ich rodzin oraz o zmianie ustawy o podatku rolnych (Dz. U. Nr 10 poz. 53, ze zm.) oraz art. 118 ustawy z dnia 20 grudnia 1990 r. o ubezpieczeniu społecznym rolników (Dz. U. 2016 poz. 277 ze zm.).

Z kolei w Wydziale Środowiska i Spraw Społecznych w formie elektronicznej prowadzono dwa rejestry: stowarzyszeń i klubów sportowych. Analiza akt 10 (z 68) zarejestrowanych stowarzyszeń wykazała, że w ośmiu przypadkach rejestr zawierał oprócz imion i nazwisk członków zarządu i organu kontroli wewnętrznej, także daty urodzenia tych osób i ich nr Pesel, w następnym imiona i nazwiska oraz daty urodzenia osób wchodzących w skład zarządu i organu kontrolnego, a w ostatnim imiona i nazwiska osób wchodzących w skład zarządu oraz organu kontrolnego. Zgodnie z art. 40b ust. 1 ustawy z dnia 7 kwietnia 1989 r. Prawo o stowarzyszeniach[24], 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 spraw 10 (z 33 wpisanych 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[25] nie przewidują gromadzenia przez organ prowadzący rejestr danych dotyczących nr Pesel.

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. Pełniąca obowiązki naczelnika Wydziału Geodezji Katastru i Nieruchomości 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 Środowiska i Spraw Społecznych wyjaśniła: *„Nie mieliśmy świadomości, że nie możemy przetwarzać danych innych niż niezbędne do realizacji przypisanych nam zadań. Klienci składający dokumenty do wydziału dołączali do nich także dane niewymagane przepisami prawa (data urodzenia czy nr Pesel), a my nieświadomie je przetwarzaliśmy."* (dowód: akta kontroli str. 115-118, 140-142, 149-150)

Ocena cząstkowa

Starostwo przetwarzając dane osobowe wykroczyło poza uprawnienia wynikające z przepisów oraz realizowanych zadań. Nie wywiązało się bowiem z obowiązku poinformowania GIODO o zaprzestaniu przetwarzania danych w trzech zbiorach danych osobowych (które przekazano innej jednostce). W kolejnych trzech z 21 analizowanych zbiorów zakres gromadzonych informacji wykraczał poza dane niezbędne do realizacji zadań, w związku z którymi Starostwo je prowadziło, a dodatkowo rozszerzony zakres nie był określony w zgłoszeniu skierowanym do GIODO. Spełniono zaś wymogi dotyczące dostępu do zbioru danych osobowych, których administratorem był podmiot zewnętrzny.

3. Sposób przechowywania oraz fizycznego zabezpieczania danych

Opis stanu faktycznego

W Starostwie dziewięć z 37 zbiorów danych osobowych prowadzono z wykorzystaniem systemów elektronicznych, a pozostałe papierowo. W załączniku Nr 2 do Polityki bezpieczeństwa ochrony danych osobowych określono zabezpieczenia fizyczne pomieszczeń, w których był dostęp do 26 zbiorów danych osobowych. Ich oględziny wykazały, że w 25 przypadkach przyjęte zabezpieczenia odpowiadały wymaganiom określonym w ww. załączniku. W jednym natomiast, dotyczącym zbioru „Dziennik korespondencji", nie było wymaganego zabezpieczenia zasilania (w postaci USP) komputera, w którym znajdował się ten zbiór. ASI wyjaśnił, że: *„Z powodu awarii urządzenia w połowie 2016 roku odłączono je od komputera obsługującego dziennik korespondencji. Zgłosiłem stosowne zapotrzebowanie Staroście, jednak z powodu braku środków nie przeprowadzaliśmy zakupu tego typu urządzeń"*.

Nie opracowano natomiast form ochrony fizycznej 11 zbiorów danych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 68-86, 116-118, 138-139, 151, 157-158)

[24] Dz. U. 2015 poz. 1393.
[25] Dz. U. Nr 243 poz.1449.

ASI nie gromadził informacji dotyczących bieżącej inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 99-101, 147)

W 2016 roku nie przeprowadzano likwidacji sprzętu będącego nośnikiem danych (komputerów, dysków), ani nie zlecano podmiotom zewnętrznym napraw takiego sprzętu. ASI wyjaśnił: „(...) *wszystkich napraw dokonywałem samodzielnie. W 2016 roku nie przydarzyła się awaria sprzętu informatycznego wymagająca poważnych ingerencji w sprzęt. Były to raczej drobne naprawy*". (dowód: akta kontroli str. 99-101,138-139)

Starostwo dysponowało 11 niszczarkami do dokumentów: trzema w Wydziale Geodezji, Katastru i Nieruchomości oraz po jednej w pozostałych siedmiu wydziałach i sekretariacie. W § 8 ust. 6 pkt 4 Polityki bezpieczeństwa zobowiązano pracowników do niszczenia dokumentów i tymczasowych wydruków w niszczarkach, niezwłocznie po ustaniu celu ich przetwarzania. (dowód: akta kontroli str. 67-86, 99-101)

W § 11 ust. 2 Instrukcji zarzadzania sformułowano zakaz wynoszenia poza siedzibę Starostwa nośników informacji zawierających dane osobowe. Nie określono zasad użytkowania sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych oraz możliwości korzystania ze służbowych urządzeń informatycznych poza siedzibą jednostki. W Starostwie nie opracowano również zasad bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość. ASI wyjaśnił, że: „*Pracownicy Starostwa nie mogą użytkować prywatnego sprzętu do celów służbowych. Wprawdzie w żadnym dokumencie wewnętrznych nie wymieniono takiego zakazu, ale kierownictwo Starostwa wyraźnie zabroniło wykorzystywania sprzętu prywatnego do celów służbowych. Ponadto taki sprzęt należałoby wpierw skonfigurować z systemem. Taka sytuacja nigdy do tej pory nie wystąpiła. Pracownicy nie mają też możliwości korzystania z systemów informatycznych Starostwa poza jego siedzibą*".
(dowód: akta kontroli str. 57-66, 99-101, 138-139)

Sprzątanie pomieszczeń Starostwa powierzono podmiotowi zewnętrznemu. ABI wyjaśniła: „*Panie sprzątające rozpoczynają pracę codziennie o godz. 14 i do godz. 15[30] (tj. do zakończenia pracy Starostwa) muszą posprzątać pomieszczenia Wydziału Geodezji Katastru i Nieruchomości oraz Wydziału Komunikacji i Dróg (pomieszczenia tych wydziałów zabezpieczone są alarmem). Osoby sprzątające kończą pracę około godz. 17*".

W § 8 ust. 6 pkt 2 Polityki bezpieczeństwa zobowiązano pracowników do zabezpieczania dokumentów (zamykania na klucz w szafach i biurkach) przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy. Zgodnie z wymogami określonymi pkt. I załącznika do rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, osobom sprzątającym administrator danych wystawił upoważnienia do przebywania w obszarze przetwarzania danych.
(dowód: akta kontroli str. 34-35, 67-98, 152-156)

W § 14 ust. 1 pkt 2 i 3 Instrukcji zarządzania systemem informatycznym informatyka zobowiązano do wykonywania nie rzadziej niż raz w roku przeglądów i konserwacji systemu informatycznego. W okresie objętym kontrolą takie przeglądy i konserwacje nie były przeprowadzane, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 57-66, 151)

Stosownie do wymogów określonych w pkt. IV załącznika do rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, w Starostwie zabezpieczało przetwarzanie danych poprzez sporządzanie kopii zapasowych. Sporządzano je dla siedmiu z dziewięciu systemów wykorzystywanych do przetwarzania danych. Pełne kopie bezpieczeństwa programów EwOpis, EwMapa i Ośrodek wykonywano raz dziennie o godz. 17 i zapisywano na dysku zewnętrznym (USB), a po jego zapełnieniu przechowywano w serwerowni. Kopie bezpieczeństwa programów Kadry i Płace, Płatnik tworzono raz w tygodniu (w piątek) na dysku zewnętrznym, który przechowywano w pokoju informatyka, w zamykanej szafie. Dysponowano także wersjami instalacyjnymi programów służących do przetwarzania

danych osobowych. ASI wyjaśnił, że dane dotyczące systemów RWD-2 i CEPIK były zapisywane odpowiednio na serwerach Głównego Urzędu Nadzoru Budowlanego oraz Polskiej Wytwórni Papierów Wartościowych S .A., gdzie tworzono kopie zapasowe. W okresie objętym kontrolą nie wykonywano kopii bezpieczeństwa danych gromadzonych z wykorzystaniem systemu Smart Doc oraz zbiorów danych gromadzonych przy wykorzystaniu programu Resto, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 99-101, 138-139)

W Starostwie nie opracowano procedur na wypadek wystąpienia długotrwałego braku zasilania w energię elektryczną oraz niszczenia zbędnych kopii zapasowych. Dysponowano agregatem prądotwórczym z autostartem o mocy 88 kW, zaś dobowe zapotrzebowanie na energię wynosiło 31 kW (średnia z ostatnich trzech miesięcy 2016 roku).

(dowód: akta kontroli str. 99-101)

W okresie objętym kontrolą nie przeprowadzono testowania wykonanych kopii zapasowych oraz nie wystąpiły przypadki fizycznej utraty danych. (dowód: akta kontroli str. 99-101)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki stwierdzono następujące nieprawidłowości:

1. W załączniku Nr 2 do Polityki bezpieczeństwa ochrony danych osobowych nie określono form ochrony fizycznej 11 (z 37) funkcjonujących w jednostce zbiorów danych osobowych, mimo takiego wymogu wynikającego z § 8 ust. 3 Polityki bezpieczeństwa. ABI wyjaśnił, że: *„Była to konsekwencją nieujęcia w zał. Nr 2 do Polityki bezpieczeństwa ochrony danych osobowych wszystkich działających w Starostwie zbiorów danych osobowych"*. (dowód: akta kontroli str. 34-35, 67-86, 115-118, 151)
2. W Starostwie na bieżąco nie gromadzono danych wskazujących na utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację mimo takiego obowiązku wynikającego z § 20 ust. 2 pkt 2 rozporządzenia KRI. ASI wyjaśnił, że: *„Nigdy nie gromadziłem dokumentów pozwalających na utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Wynikało z braku czasu i dużej ilości innych obowiązków"*.

(dowód: akta kontroli str. 99-101, 138-139,147)
3. W 2016 roku w Starostwie nie przeprowadzono przeglądów i konserwacji systemów informatycznych, co było niezgodne z § 14 ust. 1 pkt 2 Instrukcji zarządzania. ASI wyjaśnił, że: *„Nie dokonywano rocznych przeglądów użytkowanych w Starostwie systemów informatycznych* z powodu *przeoczenia i dużej ilości innych obowiązków. Wszelkie usterki były usuwane na bieżąco. W 2016 roku nie było awarii żadnego z użytkowanych systemów/programów"*. (dowód: akta kontroli str. 57-66, 138-139,151)
4. W Starostwie nie wykonywano kopii bezpieczeństwa danych gromadzonych w dwóch (z dziewięciu) systemach, tj. w programie Smart Doc i Resto, mimo, że zgodnie z wymogami określonymi w pkt IV załącznika do rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, dane osobowe przetwarzane w systemach informatycznych powinny być zabezpieczone poprzez wykonywanie kopii zapasowych zbiorów danych. ASI wyjaśnił, że: *„Niesporządzanie kopii bezpieczeństwa zbioru danych gromadzonych z wykorzystywaniem programów Resto oraz Smart Doc wynikało z mojego niedopatrzenia oraz dużej liczby inny obowiązków"*.

(dowód: akta kontroli str. 99-101, 138-139)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że nieprzeprowadzanie testowania kopii zapasowych może narazić Starostwo na utratę danych w przypadku uszkodzenia wykonanych kopii. ASI wyjaśnił, że: *„Wynikało to z mojego przeoczenia. Opracuję stosowną procedurę / instrukcję i będę przeprowadzał testy sporządzanych kopii zapasowych wykonanych programów"*. (dowód: akta kontroli str. 99-101, 138-139)

Ocena cząstkowa

W Polityce bezpieczeństwa określono sposób niszczenia dokumentów i tymczasowych wydruków oraz zobowiązano pracowników do zabezpieczania dokumentów przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy. W Instrukcji zarządzania sformułowano zakaz wynoszenia poza

budynek Starostwa nośników informacji zawierających dane osobowe. Przyjęte rozwiązania dotyczące przechowywania i fizycznego zabezpieczenia danych nie w pełni jednak odpowiadały przepisom regulującym ochronę danych osobowych. Nie opracowano bowiem form ochrony fizycznej 11 z 37 zbiorów danych osobowych. Nie dysponowano również dokumentami wskazującymi na bieżące utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, nie wykonywano kopii bezpieczeństwa danych gromadzonych dla dwóch systemów oraz nie przeprowadzano testów wykonanych kopii zapasowych. Nie wywiązano się też z obowiązku przeprowadzania przeglądów i konserwacji systemu informatycznego.

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

Opis stanu faktycznego

W Starostwie nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Zagadnienie dotyczące przestrzegania zasad korzystania z systemów, których administratorem danych nie był Starosta opisano w pkt 2 niniejszego wystąpienia.

Analiza uprawnień 20 (z 61) pracowników merytorycznych Starostwa, którym nadano upoważnienia do przetwarzania danych osobowych w systemach informatycznych wykazała, że wszyscy posiadali nadany login i hasło, umożliwiające prace w tych systemach. Zakres nadanych im upoważnień w odniesieniu do ich zakresów czynności opisano w pkt. 1 niniejszego wystąpienia.

Osobom, które zaprzestały świadczenia pracy w 2016 roku upoważnienia do przetwarzania danych osobowych odebrano w dniu lub dzień po rozwiązaniu umowy o pracę[26].

(dowód: akta kontroli str. 41-43, 151, 161)

Dostęp do sieci wewnętrznej Starostwa był obsługiwany poprzez router CISCO. Dane dotyczące osób i dat logowania do sieci wewnętrznej Starostwa zapisywano w rejestrze systemowym routera (w formie logów systemowych, z których można było odczytać godziny logowania i wylogowania poszczególnych użytkowników z sieci oraz informację z jakich zasobów korzystali). ASI wyjaśnił, że raz na kwartał dokonywano analizy zapisów informacji zawartych w logach, w celu m.in. weryfikacji godzin logowania użytkowników, w wyniku których nie stwierdzono niczego niebezpiecznego. Dotyczyło to logowań do sieci wewnętrznej oraz korzystania z systemów / programów takich jak: Ewopis, EwMapa, Ośrodek, Resto, RWD-2 oraz SmartDoc, Płatnik oraz Kadry i Płace. Przedmiotowej analizy nie dokonywano dla systemu CEPIK, ponieważ jego administratorem był podmiot zewnętrzny, który nie wykorzystywał łączy Starostwa. Przeprowadzane analizy zapisów informacji zawartych w logach oraz ich wyniki nie były dokumentowane. Zapisane logi systemowe przechowywano przez trzy miesiące na routerze CISCO.

(dowód: akta kontroli str. 99-101, 138-139)

Zgodnie z wymogami określonymi w § 2 ust. 3 Instrukcji zarządzania systemem informatycznym, dostęp do systemu operacyjnego komputerów z wykorzystaniem, których przetwarzano dane osobowe powinien być zabezpieczony za pomocą loginu i hasła oraz mechanizmu wymuszającego okresową zmianę haseł. Analiza dotycząca 20 (z 61) pracowników merytorycznych jednostki, którym nadano uprawnienia do przetwarzania danych osobowych w systemach informatycznych wykazała, że wszyscy posiadali własny login i hasła (hasła w celu zalogowania się do systemu informatycznego Starostwa i umożliwiające korzystanie z poszczególnych baz danych prowadzonych w wersji elektronicznej były inne). Oględziny 10 stanowisk komputerowych (trzech w Wydziale Geodezji, Katastru i Nieruchomości, po dwa w Wydziałach: Architektury i Budownictwa, Spraw Społecznych i Ochrony Środowiska, Organizacyjno-Administracyjnym oraz informatyka), z wykorzystaniem których przetwarzano m.in. dane osobowe wykazały, że konfiguracja zabezpieczeń dostępu do systemu operacyjnego komputerów nie wymuszała okresowej zmiany hasła użytkowników (zmiana hasła mogła nastąpić

[26] W 2016 roku z sześcioma osobami rozwiązano umowy o pracę.

jedynie z inicjatywy danego użytkownika). Niezapewnienie tej funkcjonalności szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 41-43, 57-66, 147)

Zgodnie z § 3 ust. 1 Instrukcji zarządzania, dostęp do poszczególnych programów przetwarzających dane osobowe wymagał użycia loginu i hasła[27]. Natomiast stosownie do zapisów § 3 ust. 2 i 7 Instrukcji dla programów przetwarzających dane osobowe należało zastosować mechanizm wymuszający okresową zmianę haseł oraz automatyczną blokadę dostępu do tych programów w przypadku dłuższej nieaktywności pracy użytkownika. W Starostwie dostęp do programów, w których przetwarzano dane osobowe zabezpieczony był loginem i hasłem. Spośród ośmiu programów przetwarzających dane osobowe, tylko pięć (Smart DOC, RWD-2, Płatnik, CEPIK oraz Kadry i Płace) wymuszało okresową zmianę haseł, a jedynie w trzech (CEPIK, Smart DOC i RWD-2) zastosowano mechanizm automatycznej blokady dostępu do programu w przypadku dłuższej nieaktywności użytkownika, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 57-66, 147)

Starostwo posiadało sieć Wi-Fi, zabezpieczoną ośmioznakowym hasłem. Nie była ona udostępnia pracownikom Starostwa, a jedynie wykorzystywana przez ASI przy dokonywaniu napraw i prac serwisowych sprzętu komputerowego zainstalowanego w jednostce. W Starostwie nie opracowano procedur / uregulowań dotyczących zasad dostępu do sieci Wi-Fi. (dowód: akta kontroli str. 99-101)

W 2016 roku nie stwierdzono przypadków wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji. Nie wystąpiła również konieczność odtwarzania zbioru danych ze sporządzonych kopii bezpieczeństwa. W celu ochrony systemów zastosowano zabezpieczenia w postaci firewalla, zainstalowanego na głównym łączu internetowym Starostwa oraz programu antywirusowego na każdym komputerze. Oprogramowania aktualizowały się automatycznie przy każdym uruchomieniu komputerów.
(dowód: akta kontroli str. 99-101)

W 2004 roku Starostwo wykupiło usługę hostingu strony internetowej, domenę internetową oraz pocztę elektroniczna w podmiocie zewnętrznym (home.pl). Dane przechowywano na serwerach wykonawcy usługi, który był również administratorem danych. Zgodnie z pkt. 7 regulaminu sieci hom.pl, podmiot realizujący usługę przetwarza dane zgodnie z zasadami wskazanymi w ustawie o ochronie danych osobowych oraz w ustawie o świadczeniu usług drogą elektroniczną i zapewnia bezpieczeństwo zgromadzonych danych. (dowód: akta kontroli str. 151)

W Starostwie użytkowano 51 komputerów, w tym m.in.: [1] 28 pozyskanych w 2014 roku w ramach projektu „Wdrażanie elektronicznych usług dla ludności województwa podlaskiego – cześć II, administracja samorządowa" za kwotę 124,3 tys. zł; [2] jeden pozyskany w 2012 roku, za 4,3 tys. zł, w wyniku realizacji projektu „Modernizacja infrastruktury dydaktycznej dla współpracy polsko białoruskiej na rzecz osób niepełnosprawnych"; [3] trzy stacjonarne zestawy zakupione w 2013 roku za 12,7 tys. zł w ramach projektu „Platforma współpracy na rzecz zrównoważonego rozwoju Puszczy Białowieskiej"; [4] siedem zakupionych ze środków własnych w latach 2012 – 2016 za 17,2 tys. zł.

Oględziny 10 (z 39 ww. komputerów) wykazały, że wszystkie miały zainstalowany system operacyjny Windows 7 i nie stwierdzono instalacji programów, na które Starostwo nie posiadało licencji.

Ponadto dysponowano sześcioma komputerami zakupionymi w 2005 roku, na których zainstalowano oprogramowanie Windows XP, z czego cztery użytkowano w Wydziale Geodezji, Katastru i Nieruchomości (trzy wykorzystywano do bieżącej pracy, m.in. logowania się do systemu EwOpis, zaś jeden wyłącznie do skanowania dokumentów), a z pozostałych korzystał radca prawny oraz Wydział Promocji Starostwa. Z wykorzystaniem tych komputerów nie prowadzono rejestrów i nie przechowywano w nich zbiorów danych. ASI wyjaśnił: *„Użytkujemy je jedynie z powodu braków środków finansowych na zakup nowego sprzętu informatycznego. Sukcesywnie wymieniamy stare komputery na nowe*

[27] Hasła składały się co najmniej z ośmiu znaków.

z systemami operacyjnymi, które mają takie wsparcie". Natomiast w Wydziale Komunikacji i Dróg użytkowano sześć komputerów podłączonych do systemu CEPIK, właścicielem których była Państwowa Wytwórnia Papierów Wartościowych S.A. – urządzenia te nie posiadały dostępu do Internetu. (dowód: akta kontroli str. 99-101, 138-139, 147)

W Starostwie nie opracowano procedur związanych z płatnościami realizowanymi drogą elektroniczną. Dokonywano ich za pośrednictwem systemu bankowego, dostępnego na stronie internetowej. Po sprawdzeniu dokumentu pod względem merytorycznym i formalno-rachunkowym oraz zatwierdzeniu go do wypłaty/przelewu, wyznaczony pracownik sporządzał przelew, który następnie był zatwierdzany przez dwie z czterech uprawnionych osób. Przelewy autoryzowano / podpisywano za pośrednictwem bankowego podpisu elektronicznego w systemie banku. (dowód: akta kontroli str. 99-101)

W 2016 roku wydatki Starostwa na zakup programów związanych z zapewnieniem bezpieczeństwa przetwarzania danych wniosły 3,9 tys. zł[28].
(dowód: akta kontroli str. 165-168)

Ustalone nieprawidłowości

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

1. 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: „*Spowodowane to było przeoczeniem. Będziemy przeprowadzać rokrocznie przedmiotowe analizy*".
(dowód: akta kontroli str. 135,151)

2. W systemach operacyjnych 10 stanowisk komputerowych objętych analizą, nie wprowadzono rozwiązań wymuszających na użytkownikach okresową zmianę haseł, mimo takiego obowiązku określonego w § 2 ust. 3 pkt. 3 Instrukcji zarządzania. ASI wyjaśnił: „*Wynikało to jedynie z mojego przeoczenia. Po zakończeniu kontroli dokonam przeglądu wszystkich komputerów użytkowanych w Starostwie pod katem weryfikacji tych ustawień. Podkreślam, że na tych komputerach zainstalowano oprogramowanie antywirusowe chroniące przed różnymi zagrożeniami związanymi z ich użytkowaniem*".
(dowód: akta kontroli str. 57-66, 138-139, 147-148)

3. Spośród ośmiu programów, z wykorzystaniem których przetwarzano dane osobowe w wersji elektronicznej, trzy (EwOpis, Ośrodek i Resto) nie wymuszały okresowej zmiany haseł, zaś w pięciu (EwOpis, Ośrodek, Płatnik, Kadry i Place oraz Resto) nie zastosowano mechanizmu automatycznej blokady dostępu do systemu w przypadku dłuższej nieaktywności użytkownika. Było to niezgodne z § 3 ust. 2 i 7 Instrukcji zarządzania. ASI wyjaśnił: „*Niezastosowanie tych mechanizmów w programach wynikało z braku czasu oraz dużej ilości innych zajęć. Podkreślam, że jestem jedynym informatykiem zatrudnionym w Starostwie*".
(dowód: akta kontroli str. 57-66, 147, 138-139)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że z dniem 8 kwietnia 2014 r. producent oprogramowania zakończył udzielanie wsparcia dla posiadanego systemu operacyjnego, w konsekwencji czego sześć komputerów, w których zainstalowano to oprogramowanie może nie dość skutecznie chronić dane przetwarzane z ich wykorzystaniem.

Ocena cząstkowa

Starostwo, w celu ochrony systemów przed nieuprawnionym dostępem, zastosowało zabezpieczenia w postaci firewalla zainstalowanego na głównym łączu internetowym oraz programu antywirusowego zainstalowanego na każdym komputerze. 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. Konfiguracja zabezpieczeń dostępu do systemu operacyjnego 10 komputerów objętych analizą oraz trzech (z ośmiu programów, w których przetwarzano dane osobowe) nie wymuszała bowiem okresowej zmiany hasła użytkowników, a jedynie w kolejnych trzech zastosowano

[28] Faktura VAT Nr 1131/07/2016 z 7 lipca 2016 r. na zakup programu antywirusowego.

mechanizm automatycznej blokady dostępu do programu w przypadku dłuższej nieaktywności użytkownika. Nie wywiązano się z obowiązku przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Ponadto w Starostwie użytkowano komputery z zainstalowanym systemem operacyjnym, którego producent zakończył udzielanie wsparcia, co w znaczący sposób wpłynęło na obniżenie skuteczności ochrony danych przetwarzanych przy jego wykorzystaniu.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi 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[29] wnosi o:

1. Terminowe zgłaszanie do GIODO zmian na stanowisku ABI oraz zmian zakresu danych gromadzonych w zarejestrowanych zbiorach danych osobowych przetwarzanych w Starostwie.
2. Prowadzenie przez ABI rejestru zbiorów danych, stosownie do wymogów wynikających z art. 36 a ust. 2 pkt 2 ustawy o ochronie danych osobowych.
3. Dostosowanie zapisów Instrukcji zarządzania systemem informatycznym do wymogów § 5 pkt. 5 i 7 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz stosowanie regulacji dotyczących: udostępniania danych osobowych podmiotom zewnętrznym, przeprowadzania przeglądów i konserwacji systemu informatycznego i okresowej zmiany haseł.
4. 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.
5. Ujęcie wszystkich zbiorów wykorzystywanych w Starostwie w wykazie zbiorów danych osobowych, stanowiącym element Polityki bezpieczeństwa.
6. Określenie poziomów bezpieczeństwa, o których mowa w § 6 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, dla przetwarzania danych osobowych w poszczególnych systemach informatycznych.
7. Dostosowanie wszystkich programów wykorzystywanych w Starostwie do przetwarzania danych osobowych do wymogów określonych w § 7 ust. 3 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych.
8. Przetwarzanie w zbiorach wyłącznie danych niezbędnych do realizacji obowiązków wynikającego z przepisów prawa.
9. Opracowanie regulacji dotyczących fizycznej ochrony danych osobowych wszystkich zbiorów przetwarzanych w jednostce.
10. Bieżące gromadzenie danych pozwalających na utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji.
11. Wykonywanie kopii bezpieczeństwa danych przetwarzanych z wykorzystaniem programów Smart Doc oraz Resto.

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

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 17 marzec 2017 r.

Kontroler
Piotr Jurkin
starszy inspektor kontroli państwowej

podpis

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

podpis