NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.04.2017
P/17/062

02253517

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	P/17/062 – Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontrolerzy	Adrian Gosk – specjalista k. p., upoważnienie do kontroli nr LBI/154/2017 z 6 listopada 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Starostwo Powiatowe w Zambrowie, ul. Fabryczna 3, 18-300 Zambrów[1]
Kierownik jednostki kontrolowanej	Robert Maciej Rosiak – Starosta Zambrowski[2] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[3]

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości zapewnienie przez Starostwo właściwej ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem[4].

Uzasadnienie oceny ogólnej

Pozytywna ocena wynika w szczególności z: opracowania wymaganej dokumentacji bezpieczeństwa oraz procedur ochrony danych[5], które odpowiadały wymogom zawartym w § 4 – 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[6], zapewnienia ochrony pomieszczeń, sprzętu oraz przetwarzanych danych zgodnej z ww. regulacjami, a także gromadzenia wyłącznie danych osobowych niezbędnych z punktu widzenia zadań Starostwa.

Stwierdzono jednak nieprawidłowości polegające na:

- niewydaniu upoważnień dostępu do systemów informatycznych i upoważnień do przetwarzania danych osobowych trzem pracownikom (z 30 analizowanych) oraz niepoinformowaniu administratora systemu zewnętrznego o utracie uprawnień do przetwarzania danych osobowych w tym systemie przez dwóch byłych pracowników, co było niezgodne z pkt 4 – 5 załącznika nr 4 do PBI oraz art. 36, art. 37 i art. 39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[7],
- niemonitorowaniu dostępu do informacji, a także nieprzeprowadzaniu corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, mimo wymogów zawartych w § 20 ust. 2 pkt 7 lit a i pkt 14 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[8],

---

1 Dalej: „Starostwo".
2 Robert Maciej Rosiak jest Starostą Zambrowskim od 29 grudnia 2014 r.
3 Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
4 Okres objęty kontrolą to od 1 stycznia 2016 r. do dnia zakończenia czynności kontrolnych.
5 Zarządzeniem Nr 120.20.2014 z dnia 30 września 2014 r. Starosta Zambrowski wprowadził do użytku służbowego: [1] Politykę Bezpieczeństwa Informacji (zwaną dalej „PBI"), [2] Politykę bezpieczeństwa danych osobowych oraz [3] Instrukcję zarządzania systemem informatycznym (zwaną dalej „Instrukcją zarządzania").
6 Dz. U. Nr 100 poz. 1024. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie dokumentacji przetwarzania danych osobowych".
7 Dz. U. 2016 poz. 922.
8 Dz. U. 2017 r. poz. 2247. Rozporządzenie zwane dalej: „rozporządzeniem KRI".

- nieuregulowaniu odpowiedniego poziomu bezpieczeństwa serwera poczty, wbrew obowiązkowi wynikającemu z § 20 ust. 2 pkt 10 rozporządzenia KRI,
- niezarejestrowaniu u Generalnego Inspektora Ochrony Danych Osobowych (dalej: „GIODO") sześciu (z 22) zbiorów danych osobowych prowadzonych z wykorzystaniem systemów informatycznych, a także niezgłoszeniu GIODO rozszerzenia w latach 2016 – 2017 zakresu przetwarzanych danych w 12 zbiorach danych, co naruszało art. 40 i art. 41 ust. 2 ustawy o ochronie danych osobowych,
- niezapewnieniu pracownikom zaangażowanym w proces przetwarzania informacji szkoleń, o których mowa w § 20 ust. 2 pkt 6 rozporządzenia KRI,
- nieprzeprowadzaniu kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, mimo takiego obowiązku ustalonego w art. 36a ust. 2 w związku z art. 36b ustawy o ochronie danych osobowych,
- niezaktualizowaniu polityki bezpieczeństwa przetwarzania danych osobowych, przewidzianej § 20 ust. 2 pkt 1 rozporządzenia KRI.

III. Opis ustalonego stanu faktycznego

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

Opis stanu faktycznego

1.1. W okresie objętym kontrolą do gromadzenia i przetwarzania danych wykorzystywano 20 systemów informatycznych (w 14 z nich przetwarzano dane osobowe), które funkcjonowały na 42 stacjach roboczych (36 komputerów stacjonarnych oraz sześć laptopów[9]). Spośród tych urządzeń, sześć nie posiadało dostępu do Internetu, a na pozostałych stworzono taką możliwość, przy czym sieć lokalna oparta była na architekturze klient – serwer, tak więc praca na oprogramowaniu służbowym (w tym na komputerach przenośnych) odbywać się mogła wyłącznie w sieci lokalnej. Oględziny 30 (z 42) stacji roboczych wykazały stosowanie właściwych zabezpieczeń. Między innymi [1] dostęp do systemu zabezpieczony został odpowiednimi narzędziami informatycznymi (w 28 przypadkach loginem i odpowiedniej jakości hasłem, a w dwóch logowanie następowało z wykorzystaniem indywidualnej karty z certyfikatem, po podaniu PIN-u); [2] użytkownicy posiadali dostęp wyłącznie do oprogramowania niezbędnego w ich pracy, a nadane im uprawnienia były adekwatne do sprawowanych funkcji; [3] dostęp do Internetu zapewniono na 28 komputerach, a pozostałe dwa ze względów bezpieczeństwa nie posiadły takiej funkcjonalności (co było zgodne z warunkami dostępu do systemów na nich zainstalowanych), [4] korzystano wyłącznie z aktualnych i dopuszczalnych aplikacji, w tym z oprogramowania antywirusowego; [5] dane były na bieżąco (codziennie) automatycznie archiwizowane. (dowód: akta kontroli str. 77-92, 210-217)

1.2. W Starostwie – zgodnie z § 5 regulaminu eksploatacyjnego systemów informatycznych, stanowiącego element PBI – informatyk przeprowadzał okresowe „przeglądy eksploatacyjne", wymagane § 20 ust. 2 pkt 3 rozporządzenia KRI. W latach 2016 – 2017 (do 19 października) w dzienniku systemu odnotowano 35 wewnętrznych przeglądów bądź testów: uprawnień, kont, aplikacji, stacji roboczych oraz serwerów. W żadnym przypadku nie stwierdzono nieprawidłowości. Informatyk wyjaśnił, że w latach 2014 – 2015 w Starostwie przeprowadzono dwa profesjonalne audyty informatyczne, które potwierdziły wysoki poziom bezpieczeństwa i od tego czasu nie wystąpiły żadne incydenty, a brak przeglądów zewnętrznych w kolejnych latach związany był z wysokimi kosztami takich usług. (dowód: akta kontroli str. 9, 47-74)

W wyniku dwóch ww. audytów w Starostwie m.in.: opracowano dokumentację bezpieczeństwa informacji, wprowadzono dodatkowe zabezpieczenia wewnątrzorganizacyjne (zobowiązano pracowników m.in. do uprzątnięcia i doposażenia serwerowni oraz dochowywania tajemnicy haseł), przewidziano systematyczną (nie rzadziej niż co dwa lata) realizację szkoleń z zakresu bezpieczeństwa informacji i technik

[9] Starostwo nie posiadało służbowych tabletów bądź innych urządzeń mobilnych skonfigurowanych z siecią lokalną.

informatycznych, a także wprowadzono obowiązek wyciągania konsekwencji z tytułu prób nieautoryzowanego dostępu przez dostawców usług. Jednocześnie audytorzy w listopadzie 2015 roku zwrócili uwagę Staroście na nieskuteczne zgłoszenie Administratora Bezpieczeństwa Informacji („ABI") do GIODO oraz niemonitorowanie dostępu do sieci Internet. W odpowiedzi Starosta zaznaczył, iż obowiązujące przepisy przewidywały uprawnienie (a nie obowiązek) powołania ABI, stąd zdecydował się na częściowe przekazanie kompetencji administratora danych osobowych dwóm pracownikom Wydziału Organizacyjnego Starostwa i zadeklarował rozważenie możliwości wprowadzenia mechanizmów monitorujących dostęp do Internetu. Do zakończenia niniejszej kontroli w Starostwie nie wprowadzono ww. monitorowania, ani nie powołano ABI, gdyż – jak wyjaśnił Starosta – „sytuacja w tym zakresie nie uległa zmianie", a dotychczasowe rozwiązanie organizacyjne uznał za „optymalne." (dowód: akta kontroli str. 75, 112-160)

1.3. Analiza 30 kont użytkowników korzystających z systemów informatycznych, w których przetwarzano dane wykazała, że wszyscy posiadali indywidualne loginy i hasła do systemów operacyjnych, a 27 (z 30) użytkowników posiadało także imienne upoważnienia Starosty do przetwarzania danych w poszczególnych systemach / programach, których zakres odpowiadał zakresom czynności służbowych tych osób. Nadanie uprawnień pięciu (z 27) pracowników, którzy rozpoczęli świadczenie pracy w okresie objętym kontrolą nastąpiło w pierwszym dniu zatrudnienia (w zbadanej próbie nie było pracowników, którzy w tym okresie zakończyli pracę w Starostwie). Z kolei trzech (z 30) pracowników Starostwa w dniu rozpoczęcia niniejszej kontroli nie posiadało upoważnień do przetwarzania danych w systemach, do których posiadali dostęp, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 77-92)

1.4. Na każdej z 30 poddanych oględzinom stacji roboczych istniała możliwość weryfikacji dostępu poszczególnych użytkowników poprzez elektroniczny dziennik systemowy, natomiast nie monitorowano logów poszczególnych aplikacji, ruchu sieciowego, a także danych wychodzących z sieci lokalnej Starostwa do sieci publicznej, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 77-92, 210-217)

1.5. Przeprowadzone w trakcie kontroli oględziny 30 stacji roboczych wykazały także, że na każdym urządzeniu hasła dostępowe do systemu operacyjnego spełniały wymagania przewidziane dla środków bezpieczeństwa na poziomie wysokim, tj. każdorazowe uwierzytelnienie użytkownika w systemie następowało po podaniu identyfikatora (w dwóch przypadkach indywidualnej karty) oraz odpowiedniej złożoności hasła lub PIN-u, a system wymuszał zmianę hasła, nie rzadziej niż co 30 dni. Dodatkowo analogiczne zabezpieczenia funkcjonowały w dwóch (z 13) lokalnych programach służących do przetwarzania danych osobowych (Płatnik i Homenet). W kolejnych sześciu programach (EGB, INFOSYSTEM, OŚRODEK, SIO, UPE i EZD) stosowano słabsze zabezpieczenia w postaci haseł o niższej złożoności, a wymuszenie ich zmiany następowało jedynie w dwóch programach (EGB i SIO). Informatyk Starostwa wyjaśnił, iż PBI przewiduje dwustopniowe uwierzytelnianie jedynie jeśli jest to technicznie możliwe i we wszystkich przypadkach stosowano zabezpieczenia zaprojektowane przez poszczególnych producentów, a niskie progi zabezpieczeń wynikały najczęściej ze starej architektury tego oprogramowania. Z kolei w pozostałych pięciu lokalnych aplikacjach wykorzystywanych do przetwarzania danych nie wprowadzono jakichkolwiek zabezpieczeń dostępu, co szerzej omówiono w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności ".

Starostwo posiadało także dwie sieci bezprzewodowe, tj. nie zabezpieczoną hasłem dla klientów Starostwa oraz sieć z dostępem na hasło (oględziny 30 komputerów wykorzystywanych w Starostwie wykazały, że żaden nie posiadał dostępu do tej sieci). Według informatyka Starostwa hot spot dla klientów pozostawał rozdzielony logicznie od sieci Starostwa i wyznaczono ograniczone pasma, tak aby wyeliminować blokowanie pracy (maks. 10 użytkowników na jeden z trzech utworzonych punktów dostępowych). Z kolei bezprzewodowa sieć wewnętrzna nie służyła do bieżącej pracy, a – jak wyjaśnił informatyk – pracowników nie zapoznawano z hasłem zmienianym średnio co 45 dni i była ona wykorzystywana tylko w wyjątkowych sytuacjach, tj. najczęściej podczas sesji bądź

szkoleń. Ponadto sieć bezprzewodowa umożliwiała jedynie dostęp do Internetu, a nie poszczególnych programów zainstalowanych na stacjach roboczych pracowników. Według informatyka obie sieci bezprzewodowe funkcjonowały około 12 miesięcy i nie odnotował on jakichkolwiek incydentów. (dowód: akta kontroli str. 47-50, 77-92, 210-217)

W opinii powołanego w trakcie niniejszej kontroli biegłego z zakresu teleinformatyki zabezpieczenie usług sieciowych, serwerowni, a także stacji roboczych w Starostwie było właściwe. (dowód: akta kontroli str. 210-217)

1.6. W regulacjach wewnętrznych Starostwa nie przewidziano możliwości wykorzystywania sprzętu prywatnego do realizacji obowiązków służbowych, czego powodem – jak wyjaśnił informatyk Starostwa – były względy bezpieczeństwa. W trakcie niniejszej kontroli ustalono jednak, że ze sprzętu takiego korzystał informatyk w trakcie wykonywanych zdalnie czynności służbowych, co omówiono szerzej w pkt 1.8. niniejszego wystąpienia pokontrolnego. (dowód: akta kontroli str. 5-46, 47-50, 77-92, 210-217)

W opinii powołanego w trakcie niniejszej kontroli biegłego z zakresu teleinformatyki jedyną drogą do przejęcia danych służbowych była możliwość podłączenia przez użytkowników pozasłużbowych pamięci zewnętrznych. Stwarzało to również niebezpieczeństwo zainfekowania komputerów złośliwym oprogramowaniem. Jednocześnie biegły zaznaczył, iż fakt podłączenia zewnętrznych nośników był odnotowywany w logach systemu operacyjnego, a logi generowane przez urządzenia sieciowe, systemy operacyjne i aplikacje specjalistyczne (mimo braku automatycznego monitorowania) zostały zabezpieczone przed utratą integralności i skasowania, co w razie potrzeby umożliwiało ustalenie użytkowników odpowiedzialnych za ewentualne naruszenia. Zgodnie z Instrukcją zarządzania, przechowywanie wymiennych nośników informacji (z wyjątkiem kopii bezpieczeństwa) dopuszczono jedynie w obszarze przetwarzania danych osobowych w siedzibie Starostwa.
(dowód: akta kontroli str. 5-46, 210-217)

1.7. W okresie objętym kontrolą nie odnotowano w Starostwie przypadków wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, fizycznej utraty danych i konieczności odtwarzania zbioru danych ze sporządzonych kopii bezpieczeństwa. Zdaniem Informatyka, ostatnie takie zdarzenie (atak na zabezpieczenia serwera) miało miejsce w 2013 roku. Zgłoszenie pochodziło od lokalnego dostawcy Internetu, jednak zabezpieczenia „wytrzymały" i nie było dalszych konsekwencji tego incydentu.
(dowód: akta kontroli str. 199-200)

1.8. W Starostwie dopuszczono możliwość „okresowego" użytkowania służbowych urządzeń przenośnych (laptopów) poza siecią Starostwa, jednak techniczną możliwość zdalnej łączności z zasobami jednostki utworzono jedynie dla administratora (informatyka). Przeprowadzone w trakcie niniejszej kontroli oględziny czterech (z sześciu posiadanych) laptopów wykazały, iż na żadnym z tych urządzeń nie zastosowano szyfrowania danych oraz żaden z laptopów służbowych nie został powierzony administratorowi. Informatyk Starostwa wyjaśnił, iż nigdy żaden z laptopów nie był wynoszony poza siedzibę, a zdalne łączenie się z zasobami jednostki wynikało z braku odpowiednio wykwalifikowanej osoby w razie jego nieobecności. W takich sytuacjach informatyk wykorzystywał „zabezpieczony komputer prywatny", co szerzej omówiono w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności ". Częstotliwość takich logowań informatyk określił na średnio „kilka w tygodniu". (dowód: akta kontroli str. 9, 47-50, 77-92, 210-217)

1.9. W okresie objętym kontrolą Starostwo nie korzystało z naprawy komputerów przez firmy zewnętrzne, gdyż – jak wyjaśnił Informatyk – obecnie użytkowany sprzęt, po kompleksowej wymianie w 2015 roku, jest stosunkowo nowy i zasadniczo nie wymagał napraw w dwóch ostatnich latach. Drobne usterki mechaniczne sprzętu oraz zgłoszenia nieprawidłowej pracy wszystkich programów sieciowych eliminował osobiście.
(dowód: akta kontroli str. 47-50)

1.10. W celu ochrony systemów informatycznych Starostwa zastosowano zabezpieczenia w postaci m.in. firewalla sprzętowego, systemu antywirusowego i antyspamowego uznane przez powołanego biegłego z zakresu teleinformatyki za „profesjonalne". Oględziny 30 z 42 użytkowanych w Starostwie komputerów wykazały także, że na wszystkich urządzeniach

zainstalowany został program antywirusowy, a jego aktualizacja odbywała się automatycznie, jednak na wszystkich pięciu stacjach roboczych służących do obsługi systemu zewnętrznego (CEPIK) baza antywirusowa była nieaktualna. Informatyk Starostwa wyjaśnił, iż nie miał wpływu na proces aktualizacji tej bazy, gdyż administrowanie i nadzór nad tym systemem prowadzi podmiot zewnętrzny.

(dowód: akta kontroli str. 77-92, 97, 210-220)

W opinii ww. biegłego zastosowane w tym zakresie rozwiązania pozwalały uznać, iż elektroniczne zasoby informacyjne Starostwa były właściwie chronione przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych.

(dowód: akta kontroli str. 210-217)

1.11. W okresie objętym kontrolą Starostwo posiadało wykupioną usługę hostingu strony internetowej oraz domeny internetowej w podmiocie zewnętrznym, przy czym nie dysponowano pisemną umową zawartą z tym podmiotem, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Informatyk dodał, iż adresy, z których otrzymywano wiadomości typu SPAM były przez niego dodatkowo ręcznie blokowane (przy składaniu wyjaśnienia okazał listę tych adresów), gdyż firewall nie był zabezpieczeniem stuprocentowym – w jego opinii na rynku nie było w pełni skutecznych narzędzi w tym zakresie. (dowód: akta kontroli str. 47-50)

1.12. Kopie zapasowe danych z posiadanych systemów i aplikacji wykonywane były automatycznie (dwa razy dziennie) na serwerze głównym Starostwa. Najstarsza kopia zapasowa (sprzed siedmiu dni) zastępowana była najnowszą. Informatyk odpowiedzialny był także za codzienne sporządzanie kopii bezpieczeństwa na mobilnym elektronicznym nośniku informacji (zastępowanie najstarszej kopii następowało w sposób analogiczny), który przewożony był do jednej z jednostek podległych. Według informatyka zastosowanie takiego rozwiązania wynikało z zaleceń audytora wewnętrznego, a nienaruszalność poufności danych gwarantowało stosowanie zabezpieczeń na odpowiednio wysokim poziomie (nośnik analogicznie do stacji roboczych zabezpieczono hasłem o odpowiedniej złożoności). W okresie objętym kontrolą nie wystąpiła w Starostwie konieczność odtwarzania zbioru danych ze sporządzonych kopii, a testowanie kopii odbywało się zgodnie z PBI raz do roku. (dowód: akta kontroli str. 47-50, 77-92, 199-200, 210-217)

1.13. Na każdej z 30 poddanych oględzinom stacji roboczych zainstalowane było wyłącznie dopuszczone oprogramowanie służbowe, posiadające wsparcie producentów, a do konfigurowania systemu przewidziano wyłącznie administratora. Według biegłego z zakresu teleinformatyki pracownicy posiadali techniczną możliwość ściągnięcia aplikacji i plików wykonalnych, ale bez możliwości ich zainstalowania i uruchomienia, co jego zdaniem było rozwiązaniem w pełni bezpiecznym.

(dowód: akta kontroli str. 77-92, 210-217)

1.14. Według informatyka Starostwa aktualizacja poszczególnych programów branżowych każdorazowo następowała ręcznie po przeprowadzeniu konsultacji z kierownikiem danej komórki organizacyjnej, aby wyeliminować dodawanie aktualizacji zbędnych z punktu widzenia zadań Starostwa. Zaakceptowane aktualizacje zdaniem informatyka następowały w terminie kilkudniowym po udostępnieniu aktualizacji. W opinii biegłego z zakresu teleinformatyki przy instalacji aktualizacji administrator podejmował szereg istotnych i właściwych działań (proces poprzedzano sprawdzeniem autentyczności pakietu aktualizacyjnego, weryfikacją zakresu aktualizacji i zasadności jej instalacji oraz przydatności poszczególnym użytkownikom). Informatyk Starostwa nie wykonywał natomiast aktualizacji bazy antywirusowej na komputerach służących do obsługi systemu zewnętrznego, co omówiono w pkt 1.10 niniejszego wystąpienia.

(dowód: akta kontroli str. 47-50, 210-220)

1.15. Zgodnie z obowiązującą w Starostwie polityką rachunkowości, poza tradycyjną (papierową) formą sporządzania i przesyłania przelewów, uruchomiono także płatności drogą elektroniczną z wykorzystaniem oprogramowania Homenet. Wykonanie takiego przelewu, po zatwierdzeniu dokumentu pod względem merytorycznym i formalno-rachunkowym, wymagało od wskazanego pracownika Wydziału Finansowego wpięcia się do systemu dedykowanym narzędziem (klucz do podpisu znajdował się na mobilnym

228

nośniku). Analogiczne zabezpieczenie wymagane było do zatwierdzenia przez Skarbnika, Starostę bądź Wicestarostę. (dowód: akta kontroli str. 47-50, 161-166)

Ustalone nieprawidłowości

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

1. Trzech (spośród 30 analizowanych) użytkowników systemów / programów informatycznych, w których przetwarzano dane osobowe, nie posiadało imiennych upoważnień Starosty do przetwarzania takich danych, mimo wymogu ustalonego w pkt 4 – 5 załącznika nr 4 do PBI (dotyczyło to księgowej, inspektora w Wydziale Organizacyjnym oraz informatyka). Informatyk wyjaśnił, że ww. księgowa zajmowała się z reguły płacami, a inspektor przede wszystkim obroną cywilną, tak więc co do zasady oboje mieli dostęp do danych ogólnodostępnych i danych pracowników Starostwa, a nie osób z zewnątrz. Z kolei brak swojego upoważnienia wyjaśnił faktem, iż Starosta pośrednio upoważnił go do takiego przetwarzania innymi dokumentami, w tym zakresem czynności i regulacjami PBI, a zatem ewentualne upoważnienie byłoby jedynie powieleniem już posiadanych upoważnień. Ponadto wyjaśnił, że wszystkie trzy ww. osoby złożyły oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych, zobowiązały się do ich przestrzegania i zgłaszania wszelkich naruszeń w tym zakresie. W trakcie niniejszej kontroli NIK uzupełnione zostały upoważnienia dla wszystkich trzech ww. pracowników.
(dowód: akta kontroli str. 24, 47-50, 77-92, 199-203)

2. W latach 2016 – 2017 w Starostwie nie monitorowano dostępu do informacji, mimo takiego wymogu zawartego w § 20 ust. 2 pkt 7 lit a rozporządzenia KRI, gdyż nie analizowano logów poszczególnych aplikacji, ruchu sieciowego, a także danych wychodzących z sieci lokalnej Starostwa do sieci publicznej. Według informatyka czynności tych nie wykonywano, ponieważ nie było przesłanek wskazujących na taką potrzebę, a wprowadzenie takiego obowiązku znacznie spowolniłoby pracę systemów. Ponadto ewentualny zakup narzędzia informatycznego służącego do automatycznego monitorowania wiązałoby się ze znaczącymi kosztami.
(dowód: akta kontroli str. 47-50, 77-92, 210-217)

   W opinii powołanego w trakcie niniejszej kontroli biegłego z zakresu teleinformatyki wdrożenie narzędzi do automatycznego gromadzenia, zabezpieczania i analizy logów dotyczących dostępu do informacji jest niezbędne do skutecznej kontroli bezpieczeństwa informacji. (dowód: akta kontroli str. 210-217)

3. W okresie objętym kontrolą Starostwo korzystało z usług hostingu strony internetowej oraz domeny internetowej w podmiocie zewnętrznym, jednak bez podpisanej umowy z tym podmiotem, tj. wbrew wymogom § 20 ust. 2 pkt 10 rozporządzenia KRI. Jak wyjaśnił informatyk Starostwa, powodem była niska wartość tej usługi (kilkaset złotych rocznie). (dowód: akta kontroli str. 47-50)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na:

1. Niewyposażenie administratora w służbowy laptop, służący do pracy zdalnej oraz łączenia się z zasobami jednostki i wykorzystywanie do tego celu sprzętu prywatnego, co może podnosić ryzyko utraty danych. Odpowiedzialny za nadzór nad pracą administratora inspektor z Wydziału Organizacyjnego Starostwa wyjaśnił, że generalnie w jednostce nie zachodzi potrzeba administrowania systemami informatycznymi poza godzinami pracy, a jeśli były takie przypadki odbywały się one za wiedzą przełożonych. Dodał, że problem ten zostanie przeanalizowany i w razie stwierdzenia takiej potrzeby informatyk zostanie doposażony w odpowiedni sprzęt. W opinii powołanego w trakcie niniejszej kontroli biegłego z zakresu teleinformatyki nieprofesjonalne jest prowadzenie prac administracyjnych z komputera, który nie jest do tego dedykowany. Jeśli specyfika pracy Starostwa tego wymaga, należy wyposażyć administratora w komputer przenośny i niezbędne oprogramowanie, co pozwoliłoby administratorowi realizować powierzone zadania z zachowaniem należytego profesjonalizmu i bezpieczeństwa.
(dowód: akta kontroli str. 9, 47-50, 77-92, 112, 168-170, 210-217)

2. Niewprowadzenie zabezpieczeń dostępu (haseł bądź PIN-ów) w pięciu lokalnych aplikacjach wykorzystywanych do przetwarzania danych (Foris, Legislator, Foldery, Geodezja i Aplikacje Własne), co mogło mieć w pływ na obniżenie poziomu bezpieczeństwa danych w nich zamieszczonych. Informatyk Starostwa wyjaśnił, iż brak dodatkowych zabezpieczeń w tych systemach spowodowany był brakiem takiej funkcjonalności, a jej ewentualne zamówienie u producentów wiązałoby się z pracochłonnością i odpłatnością. (dowód: akta kontroli str. 47-48, 84)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, skuteczność przyjętych w Starostwie rozwiązań dotyczących zabezpieczenia dostępu do poszczególnych systemów informatycznych i usług sieciowych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych.

2. Dokumentacja i procedury dotyczące ochrony danych osobowych

Opis stanu faktycznego

2.1. W latach 2016 – 2017 Starostwo nie dysponowało aktualnym wykazem zbiorów danych osobowych. Posiadany wykaz, będący elementem regulacji wewnętrznych dotyczących bezpieczeństwa, zawierał 33 zbiory (w tym 16 funkcjonujących z wykorzystaniem systemów informatycznych), chociaż w okresie objętym kontrolą w Starostwie przetwarzano dane osobowe w 47 zbiorach (w tym w 22 przetwarzano dane z wykorzystaniem systemów informatycznych). Do dnia rozpoczęcia niniejszej kontroli Starostwo zarejestrowało w GIODO jedynie 16 (z 22) zbiorów danych osobowych prowadzonych z wykorzystaniem systemów informatycznych (zgłoszenia nastąpiły przed 1 stycznia 2016 r.), co szerzej omówiono w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". W okresie objętym kontrolą nie aktualizowano danych, ani nie występowano do GIODO o wykreślenie zarejestrowanego zbioru. Nie nastąpiła również odmowa rejestracji. (dowód: akta kontroli str. 47-50, 56-59, 77-92, 168-170)

2.2. Obowiązująca w Starostwie PBI przewidywała funkcjonowanie ABI oraz określała dla niego zakres zadań. W związku z nieskutecznym zgłoszeniem ABI (nie zawierało ono wszystkich wymaganych elementów formalnych) do GIODO z 2015 roku, Starosta zrezygnował z jego powoływania i powierzył wykonywanie części obowiązków ABI dwóm pracownikom (rozszerzając zakresy czynności). Inspektora w Wydziale Organizacyjnym zobowiązano m.in. do sprawdzania zgodności przetwarzania danych osobowych z przepisami, zapewnienia zapoznawania się osób upoważnionych z tymi przepisami oraz nadzoru nad zabezpieczeniem danych i przestrzeganiem przepisów, a także do aktualizacji dokumentacji w tym zakresie. Informatyka zaś zobowiązano do współpracy z ww. inspektorem. (dowód: akta kontroli str. 5-46, 75, 112-123)

2.3. Stosownie do przepisu art. 36b ustawy o ochronie danych osobowych, w latach 2016 – 2017 zapoznano pracowników przetwarzających dane z przepisami regulującymi te kwestie. Nie przeprowadzano natomiast kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Nie aktualizowano też dokumentacji opisującej przetwarzanie danych osobowych, co omówiono szerzej w pkt 2.10. niniejszego wystąpienia pokontrolnego.
(dowód: akta kontroli str. 47-50, 77-92, 168-170, 202)

2.4. W Starostwie prowadzono ewidencję osób upoważnionych do przewarzania danych osobowych obejmującą wszystkie elementy określone w art. 39 ust. 1 ustawy o ochronie danych osobowych. Jednak nie wszyscy pracownicy Starostwa przetwarzający takie dane posiadali wymagane upoważnienia, a administratora jedynego systemu zewnętrznego nie poinformowano na bieżąco o zmianach w ewidencji pracowników upoważnionych do przetwarzania danych osobowych w tym systemie, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Zgodnie z wymogami art. 38 ustawy o ochronie danych osobowych, w Starostwie zapewniono kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbiorów wprowadzone. Nie weryfikowano natomiast prawidłowości procesu przekazywania tych danych, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 47-50, 77-96, 171-177)

230

2.5. W okresie objętym kontrolą nie wystąpiły zmiany organizacyjne uzasadniające potrzebę aktualizacji regulacji wewnętrznych dotyczących gromadzenia i przetwarzania posiadanych zasobów informacyjnych. Nieaktualizowanie dokumentacji opisującej przetwarzanie danych osobowych omówiono szerzej w pkt 2.10. niniejszego wystąpienia pokontrolnego.

(dowód: akta kontroli str. 5-50, 168-170,199)

2.6. Regulacje wewnętrzne dotyczące bezpieczeństwa informacji informatykowi powierzały obowiązki związane z administrowaniem systemami, w których gromadzono i przetwarzano dane osobowe. Do jego zadań należało m.in. zabezpieczenie zbiorów danych prowadzonych w systemach informatycznych oraz przeciwdziałanie dostępowi osób niepowołanych do systemów, w których przetwarzano takie dane. Informatyk został zapoznany z przepisami dotyczącymi bezpieczeństwa teleinformatycznego, zobowiązał się do zachowania w tajemnicy przetwarzanych danych oraz ich zabezpieczenia, a w trakcie niniejszej kontroli otrzymał brakujące upoważnienie do przetwarzania danych osobowych we wszystkich systemach informatycznych Starostwa.

(dowód: akta kontroli str. 5-46, 116-122, 201-203)

2.7. W Starostwie w latach 2016 – 2017 (do 5 grudnia) 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. 47-50)

2.8. W okresie objętym kontrolą pracownicy Starostwa nie uczestniczyli w szkoleniach z zakresu bezpieczeństwa przetwarzania danych / informacji, co szerzej omówiono w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 168-170, 194)

2.9. W okresie objętym kontrolą Starostwo nie było kontrolowane przez podmioty zewnętrzne w zakresie bezpieczeństwa danych. W latach 2016 – 2017 nie otrzymywało również skarg związanych z przypadkami ujawnienia danych osobowych. W czerwcu 2016 roku Starosta otrzymał zaś z GIODO wystąpienie, będące wynikiem czynności sprawdzających, wynikających ze skargi, złożonej do tej instytucji przez osobę fizyczną. W sprawie tej chodziło o bezprawne upublicznienie danych osobowych skarżącego (imienia i nazwiska) w treści opublikowanej uchwały i w związku z tym zalecono wyeliminowanie podobnych nieprawidłowości. W odpowiedzi Starosta potwierdził usunięcie danych osobowych skarżącego, a także zobowiązał pracowników do anonimizowania wszelkich danych osobowych przed publikacją dokumentów.

(dowód: akta kontroli str. 103-106, 199-200)

2.10. Zarządzeniem Nr 120.20.2014 Starosty Zambrowskiego z 30 września 2014 r., wprowadzono PBI, politykę bezpieczeństwa przetwarzania danych osobowych oraz Instrukcję zarządzania. Ww. regulacje spełniały wymogi formalne określone w rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych, jednak zawierały nieaktualny wykaz zbiorów przetwarzanych danych osobowych oraz nie uzupełniono obszaru przetwarzania poszczególnych danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 5-50, 77-92)

Ustalone nieprawidłowości

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

1. Do dnia rozpoczęcia niniejszej kontroli NIK nie zarejestrowano w GIODO sześciu z 22 zbiorów danych osobowych prowadzonych w Starostwie z wykorzystaniem systemów informatycznych, co naruszało wymogi art. 40 ustawy o ochronie danych osobowych. Odpowiedzialny za rejestrację w GIODO informatyk Starostwa wyjaśnił, że niezgłoszenie tych zbiorów wynikało z braku informacji w tym zakresie od kierowników komórek organizacyjnych Starostwa. W trakcie niniejszej kontroli zgłoszono do GIODO sześć brakujących zbiorów danych osobowych prowadzonych z wykorzystaniem systemów informatycznych, a ww. zgłoszenia zawierały wszystkie elementy wymagane art. 41 ust. 1 ustawy o ochronie danych osobowych.

(dowód: akta kontroli str. 49, 56-59, 77-92,199-200)

2. W Starostwie w okresie objętym kontrolą 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. Odpowiedzialny za to zadanie inspektor z Wydziału Organizacyjnego Starostwa wyjaśnił, że powodem tego był brak incydentów związanych z przetwarzaniem danych osobowych oraz niestwierdzenie nieprawidłowości w obszarze danych osobowych w trakcie audytów z lat 2014 – 2015. Zaznaczył także, że przywołane przepisy nie określały formy i częstotliwości takich kontroli.
(dowód: akta kontroli str. 112-115, 168-170)

3. W okresie objętym kontrolą pracownicy Starostwa nie uczestniczyli w szkoleniach z zakresu bezpieczeństwa przetwarzania danych / informacji. Obowiązek zapewnienia szkoleń osobom zaangażowanym w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo, wynika z § 20 ust. 2 pkt 6 rozporządzenia KRI. Ponadto w opinii powołanego w trakcie niniejszej kontroli biegłego z zakresu teleinformatyki rozmiar oraz poziom zarządzania siecią informatyczną uzasadnia rozważenie podniesienia wiedzy specjalistycznej informatyka, w szczególności w zakresie obsługi urządzeń CISCO. Odpowiedzialny za to zadanie inspektor z Wydziału Organizacyjnego Starostwa wyjaśnił, że audyty z lat 2014 – 2015 nie wykazały nieprawidłowości, a w ostatnich latach nie było incydentów naruszenia danych osobowych. Dodał, że większość pracowników to doświadczeni, długoletni urzędnicy, którzy w przypadkach problematycznych zwracali się do niego o pomoc i ją otrzymywali. Inspektor zadeklarował jednocześnie rozpoczęcie cyklu wewnętrznych szkoleń z zakresu przetwarzania danych osobowych.
(dowód: akta kontroli str. 168-170, 194)

4. Trzech (spośród 30 analizowanych) pracowników, którzy przetwarzali dane osobowe z wykorzystaniem systemów informatycznych, do dnia rozpoczęcia kontroli NIK nie posiadało imiennych upoważnień Starosty do przetwarzania takich danych (dotyczyło to księgowej, inspektora w Wydziale Organizacyjnym oraz Informatyka), co było niezgodne z art. 37 ustawy o ochronie danych osobowych. Odpowiedzialny za to inspektor z Wydziału Organizacyjnego Starostwa wyjaśnił, że chodzi o pracowników z wieloletnim stażem na zajmowanych stanowiskach, którzy – mimo braku oddzielnego dokumentu „upoważnienia" – posiadali zakresy obowiązków, z których wynikało „adekwatne" upoważnienie do przetwarzania takich danych. W trakcie niniejszej kontroli NIK wydano stosowne upoważnienia tym pracownikom. (dowód: akta kontroli str. 77-92, 168-170)

5. Administratora systemu zewnętrznego (CEPIK) nie poinformowano o rozwiązaniu stosunku pracy z dwoma pracownikami upoważnionymi do przetwarzania danych osobowych w tym systemie, co było niezgodne z art. 36 ustawy o ochronie danych osobowych. W konsekwencji w wykazie aktywnych kont w trakcie niniejszej kontroli nadal pozostawali dwaj byli pracownicy Starostwa, których zatrudnienie ustało w listopadzie 2014 roku i w lipcu 2017 roku. Informatyk wyjaśnił, że obie osoby odchodząc z pracy rozliczyły się z kart służących do obsługi systemu, jednak ówczesny kierownik Wydziału nie zgłosił potrzeby usunięcia konta dla pracownika odchodzącego w listopadzie 2014 roku. Z kolei zgłoszenie usunięcia konta dla ww. kierownika mogło nastąpić dopiero po otrzymaniu certyfikatu przez jego następcę, co miało miejsce dopiero 28 listopada br. Ostatecznie w trakcie kontroli NIK wystąpiono do administratora systemu CEPIK o usunięcie kont obu pracowników.
(dowód: akta kontroli str. 47-50, 171-177)

6. W Starostwie od 2016 roku 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. Informatyk wyjaśnił, że w latach 2014 – 2015 przeprowadzono profesjonalne audyty informatyczne, które potwierdziły wysoki poziom bezpieczeństwa i od tego czasu nie wystąpiły żadne

235

incydenty, a brak ww. audytów w kolejnych latach związany był z wysokimi kosztami takich usług. (dowód: akta kontroli str. 47-50)

7. W okresie objętym kontrolą nie zaktualizowano polityki bezpieczeństwa przetwarzania danych osobowych, chociaż zamieszczono w niej nieaktualny wykaz zbiorów danych osobowych oraz służącego do tego oprogramowania (wraz z określeniem przepływu danych między systemami) oraz nieaktualny obszar przetwarzania danych osobowych. Naruszono w ten sposób wymóg § 20 ust. 2 pkt 1 rozporządzenia KRI. Odpowiedzialny za to inspektor z Wydziału Organizacyjnego Starostwa stwierdził, że ww. regulacje zostaną zaktualizowane. (dowód: akta kontroli str. 5-46, 168-170,199-200)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości działalność Starostwa dotyczącą opracowania i wdrożenia dokumentacji oraz procedur ochrony danych, natomiast negatywnie zgłaszanie zbiorów do GIODO, a także realizację ustawowych zadań administratora danych osobowych, w tym przez pracowników, którym powierzono część tych zadań.

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. W Starostwie zapewniono ochronę pomieszczeń, sprzętu i infrastruktury informatycznej przed działaniem czynników fizycznych i zdarzeń nadzwyczajnych (pożaru, kradzieży, wandalizmu itp.) zgodną z postanowieniami PBI i Instrukcji zarządzania. Nie opracowano tzw. „polityki kluczy", jednak wprowadzono regulację wewnętrzną określającą listę pracowników posiadającą dostęp do pomieszczeń służbowych poza godzinami pracy, a także stosowano zbiorcze skrzynki na klucze. Siedzibę Starostwa wyposażono w system alarmowy, przeciwpożarowy, a także monitoring (wewnętrzny i zewnętrzny). W trakcie oględzin nie stwierdzono uchybień skutkujących potencjalnym zagrożeniem utraty bądź zniszczenia danych. (dowód: akta kontroli str. 77-96)

3.2. Informatyk Starostwa na bieżąco gromadził dane, o których mowa w § 20 ust. 2 pkt 2 rozporządzenia KRI, tj. prowadził w formie elektronicznej ewidencję obejmującą aktualne dane dotyczące całości służbowego sprzętu informatycznego (rodzaj sprzętu wraz z konfiguracją) i oprogramowania (systemy operacyjne, programy i aplikacje branżowe, posiadane licencje itp.). (dowód: akta kontroli str. 77-96)

3.3. W okresie objętym kontrolą zlikwidowano dwa komputery, 23 programy, a także inny sprzęt biurowy (m.in. monitory, drukarki i kserokopiarki), które przekazano do firmy utylizacyjnej. Informatyk wyjaśnił, iż dane z likwidowanego sprzętu zostały zabezpieczone poprzez usunięcie dysków i złożenie w szafie pancernej, która była w jego dyspozycji. Nośniki oprogramowania zostały zaś przed przekazaniem komisyjnie trwale uszkodzone. (dowód: akta kontroli str. 50, 187-191)

3.4. Do niszczenia bieżących wydruków oraz dokumentów niewymagających archiwizacji wykorzystywano w Starostwie 14 niszczarek (w poszczególnych wydziałach znajdowało się od jednej do trzech sztuk, a jedna ogólnodostępna niszczarka umieszczona została w sekretariacie), jednak nie opracowano w tym zakresie żadnych wytycznych lub procedur. Według informatyka do tej pory przy niszczeniu zbędnej dokumentacji nie było potrzeby korzystania z usług podmiotów zewnętrznych. (dowód: akta kontroli str. 77-92, 219-220)

3.5. Starostwo zabezpieczyło się przed ryzykiem utraty danych w trakcie realizacji usług sprzątania pomieszczeń. Do umowy z podmiotem zewnętrznym wprowadzono bowiem obostrzenia dotyczące m.in.: dostępu do wybranych pomieszczeń wyłącznie w godzinach pracy oraz przy obecności uprawnionego pracownika, a także klauzulę o dochowaniu tajemnicy w związku z realizacją tych usług. Ponadto z oświadczenia informatyka wynika, że pomieszczenia serwerowni zostały wyłączone z tej umowy i sprzątane były przez niego osobiście. (dowód: akta kontroli. str. 77-92, 107-111)

3.6. Zgodnie z pkt XI Instrukcji zarządzania, przeglądy oraz konserwacja sprzętu i oprogramowania informatycznego powinny być realizowane zgodnie z zaleceniami poszczególnych producentów. W okresie objętym kontrolą Starostwo nie korzystało z napraw świadczonych przez firmy zewnętrzne. Informatyk wyjaśnił, iż obecnie użytkowany sprzęt – po kompleksowej wymianie w 2015 roku – jest stosunkowo nowy i zasadniczo nie

wymagał napraw w dwóch ostatnich latach. Z kolei drobne usterki mechaniczne sprzętu oraz zgłoszenia nieprawidłowej pracy wszystkich programów sieciowych eliminował osobiście. (dowód: akta kontroli str. 40, 48)

3.7. Starostwo wyposażyło serwer główny w urządzenie UPS, umożliwiające podtrzymanie jego pracy na ok. 30 minut, a przeprowadzone w trakcie kontroli oględziny 30 stacji roboczych wykazały, że 28 komputerów posiadało zasilacze awaryjne UPS bądź akumulatory podtrzymujące zasilanie. Takiego wyposażenia brakowało na dwóch komputerach stacjonarnych w Wydziale Komunikacji. Ponadto w Starostwie nie opracowano procedur na wypadek wystąpienia sytuacji nadzwyczajnych, w tym długotrwałego braku zasilania, dotyczących przywracania systemów po awarii oraz planu ciągłości działania, umożliwiającego kontynuację wykonywania zadań publicznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności". (dowód: akta kontroli str. 4-50, 77-92, 199)

3.8. W okresie objętym kontrolą nie stwierdzono w Starostwie przypadków fizycznej utraty danych i konieczności odtwarzania ich z kopii bezpieczeństwa.
(dowód: akta kontroli str. 199-200)

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na potrzebę opracowania w Starostwie wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. długotrwałego braku zasilania lub przywracania systemów po awarii oraz planu ciągłości działania, umożliwiającego kontynuację wykonywania zadań. Dokument ten powinien określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany. Istotne jest, aby były one jasno udokumentowane, przekazane pracownikom i aktualizowane w celu odzwierciedlenia bieżącej działalności jednostki. Starostwo nie było też w pełni przygotowane do wykonywania zadań w sytuacji długotrwałej utraty zasilania. Nie posiadało bowiem agregatu prądotwórczego, a dwa (z 30 analizowanych) komputerów nie posiadały zasilaczy awaryjnych UPS bądź urządzeń o podobnej funkcjonalności. Informatyk wyjaśnił, że żaden z pięciu komputerów otrzymanych do obsługi systemu CEPIK nie został przekazany wraz z UPS-em i ze względu na wysoką wartość tego sprzętu oraz ryzyko potencjalnego zwarcia w UPS-ie zdecydowano się nie dostawiać własnych urządzeń podtrzymujących zasilanie. Dodał, że żadna z instytucji publicznych zlokalizowana w budynku będącym siedzibą Starostwa nie posiadała agregatu, a negocjacje na temat przyszłej lokalizacji i sfinansowania jego zakupu trwają od kilku lat. Jednocześnie zaznaczył, iż jedyna długotrwała przerwa w dostawach prądu miała miejsce raz w okresie ostatnich 10 lat. Obowiązek zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej wynika z regulacji rozdz. A pkt. III załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych.
(dowód: akta kontroli str. 4-50, 77-92,199)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działania Starostwa dotyczące przestrzegania przyjętych procedur w zakresie przechowywania i zabezpieczania danych, które zapewniały ich właściwą ochronę.

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności jednostki

Opis stanu faktycznego

4.1. W okresie objętym kontrolą w Starostwie przetwarzano dane w 47 zbiorach danych, z których 22 prowadzono z wykorzystaniem systemów informatycznych, a pozostałe 25 w formie tradycyjnej (papierowej). Z kolei w wykazie zbiorów danych zawartych w PBI ujęto 33 zbiory i tyle samo zgłoszono do GIODO. (dowód: akta kontroli str. 77-92)

4.2. Spośród zgłoszonych zbiorów danych, w 21 przypadkach zakres przetwarzanych danych był zgodny ze zgłoszeniem, zaś w 12 przypadkach w latach 2016 – 2017 gromadzono również dane nie objęte zgłoszeniem, co szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 77-92)

234

4.3. Analiza 47 zbiorów danych prowadzonych w poszczególnych komórkach organizacyjnych Starostwa wykazała, że we wszystkich przypadkach zakres przetwarzanych danych był niezbędny do realizacji zadań przypisanych poszczególnym komórkom. (dowód: akta kontroli str. 77-92)

Starostwo informowało kandydatów do pracy o uprawnieniach wynikających z art. 24 ust. 1 ustawy o ochronie danych osobowych. W ogłoszeniach wzmiankowano m.in. o obowiązku składnia oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych oraz podstawie prawnej takiego żądania, a dokumenty kandydatów do pracy – w zależności od wyników konkursu – były włączane do akt osobowych, wydawane nadawcom albo komisyjnie niszczone, o czym również uprzednio informowano w ogłoszeniach rekrutacyjnych. (dowód: akta kontroli str. 76, 195-198)

4.4. Starostwo uzyskało dostęp do jedynego zewnętrznego zbioru danych przetwarzanych z wykorzystaniem systemu informatycznego (CEPIK) na podstawie umowy zawartej z Polską Wytwórnią Papierów Wartościowych S.A. i spełniło wymogi techniczno-organizacyjne dostępu do tego zbioru danych, które określał załącznik nr 5 do tej umowy. (dowód: akta kontroli str. 77-92, 178-183)

Starostwo nie informowało jednak na bieżąco administratora systemu CEPIK o zmianach w ewidencji osób (pracowników) upoważnionych do przetwarzania danych osobowych w tym systemie, co szerzej opisano w pkt 2 wystąpienia pokontrolnego. (dowód: akta kontroli str. 47-50, 77-92, 171-177)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na niezgłoszeniu GIODO informacji o rozszerzeniu w latach 2016 – 2017 zakresu przetwarzanych danych w 12 zbiorach danych osobowych. Naruszono w ten sposób wymogi art. 41 ust. 2 ustawy o ochronie danych osobowych. Informatyk wyjaśnił, że kierownicy poszczególnych wydziałów zgłaszali przed laty problem braku miejsca do wpisania kolejnej kategorii danych innych niż enumeratywnie wymienione, jednak ostatecznie – po wyeliminowaniu tej przeszkody technicznej – nie zgłaszano już potrzeby aktualizowania danych do GIODO. (dowód: akta kontroli str. 47-50, 77-92)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonej nieprawidłowości, sposób przetwarzania zasobów informacyjnych, który był zgodny z zakresem działalności Starostwa. W odniesieniu do zbioru zewnętrznego, spełniono wymogi związane z dostępem do tego zbioru.

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[10], wnosi o:

1. Monitorowanie dostępu do informacji stosownie do wymogów § 20 ust. 2 pkt 7 lit. a rozporządzenia KRI.
2. Podpisanie z usługodawcą hostingu strony internetowej oraz domeny internetowej umowy spełniającej wymogi zawarte w § 20 ust. 2 pkt 10 rozporządzenia KRI.
3. Przeprowadzanie, w ramach realizacji obowiązku – wynikającego z art. 36a ust. 2 w związku z art. 36b ustawy o ochronie danych osobowych – okresowych kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
4. Zaktualizowanie przyjętych regulacji wewnętrznych oraz zapewnienia audytów wewnętrznych z zakresu bezpieczeństwa informacji, stosownie do z § 20 ust. 1 i ust. 2 pkt 1 i 14 rozporządzenia KRI.
5. Zapewnienie pracownikom zaangażowanym w proces przetwarzania informacji szkoleń, o których mowa w § 20 ust. 2 pkt 6 rozporządzenia KRI.

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

6. Zgłaszanie GIODO wszelkich zmian dotyczących zarejestrowanych zbiorów danych, zgodnie z wymogami art. 41 ust. 2 ustawy o ochronie danych osobowych.
7. Ujęcie wszystkich zbiorów wykorzystywanych w Starostwie w wykazie zbiorów danych osobowych, stanowiącym element regulacji wewnętrznej dotyczącej bezpieczeństwa informacji.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika 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 12 stycznia 2018 r.

Adrian Gosk
specjalista kontroli państwowej

.....
podpis

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

.....
podpis