NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.13.2017
P/17/062

02264017

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
Kontroler	Piotr Jurkin – starszy inspektor k. p., upoważnienie do kontroli nr LBI/166/2017 z 27 listopada 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Starostwo Powiatowe w Łomży, ul. Szosa Zambrowska 1/27, 18-400 Łomża[1]
Kierownik jednostki kontrolowanej	Elżbieta Parzych – Starosta Łomżyński[2] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[3]

Ocena ogólna

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

Uzasadnienie oceny ogólnej

Stwierdzono bowiem nieprawidłowości polegające w szczególności na:

- niezabezpieczeniu hasłem dostępu do trzech (z 30 objętych oględzinami) komputerów, za pomocą których przetwarzano dane osobowe, co naruszało przepis § 20 ust. 2 pkt 7 lit. c 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[5], w związku z § 6 ust. 4 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],
- niewykonywaniu kopii bezpieczeństwa pięciu (z ośmiu) systemów wykorzystywanych do przetwarzania danych osobowych, tj. wbrew wymogom pkt IV załącznika do rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych,
- nieanalizowaniu i niezabezpieczaniu przed modyfikacją lub zniszczeniem logów systemów operacyjnych, mimo takiego wymogu zawartego w § 20 ust. 2 pkt 7 lit a rozporządzenia KRI,
- niezamieszczeniu w umowach na świadczenie usług poczty elektronicznej zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający ujawnienie osobom nieuprawnionym, co naruszało § 20 ust. 2 pkt 9 i 10 rozporządzenia KRI,
- umożliwieniu 25 pracownikom (z 30 objętych badaniem) przetwarzania danych w zbiorze danych osobowych EZD SmartDoc bez stosownych upoważnień oraz upoważnieniu informatyka Starostwa do przetwarzania danych osobowych

---

1 Dalej: „Starostwo".
2 Pełniąca funkcję od 5 grudnia 2014 r.
3 Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
4 Kontrolą objęty został okres od 1 stycznia 2016 r. do zakończenia czynności kontrolnych.
5 Dz. U. z 2017 poz.2247. Rozporządzenie zwane dalej: „rozporządzeniem KRI".
6 Dz. U. Nr 100 poz. 1024. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie dokumentacji przetwarzania danych osobowych".

w administrowanych systemach dopiero w trakcie kontroli NIK, co naruszało art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[7],

- odebraniu trzem osobom, które zaprzestały świadczenia pracy, uprawnień do systemu SmartDoc dopiero po upływie od 21 do 355 dni od dnia rozwiązania umów o pracę, co naruszało postanowienia § 20 ust. 2 pkt 5 rozporządzenia KRI,
- opracowaniu polityki bezpieczeństwa informacji[8] nieodpowiadającej wymogom § 2 pkt 15 w związku § 20 ust. 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

Opis stanu faktycznego

1.1. W okresie objętym kontrolą do gromadzenia i przetwarzania danych, w tym danych osobowych, w Starostwie wykorzystywano 15 programów / systemów informatycznych, które funkcjonowały na 58 stacjach roboczych (50 komputerach i ośmiu laptopach[9]). Oględziny 30 stacji roboczych z wykorzystaniem, których gromadzono i przetwarzano dane wykazały, m.in. że: [1] w 27 dostęp do systemu zabezpieczony był w sposób odpowiedni, co szerzej opisano w pkt. 1.5. niniejszego wystąpienia, zaś na trzech – wykorzystujących system Windows XP – nie wprowadzono tego typu zabezpieczeń; [2] użytkownicy posiadali dostęp do oprogramowania niezbędnego w ich pracy; [3] dostęp do Internetu zapewniono na 26 komputerach, a pozostałe cztery nie posiadały tej funkcjonalności, co było zgodne z warunkami dostępu do systemów na nich zainstalowanych; [4] zainstalowany na 27 komputerach system operacyjny Windows 7 Pro automatycznie podlegał aktualizacji, a w przypadku pozostałych trzech komputerów z systemem Windows XP producent oprogramowania zakończył udzielanie wsparcia technicznego dla tego systemu; [5] na 27 komputerach zainstalowano program antywirusowy, który był codziennie automatycznie aktualizowany, natomiast oprogramowanie tego typu zamieszczone na trzech pozostałych komputerach (wykorzystujących system Windows XP) nie było aktualizowane od sierpnia 2017 roku; [6] na objętych oględzinami stanowiskach nie stwierdzono instalacji programów, na które Starostwo nie posiadało licencji. Zagadnienia przedstawione w pkt. 1 szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 4-8, 11)

1.2. 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". (dowód: akta kontroli str. 9-10)

1.3. Porównanie dostępu 30 pracowników do systemów informatycznych Starostwa (w tym czterech, którzy odeszli na emeryturę w 2016 roku[10]) z wystawionymi upoważnieniami oraz zadaniami przypisanymi im w zakresach obowiązków wykazało, że wszyscy mieli nadane indywidualne loginy i hasła do systemów operacyjnych, natomiast 25 pracowników nie posiadało upoważnień do przetwarzania danych osobowych w systemie Elektronicznego Zarządzania Dokumentami („EZD") SmartDoc. Osobom, które zaprzestały świadczenia pracy w 2016 roku niezwłocznie usunięto konta użytkowników z systemu EWID, do których miały dostęp. Natomiast uprawnienia do systemu SmartDoc zostały im zablokowane dopiero po upływie od 21 do 355 dni od rozwiązania umów o pracę, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Ponadto dwóch pracowników posiadało uprawnienia administratora dla systemu EWID, mimo nieokreślenia tego rodzaju zadań w zakresach ich obowiązków. Dwóm innym przypisano w zakresach obowiązków prowadzenie rejestrów / zbiorów danych osobowych, mimo nieposiadania przez nich upoważnień wymaganych przepisami prawa, a kolejni dwaj

---

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

[8] Opisane w Polityce Bezpieczeństwa Informacji (dalej: „Polityka bezpieczeństwa") oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (dalej: „Instrukcja zarządzania").

[9] Starostwo nie posiadało służbowych tabletów lub innych urządzeń mobilnych skonfigurowanych z systemem.

[10] W 2016 roku z czterema osobami rozwiązano umowy o pracę. W czasie zatrudnienia miały one dostęp do systemu EWID i SmartDoc.

przetwarzali dane w nadzorowanych przez nich zbiorach / rejestrach danych osobowych, mimo braku tego rodzaju zadań w zakresach obowiązków i bez stosownych upoważnień. Z kolei ASI, powołany zarządzeniem Nr 9 Starosty Łomżyńskiego z 15 marca 2017 r., do dnia rozpoczęcia kontroli NIK nie posiadał upoważnień do dostępu, przetwarzania lub administrowania systemami informatycznymi wykorzystywanymi w Starostwie, w tym uprawnień administracyjnych, co szerzej opisano w pkt 2.4. niniejszego wystąpienia. Nie stwierdzono przypadku użytkowania jednego konta przez więcej niż jednego użytkownika. (dowód: akta kontroli str. 5-8, 12-18, 21-24, 179, 359-362)

1.4. Dla żadnej z 30 objętych oględzinami stacji roboczych nie prowadzono rejestru dostępu do komputera. Nie gromadzono również logów aktywności użytkowników systemu co uniemożliwiało analizowanie ruchu sieciowego. Nie analizowano 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. 5-8, 11, 34-37)

1.5. W okresie objętym kontrolą Starostwo nie posiadało sieci Wi-Fi, a w związku z tym nie opracowano zasad dostępu do zbiorów danych za jej pośrednictwem.

Zgodnie z pkt. 9.1.3 Instrukcji zarządzania, wysoki poziom bezpieczeństwa przetwarzania danych osobowych stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest siecią z Internetem. Przeprowadzone w trakcie kontroli oględziny 30 stacji roboczych wykazały, że na 27 urządzeniach 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 czterech przypadkach indywidualnej karty) oraz odpowiedniej jakości hasła lub PIN-u, a system wymuszał (nie rzadziej niż co 30 dni) zmianę hasła o odpowiedniej długości i jakości. Analogiczne zabezpieczenia funkcjonowały także w sześciu z 11 lokalnych programach objętych oględzinami, służących do przetwarzania danych osobowych (Smart Doc, Subiekt, InSertGT, SIO, RWDZ i TurboEwid). W kolejnych pięciu programach (jProbit, QNT, Home Banking, Bestia oraz WebEwid) stosowano hasła o niższej złożoności oraz nie wymuszano ich zmiany co 30 dni. Informatyk Starostwa wyjaśnił, iż brak wysokiego poziomu zabezpieczeń we wskazanych systemach wynika z braku takiej funkcjonalności. Zostaną opracowane instrukcje zobowiązujące użytkowników do zmiany haseł co 30 dni.

(dowód: akta kontroli str. 9-11, 19-20,180-230)

1.6. W regulacjach wewnętrznych nie przewidziano możliwości wykorzystywania sprzętu prywatnego do realizacji zadań służbowych. Pracownicy Starostwa nie mogli używać sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków oraz nie mogli korzystać ze służbowych urządzeń informatycznych poza siedzibą jednostki. W Starostwie nie opracowano zasad bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość. Administrator Bezpieczeństwa Informacji (dalej: „ABI") wyjaśnił, że funkcjonuje powszechny ustny zakaz Starosty do korzystania ze sprzętu prywatnego w celach służbowych (dotyczący m.in. komputerów, telefonów oraz tabletów). W trakcie oględzin nie stwierdzono przypadków wykorzystywania sprzętu prywatnego do celów służbowych. (dowód: akta kontroli str. 5-10, 381)

1.7. W okresie objętym kontrolą nie występowały przypadki wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji i danych osobowych, w tym nie stwierdzono penetracji systemów informatycznych przez osoby nieuprawnione.

(dowód: akta kontroli str. 9-10)

1.8. W Starostwie nie wykonywano obowiązków służbowych z wykorzystaniem mobilnego przetwarzania danych, w tym pracy na odległość. W związku z tym nie opracowano zasad wykorzystywania urządzeń mobilnych do tych celów. (dowód: akta kontroli str. 9-10, 34-37)

1.9. W okresie objętym kontrolą Starostwo nie korzystało z naprawy komputerów przez podmioty zewnętrzne. Wszelkie naprawy lub usterki sprzętu oraz zgłoszenia nieprawidłowej pracy programów sieciowych wykonywał informatyk. W okazanych sześciu umowach dotyczących serwisu i aktualizacji programów wykorzystywanych w Starostwie do gromadzenia i przetwarzania danych osobowych zawarto zapisy zobowiązujące ich

dostawcę do zachowania tajemnicy i nieudostępnienia danych osobowych przekazywanych przez Starostwo. (dowód: akta kontroli str. 11)

1.10. W celu ochrony systemów informatycznych Starostwa na komputerach z systemem Windows 7 Pro zastosowano zabezpieczenia w postaci m.in. firewalla sprzętowego, programu antyspamowego i antywirusowego. Aplikacja zawierająca te zabezpieczenia była zarządzana centralnie, co pozwalało na kontrolę aktualności systemu zabezpieczeń. Oględziny 30 komputerów użytkowanych w Starostwie wykazały że na 27 urządzeniach zainstalowany został program antywirusowy, którego aktualizacja odbywala się automatycznie. W pozostałych trzech komputerach, wykorzystujących system Windows XP, program antywirusowy nie był aktualizowany od sierpnia 2017 roku, co szerzej opisano w pkt 1.1. niniejszego wystąpienia. (dowód: akta kontroli str. 5-10, 32-37)

1.11. Starostwo zawarło umowy na świadczenie usług poczty elektronicznej z podmiotem zewnętrznym[11]. Nie zawarto w nich jednak zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający ich ujawnienie osobie nieuprawnionej, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 25-30)

1.12. Zgodnie z zapisami w Instrukcji zarządzania, dane poszczególnych systemów powinny być kopiowane w trybie tygodniowym. W Starostwie tylko dla trzech (z ośmiu) zbiorów danych, dla których administratorem był Starosta (Administrator Danych Osobowych; dalej: „ADO"), sporządzano kopie bezpieczeństwa. Wykonywano je dla: [1] bazy danych programu finansowo-księgowego QNT (była ona zgrywana dwa razy w tygodniu na dysk przenośny), [2] danych z systemu TurboEWID, które zgrywano raz w tygodniu na dysk przenośny oraz [3] danych z systemu Smart Doc. Dla pozostałych pięciu systemów nie wykonywano wymaganych kopii bezpieczeństwa[12], co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". W okresie objętym kontrolą nie testowano wykonanych kopii zapasowych, co szerzej opisano w dalszej części wystąpienia, w sekcji „Uwagi dotyczące badanej działalności.
(dowód: akta kontroli str. 9-11, 32-38, 180-230)

1.13. Na 27 poddanych oględzinom stacjach roboczych zainstalowane było wyłącznie dopuszczone oprogramowanie służbowe, a na pozostałych trzech – oprogramowanie bez wsparcia producenta (Windows XP), co opisano w dalszej części wystąpienia, w sekcji „Uwagi dotyczące badanej działalności". Do konfigurowania systemu operacyjnego przewidziano wyłącznie administratora. Pracownicy posiadali techniczną możliwość ściągnięcia aplikacji i plików, ale bez możliwości ich zainstalowania i uruchomienia. Według informatyka Starostwa (pełniącego funkcję Administratora Systemów Informatycznych; dalej: ASI) rozwiązanie takie oszczędzało czas i było w pełni bezpieczne.
(dowód: akta kontroli str. 5-8, 11, 31-37)

1.14. Powołany w trakcie niniejszej kontroli biegły z zakresu bezpieczeństwa systemów informatycznych stwierdził, że wszystkie zbadane komputery (poza wykorzystującymi system Windows XP) posiadały aktualne wersje systemów operacyjnych i aplikacji bezpieczeństwa. Aktualizacje były wykonywane zgodnie z harmonogramem ustawionym przez administratora. Aktualna była również wersja specjalistycznego oprogramowania zainstalowanego na komputerach i na serwerze. (dowód: akta kontroli str. 34-37)

1.15. Zgodnie z obowiązującą w Starostwie polityką rachunkowości, poza tradycyjną formą (papierową) sporządzania i przesyłania przelewów stosuje się wykonywane płatności drogą elektroniczną. Nie opracowano procedury dokonywania płatności drogą elektroniczną. Zasady dokonywania płatności tą drogą regulowała umowa zawarta z bankiem. Wykonanie przelewu po zatwierdzeniu dokumentu pod względem merytorycznym i formalno-rachunkowym wymagało wprowadzenia indywidualnego kodu PIN przez wyznaczonego pracownika Wydziału Finansowego. Do wykonania transakcji konieczna była dwukrotna autoryzacja (dokonują jej dwie osoby poprzez bankowy podpis elektroniczny – Starosta, Wicestarosta lub Sekretarz i Skarbnik). Transakcje wykonywano za pośrednictwem

[11] Umowy z 31 grudnia 2013 r. i 30 czerwca 2017 r.

[12] Starostwo użytkowało 15 programów, z których dla ośmiu administratorem danych był Starosta, a dla siedmiu – podmioty zewnętrzne.

programu HomeBanking, z wykorzystaniem połączenia VPN (tzw. wydzielonego połączenia do danej transakcji). (dowód: akta kontroli str. 11)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono niżej wymienione nieprawidłowości.

1. W Starostwie dostęp do trzech[13] (z 30 objętych oględzinami) komputerów, za pomocą których przetwarzano dane osobowe oraz wykorzystujących system Windows XP nie był zabezpieczony hasłem, co naruszało przepis § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI w związku z § 6 ust. 4 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych. Ponadto, zgodnie z pkt 9.1.3. Instrukcji zarządzania, wysoki poziom bezpieczeństwa przetwarzania danych osobowych stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego służące do przetwarzania danych osobowych podłączone jest z siecią publiczną. ASI wyjaśnił, że powodem tego było niedopatrzenie, wynikające z sporadycznego użytkowania przedmiotowych stacji roboczych.
(dowód: akta kontroli str. 5-8, 31, 180-230)

2. 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. ABI wyjaśnił, że spowodowane to było brakiem czasu, wynikającym z wykonywania innych obowiązków służbowych.
(dowód: akta kontroli str. 9-10, 40-42)

3. Trzem osobom, które zaprzestały świadczenia pracy w 2016 roku odebrano uprawnienia do systemu SmartDoc dopiero po upływie od 21 do 355 dni od dnia rozwiązania umów o pracę, co naruszało postanowienia § 20 ust. 2 pkt 5 rozporządzenia KRI, zgodnie z którymi odebranie przedmiotowych uprawnień powinno być dokonane bezzwłocznie. ASI wyjaśnił, ze opóźnienia w wyłączaniu kont dla osób odchodzących z pracy wynikały z przeoczenia, spowodowanego nadmiarem obowiązków.
(dowód: akta kontroli str. 12-16, 19-20)

4. W latach 2016 – 2017 w Starostwie nie analizowano i nie zabezpieczano przed modyfikacją lub zniszczeniem logów systemów operacyjnych wykorzystywanych komputerów, 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. ASI wyjaśnił, że: *„Nie zaistniały okoliczności wskazujące na taką potrzebę. Nie dysponuję także odpowiednimi narzędziami informatycznymi do automatycznego monitorowania, zaś „ręczne" analizowanie byłoby niemożliwe z powodu dużej ilości innych obowiązków. Taki zakup stanowiłby znaczny wydatek ze strony Starostwa*".
(dowód: akta kontroli str. 5-8, 11, 31)

5. W umowach na świadczenie usług poczty elektronicznej, zawartych przez Starostwo z podmiotem zewnętrznym, nie zamieszczono zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający ujawnienie osobom nieuprawnionym, co naruszało § 20 ust. 2 pkt 9 i 10 rozporządzenia KRI. ASI wyjaśnił, że: *„Starostwo wystąpiło z wnioskiem do podmiotu, z którym zawarta jest umowa na świadczenie usług skrzynek pocztowych o aneksowanie umowy o wpisy spełniające wymogi opisane w rozporządzeniu KRI".*
(dowód: akta kontroli str. 19-20, 25-30)

6. Nie wykonywano kopii bezpieczeństwa pięciu (z ośmiu) programów wykorzystywanych do przetwarzania danych (w tym danych osobowych), które znajdowały się w Starostwie 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. Natomiast wykonane kopie trzech zbiorów danych / programów nie były dodatkowo archiwizowane na szyfrowanym optycznym nośniku danych, co naruszało wymóg zawarty w pkt 2.1.8. załącznika Nr 1 do Instrukcji

[13] Jednego w Wydziale Rolnictwa Ochrony Środowiska i Budownictwa oraz dwóch w Wydziale Geodezji, Kartografii, Katastru i Gospodarki Nieruchomościami. Wszystkie posiadały nieograniczony dostęp do Internetu.

zarządzania. ASI wyjaśnił, że: *„Niesporządzanie kopii bezpieczeństwa dla pięciu programów / zbiorów danych wykorzystywanych w Starostwie wynikało z mojego niedopatrzenia spowodowanego dużą liczbą inny obowiązków oraz braku odpowiedniego sprzętu. Natomiast brak archiwizacji wykonanych kopii na niezależnym od serwera szyfrowanym optycznym nośniku danych wynikał z braku środków na jego zakup".* (dowód: akta kontroli str. 9-10, 31,38, 180-230)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że z dniem 8 kwietnia 2014 r. producent oprogramowania zakończył udzielanie wsparcia dla systemu operacyjnego Windows XP, a zainstalowany na trzech komputerach wykorzystujących ww. system program antywirusowy nie był aktualizowany od sierpnia 2017 roku, co mogło wpłynąć na obniżenie poziomu bezpieczeństwa danych przetwarzanych na tych urządzeniach. W Starostwie nie przeprowadzano także testowania wykonanych kopii zapasowych, co może skutkować utratą danych w przypadku ich uszkodzenia. (dowód: akta kontroli str. 9-10, 38)

Ocena cząstkowa

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

2. Dokumentacja i procedury dotyczące ochrony danych osobowych

Opis stanu faktycznego

2.1. W latach 2016 – 2017 w Starostwie przetwarzano dane osobowe w 64 zbiorach danych (w tym 15 z wykorzystaniem systemów elektronicznych). Wykaz zbiorów danych osobowych (będący załącznikiem Nr 5 do Polityki bezpieczeństwa informacji), w którym powinny zostać ujęte, był nierzetelny, ponieważ wykazano w nim jedynie 52 zbiory (w tym 11 funkcjonujących z wykorzystaniem systemów informatycznych). Ponadto przedmiotowy wykaz nie spełniał wymogów § 3 pkt 1 rozporządzenia w sprawie sposobu prowadzenia przez ABI rejestru zbiorów danych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Starosta Łomżyński z dniem 2 stycznia 2017 r. powołał ABI, co szerzej opisano w pkt 2.2. niniejszego wystąpienia.

Przed powołaniem ABI obowiązkowi zgłoszenia do rejestru zbiorów danych osobowych prowadzonych przez Generalnego Inspektora Danych Osobowych (dalej: „GIODO") podlegały wszystkie 64 zbiory danych osobowych przetwarzane w Starostwie, z których zgłoszono tylko 32. Po powołaniu ABI obowiązkowi temu podlegało, na podstawie art. 40 ustawy o ochronie danych osobowych, 12 zbiorów danych, zawierających m.in. dane wrażliwe (określone w art. 43 ust. 1a ww. ustawy), z których 11 zostało zarejestrowanych w GIODO. Do dnia rozpoczęcia kontroli NIK do GIODO nie zgłoszono jednego zbioru danych, w którym gromadzono dane wrażliwe, tj.: „Rejestru Członków Społecznej Straży Rybackiej", co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Zgłoszenia zbiorów danych do rejestracji zawierały elementy wymienione w art. 41 ust 1 ustawy o ochronie danych osobowych. W okresie objętym kontrolą nie aktualizowano danych oraz nie występowano do GIODO o wykreślenie zarejestrowanego zbioru (nie nastąpiła również odmowa rejestracji).
(dowód: akta kontroli str. 39, 43-59, 69-145, 287)

2.2. Zgodnie z postanowieniami pkt 2.3. Polityki bezpieczeństwa, zarządzeniem Nr 62/2016 z 30 grudnia 2016 r., Starosta Łomżyński powołał ABI (od 2 stycznia 2017r.), który w terminie wynikającym z art. 46 b ustawy o ochronie danych osobowych został zgłoszony do GIODO[14]. Zgłoszenie zawierało komplet informacji przewidzianych w art. 46 b ust. 2 ww. ustawy. (dowód: akta kontroli str. 58-68)

2.3. ABI, zgodnie z wymogami art. 36b ustawy o ochronie danych osobowych, w latach 2016 – 2017 wywiązał się z obowiązku zapewnienia zapoznawania się pracowników przetwarzających dane z wymaganymi przepisami, co potwierdziła analiza dokumentacji 30 wybranych pracowników.

[14] Zgłoszenia dokonano 9 stycznia 2017 r. Było to pierwszy ABI zgłoszony przez Starostę Łomżyńskiego do GIODO.

Starosta (ADO) i ABI nie wywiązali się z obowiązku przeprowadzenia kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 12-18, 39)

2.4. Starostwo dysponowało ewidencją osób upoważnionych do przewarzania danych osobowych, zawierającą wszystkie elementy określone w art. 39 ust. 1 ustawy o ochronie danych osobowych. Analiza zakresów obowiązków 30 losowo wybranych pracowników merytorycznych jednostki wykazała, że 25 z nich nie nadano upoważnień do przetwarzania danych w funkcjonującym w Starostwie systemie EZD SmartDoc. Dwóm innym nie nadano zaś upoważnień do przetwarzania danych w prowadzonych przez nich zbiorach / rejestrach danych osobowych, mimo przypisania im tego rodzaju zadań w zakresach obowiązków. Kolejni dwaj pracownicy przetwarzali dane osobowe (administrowali systemem EWID) bez przypisania im tego rodzaju zadań w zakresach obowiązków oraz bez stosownych upoważnień. Natomiast informatyk Starostwa, pełniący funkcje ASI, do dnia rozpoczęcia kontroli NIK, nie posiadł upoważnienia do dostępu / przetwarzania danych osobowych w administrowanych systemach, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 6-8, 12-16, 21-24, 146-178, 366-380)

2.5. Zarządzeniem Nr 9/2017 Starosty Łomżyńskiego z 15 marca 2017 r. wprowadzono w Starostwie „Politykę bezpieczeństwa informacji" oraz „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych". Poza ww. dokumentami nie wydano wewnętrznych aktów prawnych, procedur, instrukcji dotyczących gromadzenia i przetwarzania zasobów informatycznych. W okresie objętym kontrolą nie wystąpiły zmiany organizacyjne uzasadniające potrzebę aktualizacji regulacji wewnętrznych dotyczących gromadzenia i przetwarzania przedmiotowych zasobów.
(dowód: akta kontroli str. 179-272, 287)

2.6. Regulacje wewnętrzne dotyczące bezpieczeństwa informacji powierzały informatykowi obowiązki związane z administrowaniem systemami, w których m.in. gromadzono i przetwarzano dane osobowe. Osobie tej, zarządzeniem wprowadzającym Politykę bezpieczeństwa oraz Instrukcję zarządzania, powierzono też obowiązki ASI. Do jego zadań należało m.in. sprawowanie nadzoru nad stosowaniem środków zapewniających bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych i przeciwdziałanie dostępowi osób niepowołanych do systemów, w których przetwarzano takie dane. ASI złożył oświadczenie zobowiązujące go do zachowania w tajemnicy przetwarzanych danych oraz ich zabezpieczania, jednak do dnia rozpoczęcia kontroli nie posiadał upoważnienia do dostępu / przetwarzania danych osobowych w administrowanych systemach. Ponadto nie dokonywał kwartalnej oceny bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych do czego był zobowiązany postanowieniami Instrukcji zarządzania, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 18, 180-272, 277)

2.7. W Starostwie w latach 2016 – 2017 (do 29 listopada) 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. 39)

2.8. W okresie objętym kontrolą 36 (z 74) pracowników Starostwa brało udział w szkoleniu prowadzonym przez podmiot zewnętrzny, dotyczącym zagadnień bezpieczeństwa pracy w systemach informatycznych. Starosta wyjaśniła, że w przyszłym roku planowane jest przeszkolenie pracowników z zakresu bezpieczeństwa informacji i ochrony danych osobowych, w tym związanych ze zmianą przepisów o ochronie danych osobowych, które mają wejść w życie w maju 2018 roku, w związku z implementacją rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie

swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[15]. (dowód: akta kontroli str. 278-286)

2.9. W okresie objętym kontrolą w Starostwie nie były prowadzone zewnętrzne kontrole w zakresie bezpieczeństwa danych osobowych. Nie wpłynęły także skargi związane z przypadkami ujawnienia danych osobowych. (dowód: akta kontroli str. 287)

2.10. Obowiązująca w Starostwie dokumentacja określająca sposób przetwarzania danych osobowych, środków technicznych i organizacyjnych zapewniających ochronę tych danych oraz zarządzania bezpieczeństwem informacji przyjęta została zarządzeniem Nr 9/2017 Starosty Łomżyńskiego z 15 marca 2017 r. Składały się na nią Polityka bezpieczeństwa informacji oraz Instrukcja zarządzenia systemem informatycznym służącym do przetwarzania danych osobowych. Dokumentacja ta nie była aktualizowana.

Polityka bezpieczeństwa zawierała elementy wymagane § 4 pkt 2-5 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych, a Instrukcja zarządzania spełniała wymogi określone w § 5 pkt 1-4 oraz pkt 6 i 8 ww. rozporządzenia. W przedmiotowych dokumentach nie określono natomiast odpowiednio wszystkich pomieszczeń, w których przetwarzano dane osobowe oraz okresu przechowywania kopii zapasowych i sposobu realizacji wymogów, o których mowa w § 7 ww. rozporządzenia. Przyjęte uregulowania i procedury związane z użytkowaniem systemów informatycznych służących do przetwarzania danych dotyczyły jedynie danych osobowych. Nie odnosiły się one do ochrony innych informacji będących w posiadaniu jednostki. Nie spełniały zatem wymogu określonego w § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI, co szerzej opisano poniżej, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 180-272, 277, 287)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono niżej wymienione nieprawidłowości.

1. W prowadzonym przez ABI rejestrze zbiorów danych osobowych – wbrew obowiązkowi wynikającemu z art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych w związku z § 4 pkt 2 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych – nie uwzględniono 12 zbiorów, które przetwarzano w Starostwie. ABI wyśnił, że: *„Ujęcie mniejszej ilości rejestrów wynikało z faktu zgłoszenia mi mniejszej ich ilości przez kierowników komórek organizacyjnych urzędu w trakcie opracowywania Polityki bezpieczeństwa"*. W trakcie kontroli NIK uzupełniono Rejestr zbiorów danych osobowych o brakujące zbiory. Ponadto przedmiotowy rejestr nie zawierał kompletu informacji o każdym funkcjonującym w Starostwie zbiorze danych, wymaganych § 3 pkt 1 rozporządzenia w sprawie sposobu prowadzenia przez ABI rejestru zbiorów danych. ABI wyjaśnił, że: *„Dowolną formę Rejestru Zbioru Danych przyjęto z błędnej interpretacji przedmiotowego rozporządzenia"*. (dowód: akta kontroli str. 40-57, 277, 340-354)

2. W 2016 roku, tj. przed powołaniem ABI, wbrew obowiązkowi wynikającemu z art. 40 ustawy o ochronie danych osobowych, do rejestru zbiorów danych osobowych prowadzonych przez GIODO nie zgłoszono 32 (z 64) takich zbiorów. Starosta wyjaśniła, że: *„Spowodowane to było przeoczeniem pracownika, który prowadził sprawy z zakresu ochrony danych osobowych, a następnie przeszedł na emeryturę"*. Natomiast po powołaniu ABI, na podstawie art. 43 ust. 1a ww. ustawy, obowiązkowi temu podlegało 12 zbiorów danych osobowych – wrażliwych, z których 11 zostało zarejestrowanych w GIODO. Nie zgłoszono „Rejestru członków Społecznej Straży Rybackiej". ABI wyjaśnił, że spowodowane to było przeoczeniem. W dniu 5 grudnia 2017 r. przedmiotowy rejestr został zgłoszony do rejestracji do GIODO.
(dowód: akta kontroli str. 39, 40-59, 69-145, 283-286, 287, 288-293)

3. ADO i ABI nie wywiązali się z obowiązku przeprowadzenia kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, mimo takiego wymogu zawartego w art. 36a ust. 1lit a i ust. 2 w związku z art. 36b ustawy o ochronie danych osobowych oraz pomimo zatwierdzenia przez Starostę Planu sprawdzeń danych osobowych na 2017 rok. Starosta wyjaśniła, że nieprzeprowadzenie

[15] Dz.U.UE.L.2016.119.1.

w 2016 roku kontroli zgodności przetwarzania danych osobowych z przepisami prawa wynikało z braku czasu i nadmiaru obowiązków pracownika, który zajmował się w tym okresie ochroną informacji. Podobnej treści wyjaśnienia złożył ABI.

(dowód: akta kontroli str. 39-42, 283-286, 294-298)

4. Dla 25 pracowników Starostwa (z 30 objętych badaniem) nie nadano upoważnień, mimo umożliwienia im przetwarzania danych w zbiorze danych osobowych EZD SmartDoc. Dodatkowo dwóch z nich prowadziło bez upoważnienia zbiory danych osobowych (rejestry wniosków o pozwolenie na budowę oraz decyzji o pozwoleniu na budowę). Kolejni dwaj pracownicy przetwarzali dane w zbiorach danych osobowych bez przypisania im tego rodzaju zadań w zakresach obowiązków i bez stosownych upoważnień. Dwóch innych pracowników również bez upoważnień administrowało systemem EWID, co także nie miało odzwierciedlenia w zakresach ich czynności. Natomiast informatyk Starostwa, pełniący funkcję ASI, do dnia rozpoczęcia kontroli nie posiadł upoważnienia do dostępu / przetwarzania danych osobowych w administrowanych systemach. Takie postępowanie stanowiło naruszenie art. 37 ustawy o ochronie danych osobowych. Starosta wyjaśniła, że nienadanie przedmiotowych upoważnień i odpowiednich zapisów w zakresach obowiązków ww. osób wynikało z przeoczenia. W trakcie kontroli wszyscy wymienieni pracownicy uzyskali stosowne upoważnienia ADO.

(dowód: akta kontroli str. 12-16, 23-24, 146-178, 283-286, 359-362, 366-380)

5. ASI nie dokonywał kwartalnej oceny bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych, mimo takiego wymogu zawartego w pkt 7 rozdziału VIII Instrukcji zarządzania systemem informatycznym. Wyjaśnił, że spowodowane to było wykonywaniem innych obowiązków służbowych.

(dowód: akta kontroli str. 19-20, 180-230, 277)

6. W Starostwie w latach 2016 – 2017 nie przeprowadzano audytów wewnętrznych z zakresu bezpieczeństwa informacji, mimo obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI. W konsekwencji Starostwo nie dysponowało rzetelną oceną skuteczności przyjętych rozwiązań w zakresie ochrony danych osobowych. Starosta wyjaśniła, że: „*Spowodowane to było nadmiarem obowiązków pracownika oraz brakiem czasu. Pracownik, który zajmował się ochroną informacji w urzędzie pracował w ograniczonym wymiarze pracy, a następnie odszedł na emeryturę*".

(dowód: akta kontroli str. 39, 283-286)

7. Obowiązująca w Starostwie Polityka bezpieczeństwa nie określała wszystkich pomieszczeń, w których przetwarzano dane osobowe. Nie wymieniono w niej miejsca przechowywania wykonanych kopii danych dla systemu EWID, co naruszało § 4 pkt 1 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych. Natomiast w Instrukcji zarządzania nie określono okresu przechowywania wykonanych kopii zapasowych zbiorów danych oraz sposobu realizacji wymogów, o których mowa w § 7 ww. rozporządzenia, czym naruszono § 5 pkt 5 lit. b powyższego rozporządzenia. Starosta wyjaśniła, że brak wymaganych informacji w Polityce bezpieczeństwa wynikał z błędnego założenia, że czynność przechowywania nie jest miejscem przewarzania danych, a nieokreślenie czasu przechowywania kopii zapasowych i sposobu realizacji wymogów zawartych w § 5 pkt 7 przedmiotowego rozporządzenia spowodowane było przeoczeniem. W trakcie kontroli opracowano rozwiązania wymagane § 5 pkt 7 ww. rozporządzenia. (dowód: akta kontroli str. 180-272, 277, 283-286, 340-354)

8. Przyjęte w Starostwie uregulowania i procedury składające się na politykę bezpieczeństwa informacji dotyczyły jedynie ochrony danych osobowych. Nie odnosiły się one do innych danych będących w posiadaniu jednostki. W konsekwencji nie spełniono wymogu określonego w § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI. ABI wyjaśnił, że spowodowane to było omyłkowym pominięciem tego zagadnienia w trakcie opracowywania Polityki bezpieczeństwa informacji.

(dowód: akta kontroli str. 180-272, 283-287)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie opracowanie i wdrożenie w Starostwie, dokumentacji oraz procedur wymaganych przepisami ustawy o ochronie danych osobowych.

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. W Polityce bezpieczeństwa określono zabezpieczenia techniczne pomieszczeń, w których przetwarzano dane osobowe. Były to: system alarmowy, całodobowy monitoring, kontrola dostępu, przechowywanie papierowych zbiorów danych w zamykanych szafach lub szafie pancernej. Przyjęto politykę kluczy, w której m.in. określono godziny przebywania pracowników w budynku oraz wyznaczono miejsce przetrzymywania kluczy do poszczególnych pokoi (zabezpieczona skrzynka). Oględziny 20 pomieszczeń Starostwa, w tym dwóch serwerowni i archiwum wykazały, że przetwarzanie danych osobowych odbywało się w pomieszczeniach wskazanych w Polityce bezpieczeństwa, z wyjątkiem miejsca przechowywania kopii zbioru danych dla systemu EWID. Wejścia do budynku Starostwa oraz jego parter objęte były monitoringiem wizyjnym. Pomiędzy godziną 20^{00} a 7^{00} włączany był system alarmowy. W 10 z 20 objętych oględzinami pomieszczeń zainstalowano wzmocnione drzwi, w tym w jednej z serwerowni, w archiwum oraz w ośmiu pomieszczeniach, w których przetwarzane były dane zawarte w zbiorach „Ewidencja pojazdów", „Ewidencja kierowców", „Ewidencja gruntów i budynków". W pomieszczeniach obu serwerowni oraz w czterech pomieszczeniach, w których przetwarzane były dane zawarte w ww. zbiorach zamontowano klimatyzację. Na parterze budynku, we wszystkich pomieszczeniach objętych oględzinami, szyby w oknach były wzmocnione folią antywłamaniową. W archiwum (pomieszczenie w piwnicy) zainstalowano kraty w oknach oraz zaopatrzono je w rozwiązania zapobiegające zalaniu akt[16]. Tylko w jednej z dwóch serwerowni zainstalowano system ostrzegający o pożarze. W kolejnej serwerowni i w archiwum nie zainstalowano czujników dymu i temperatury, przez co nie zapewniono danym tam przechowywanym właściwej ochrony przed działaniem czynników fizycznych i zdarzeń losowych takich, jak pożar czy zalanie. Zagadnienie to opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

Nie dokonano oględzin pomieszczenia przechowywania akt poszczególnych pojazdów, ponieważ miejsce ich przetrzymywania zlokalizowano w pokoju, w którym umiejscowiono szafę krosową i serwer CEPIK, co szerzej opisano w dalszej części wystąpienia, w sekcji „Uwagi dotyczące badanej działalności".

Budynek Starostwa wyposażono w system przeciwpożarowy – system hydrantów oraz czujki dymu na korytarzach. W ramach systemu antywłamaniowego zainstalowano czujniki ruchu. Na korytarzach znajdowały się gaśnice. Serwerownie posiadały zabezpieczenia na wypadek nagłej utraty zasilania w postaci urządzeń UPS.

(dowód: akta kontroli str. 180-230, 299-309, 363)

3.2. ASI 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, licencje itp.).

(dowód: akta kontroli str. 5-8)

3.3. W okresie objętym kontrolą zlikwidowano dwa komputery, a także inny sprzęt biurowy (m.in. monitory, drukarki i kserokopiarki) poprzez ich przekazanie firmie utylizacyjnej. ASI wyjaśnił, iż dane z likwidowanego sprzętu zostały zabezpieczone poprzez usunięcie dysków i złożenie ich w szafie pancernej, w pokoju ABI. (dowód: akta kontroli str. 31, 311-313)

3.4. Do niszczenia bieżących wydruków oraz dokumentów niewymagających archiwizacji wykorzystywano 15 niszczarek (w poszczególnych wydziałach znajdowało się od dwóch do trzech), jednak nie opracowano w tym zakresie wytycznych lub procedur. Według ABI, Starostwo nie zleciło zewnętrznemu podmiotowi wykonywania usług niszczenia dokumentów, uznając to za zbyteczne z uwagi na posiadanie znacznej ilości własnych niszczarek. (dowód: akta kontroli str. 9-10, 314)

[16] W pomieszczeniach obu serwerowni nie przewidziano żadnych rozwiązań zapobiegających zalaniu.

3.5. ABI wyjaśnił, że pracownicy Starostwa nie mogą używać sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych oraz nie mogą korzystać ze służbowych urządzeń informatycznych poza siedzibą jednostki. W Starostwie nie opracowano zasad bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość. ABI wyjaśnił, że funkcjonuje ustny zakaz Starosty do korzystania ze sprzętu prywatnego w celach służbowych – dotyczyło to m.in. komputerów, telefonów czy tabletów.
(dowód: akta kontroli str. 9-10, 381)

3.6. Sprzątaniem pomieszczeń zajmowało się pięć sprzątaczek – pracowników Starostwa. Pomieszczenia sprzątane były od godziny 13^{00} do 20^{00}. Obie serwerownie sprzątał ASI. Pracowników sprzątających zobowiązano do zachowania w tajemnicy danych osobowych, jednak żadna z ww. osób do dnia rozpoczęcia kontroli nie posiadała zgody na przebywanie w obszarze przetwarzania danych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

W Starostwie nie opracowano zasad zabezpieczania dokumentów przed dostępem osób nieupoważnionych, jednak w trakcie oględzin stwierdzono, że pomieszczenia, w których przetwarzano dane osobowe, podczas nieobecności pracowników były zamykane na klucz. Ponadto ABI wyjaśnił, że: *„(...) w Starostwie (...) od wielu lat funkcjonuje przestrzegana przez pracowników zasada, że z chwilą zakończenia realizacji czynności, miejsce pracy jest uprzątane, a wszystkie dokumenty chowane są do zamykanych szaf. Czynnościami tymi pracownicy spełniają zasadę tzw. „czystego biurka".*
(dowód: akta kontroli str. 38, 277, 299-309, 315)

3.7. Zgodnie z rozdziałem VIII Instrukcji zarządzania, za przeglądy oraz konserwacje sprzętu i oprogramowania informatycznego odpowiadał ASI. Powinny one być wykonywane w wypadku wystąpienia takiej potrzeby. W okresie objętym kontrolą nie wykonywano przeglądów i konserwacji systemu informatycznego oraz nośników informacji służących do przetwarzania danych. Wszelkie naprawy lub usterki sprzętu oraz zgłoszenia nieprawidłowej pracy programów sieciowych wykonywał ASI. Nie korzystano też z napraw świadczonych przez firmy zewnętrzne. (dowód: akta kontroli str. 9-11, 180-230)

3.8. Starostwo wyposażyło oba serwery w urządzenia UPS, a przeprowadzone w trakcie kontroli oględziny wykazały, że 18 komputerów posiadało zasilanie awaryjne UPS lub baterie podtrzymujące zasilanie. Nie opracowało 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". Starostwo posiadało agregat prądotwórczy z autostartem o mocy 110 kW, przy dobowym zapotrzebowaniu na energię elektryczną w wysokości 70 kW[17]. Dysponowano więc skutecznymi i automatycznie włączającymi się zabezpieczeniami przed utratą zasilania kluczowych systemów teleinformatycznych. (dowód: akta kontroli str. 9-10, 38, 299-306)

3.9. W okresie objętym kontrolą nie stwierdzono w Starostwie przypadków fizycznej utraty danych i konieczności ich odtwarzania ze sporządzonych kopii bezpieczeństwa.
(dowód: akta kontroli str. 38)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowości wymienione poniżej.

1. Pomieszczenia archiwum i jednej serwerowni nie posiadały czujników ostrzegających o pożarze, a w obu serwerowniach nie zastosowano rozwiązań zapobiegających zalaniu zainstalowanego tam sprzętu. Taka sytuacja nie zapewniała właściwej ochrony zbiorów danych przed działaniem czynników fizycznych i zdarzeń losowych, jak pożar lub zalanie. Stanowiło to naruszenie art. 36 ust. 1 ustawy o ochronie danych osobowych, stosownie do którego ADO powinien zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane m. in. przed ich uszkodzeniem lub zniszczeniem. Stosownie zaś do § 6 załącznika nr 6

[17] Średnia z ostatnich trzech miesięcy 2017 roku.

do rozporządzenia w sprawie działania archiwów zakładowych[18], pomieszczenie archiwum powinno posiadać system do wykrywania ognia i dymu (przeciwpożarowy). Starostwa wyjaśniła, że: *„(...) cała instalacja przeciwpożarowa w obecnej chwili wymaga gruntownego remontu. W związku z ograniczonymi środkami finansowymi nie było możliwe do chwili obecnej zrealizowanie tego przedsięwzięcia. W roku 2018 planowana jest termomodernizacja budynku i w związku z tym możliwe będzie doposażenie budynku w czujniki przeciwpożarowe"*. (dowód: akta kontroli str. 299-309, 316-317)

2. Osoby sprzątające pomieszczenia Starostwa do dnia rozpoczęcia kontroli nie posiadały zgody do przebywania w obszarze przetwarzania danych, w tym osobowych, wymaganego pkt I załącznika do rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych. ABI wyjaśnił, że: *„Pracownicy techniczni, sprzątaczki i konserwatorzy zostali zapoznani z przepisami prawa dotyczącymi bezpieczeństwa informacji, potwierdzili ten fakt własnoręcznie podpisując odpowiednie oświadczenie. Błędnie przyjęto, że oświadczenie to spełnia wymogi określone w pkt I rozporządzenia (...) w sprawie dokumentacji przetwarzania danych osobowych (...). Omyłkę sprostowano, poprzez upoważnienie przez ADO każdej z tych osób do dostępu i przebywania w strefie przetwarzania informacji, w tym danych osobowych. Upoważnienia uzupełniono 13 grudnia 2017 r."*

(dowód: akta kontroli str. 40-42, 277, 299-309, 318)

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 Starostwa. Ponadto w trakcie oględzin stwierdzono, że pomieszczenie, w którym przechowywano akta poszczególnych pojazdów zlokalizowano w pokoju, w którym umiejscowiono szafę krosową i serwer CEPIK. Natomiast zgodnie z załącznikiem Nr 5[19] do umowy dostawy Nr 167/178 z 1 czerwca 2017 r.: *„Pomieszczenia, w których znajduje się szafa krosowa i serwer powinny być pomieszczeniami dedykowanymi, w których zapewniona będzie temperatura w przedziale 16 – 23 °C"*. Starosta wyjaśniła, że: *„(...) od 1999 do 2004 roku urząd Starosty Powiatowego znajdował się w Łomży przy ulicy Nowa 2. Od 2004 roku urząd Starostwa Powiatowego ma siedzibę w budynku przy ulicy Szosa Zambrowska 1/27. W związku z powyższym zaistniała konieczność przeniesienia szafy krosowej i serwera CEPiK do pomieszczenia na parterze budynku. Przeniesienie odbyło się za zgoda PWPW[20], które nigdy nie kwestionowało miejsca umieszczenia tych urządzeń. Mając powyższe na uwadze sądziłam, że zostały spełnione warunki umowy. W 2018 roku przewidywany jest remont pomieszczeń na parterze budynku i zostanie wygospodarowane pomieszczenie na serwerownię CEPiK"*.

(dowód: akta kontroli str. 299-309, 319-328)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości działania Starostwa dotyczące przestrzegania przyjętych procedur przechowywania i zabezpieczania danych w Urzędzie oraz zapewnienia właściwej ich ochrony.

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności kontrolowanej jednostki

Opis stanu faktycznego

4.1. W okresie objętym kontrolą w Starostwie przetwarzano dane osobowe w 64 zbiorach danych (w tym 15 z wykorzystaniem systemów elektronicznych). W wykazie zbiorów danych, będących załącznikiem do Polityki bezpieczeństwa ujęto 52 z 64 prowadzonych zbiorów, co szerzej opisano w pkt 2 niniejszego wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 39, 43-57)

---

[18] Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych. (Dz. U. Nr 14, poz. 67 ze zm.).

[19] Wymagania Techniczno-Organizacyjne dla Zamawiającego.

[20] Państwowa Wytwórnia Papierów Wartościowych.

4.2. W okresie objętym kontrolą nie dokonywano aktualizacji zbiorów danych zgłoszonych przez Starostwo do rejestracji do GIODO, mimo zaistnienia w jednym przypadku (z 12 objętych analizą) okoliczności, które powodowały konieczność takiej aktualizacji, co szerzej opisano w dalszej części niniejszego wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 287, 330-331)

4.3. Analiza danych przetwarzanych w 12 zbiorach wykazała, że gromadzone dane w 10 z nich były niezbędne do realizacji zadań, dla których je prowadzono. W dwóch kolejnych przetwarzano dane osobowe w zakresie szerszym niż wynikałoby to ze zgłoszeń do rejestru GIODO lub przepisów prawa, co zostało opisane w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Zgodnie z regulaminem naboru na wolne stanowiska urzędnicze w Starostwie[21], warunkiem udziału w naborze było wyrażenie zgody przez kandydata na przetwarzanie danych osobowych zawartych w ofercie, niezbędnych do realizacji procesu rekrutacji. W latach 2016 – 2017 w jedenastu ogłoszeniach o naborze wskazano informacje wymagane art. 24 ust. 1 ustawy o ochronie danych osobowych. (dowód: akta kontroli str. 330-339)

4.4. Starosta był administratorem zbiorów danych, do których dostęp posiadali pracownicy, z wyjątkiem m.in. elektronicznej wersji zbiorów „Pojazd" i „Kierowca" (CEPiK).

Dostęp do danych elektronicznej wersji zborów „Pojazd" i „Kierowca" (prowadzonych za pomocą systemu CEPiK) Starosta posiadał na podstawie umowy z PWPW zawartej 1 czerwca 2017 r. Zgodnie z postanowieniami tej umowy, warunkami dostępu do tych danych było m.in. wykorzystywanie dedykowanej sieci teleinformatycznej, obostrzonych środków uwierzytelniania oraz posiadanie uprawnień nadawanych przez PWPW. Z oględzin czterech stanowisk komputerowych, na których przetwarzane były dane w elektronicznym zbiorze „Pojazd" i „Kierowca" wynika, że komputery wykorzystywane do przetwarzania danych nie posiadały podłączenia do ogólnodostępnego Internetu, pracownicy posiadali aktualne uprawnienia do użytkowania systemu, korzystanie z komputera i systemu wymagało spełnienia obostrzonych środków uwierzytelniających, a komputery wykorzystywane do przetwarzania danych posiadały aktualny program antywirusowy i były podłączone do UPS. (dowód: akta kontroli str. 5-8, 321-329)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowości, polegające na gromadzeniu i przetwarzaniu w dwóch zbiorach danych osobowych, które nie były wykorzystywane przy realizacji zadań, w związku z którymi je prowadzono.

- W Wydziale Rolnictwa, Ochrony Środowiska i Budownictwa w formie papierowej prowadzono Rejestr Kart Wędkarskich. Analiza 10 z 282 zaewidencjonowanych spraw wykazała, że we wszystkich przypadkach w aktach gromadzono zakres danych szerszy niż głoszony do GIODO o serię i numer dowodu osobistego. Niezgłoszenie do GIODO pełnego zakresu przetwarzanych danych naruszało art. 41 ust. 1 pkt 3a ustawy o ochronie danych osobowych, zgodnie z którym zgłoszenie powinno zawierać m.in. zakres przetwarzanych danych. Ponadto w celu identyfikacji osób / petentów wystarczające było przetwarzanie imienia i nazwiska, daty urodzenia oraz adresu zamieszkania, tj. danych wykazanych w zgłoszeniu do GIODO.
- W Wydziale Promocji, Rozwoju i Komunikacji w formie papierowej prowadzono Rejestr klubów sportowych. Analiza dokonanych wpisów i akt spraw 10 (z 41 klubów sportowych) wykazała, że w sześciu przypadkach prowadzona ewidencja zawierała imiona i nazwiska oraz daty urodzin członków zarządu i organu kontroli wewnętrznej, a w pozostałych czterech dodatkowo nr Pesel i adresy zamieszkania ww. osób. Przepisy § 5 rozporządzenia Ministra Sportu i Turystyki z 18 października 2011 r. w sprawie ewidencji klubów sportowych[22] nie przewidują gromadzenia i zamieszczania w ww. ewidencji nr Pesel wraz z adresami zamieszkania ww. osób.

  Gromadzenie danych osobowych niewykorzystywanych do realizacji zadań narusza przepis art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, zgodnie z którym

[21] Zarządzenie Starosty Łomżyńskiego Nr 29/09 z 18 czerwca 2009 r. w sprawie wprowadzenia Regulaminu naboru na wolne stanowiska urzędnicze w Starostwie Powiatowym w Łomży.

[22] Dz. U. Nr 243 poz.1449.

przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest to niezbędne dla zrealizowania obowiązku wynikającego z przepisu prawa. Naczelnik Wydziału Rolnictwa, Ochrony Środowiska i Budownictwa wyjaśnił, że: „(...) *dla prawidłowego wydawania kart wędkarskich wystarczające są dane zgłoszone do GIODO. Dlatego też już zwrócono uwagę pracownikowi, aby nie przetwarzał danych dotyczących serii i numeru dowodu osobistego osób ubiegających się o karty wędkarskie".* Natomiast Naczelnik Wydziału Promocji, Rozwoju i Komunikacji wyjaśniała: „(...) *Niektóre składane przez kluby dokumenty, będące podstawą wpisów do ewidencji zawierały dodatkowo numer PESEL. W ewidencji niejako automatycznie, omyłkowo przenosząc dane, zamieszczono w kilku przypadkach PESEL osób z Komitetu Założycielskiego, które weszły potem w skład Zarządu (...). Nadmieniam, iż od chwili założenia Ewidencji Klubów, mimo iż istnieje taka możliwość, nikt z klientów Starostwa nie korzystał z wglądu do ww. Ewidencji. Po przeprowadzonej kontroli zbędne dane (PESEL) zostały z ewidencji usunięte".* (dowód: akta kontroli str. 330-331, 355-358, 382-383)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości sposób przetwarzania zasobów informacyjnych, który był zgodny z zakresem działalności Starostwa.

IV. Wnioski

Wnioski pokontrolne

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

1. Zabezpieczenie odpowiedniej jakości hasłami dostępu do wszystkich komputerów wykorzystanych do przetwarzania danych osobowych.
2. Wywiązywanie się z obowiązków określonych w § 20 ust. 2 pkt 3 oraz pkt 7 lit. a rozporządzenia KRI.
3. Niezwłoczne obieranie pracownikom, z którymi rozwiązano stosunek pracy, uprawnień do wszystkich systemów informatycznych, do których mieli dostęp.
4. Zawarcie w umowach na świadczenie usług poczty elektronicznej zapisów gwarantujących odpowiedni poziom bezpieczeństw informacji oraz ich zabezpieczenia w sposób uniemożliwiający ujawnienie osobom nieuprawnionym.
5. Dostosowanie „Rejestru zbiorów danych osobowych" do wymogów zawartych w § 3 pkt 1 rozporządzenia w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbioru danych.
6. Przeprowadzanie, w ramach obowiązku wynikającego z art. 36a ust. 2 w związku z art. 36b ustawy o ochronie danych osobowych, okresowych kontroli przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
7. Dokonywanie przez ASI kwartalnych ocen bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych.
8. Przeprowadzanie corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 14 rozporządzenia KRI.
9. Opracowanie i wdrożenie Polityki bezpieczeństwa informacji, stosownie do wymogów wynikających z § 2 pkt 15 w związku z § 20 ust. 1 i ust. 2 rozporządzenia KRI.
10. Zaktualizowanie wykazu budynków lub pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.
11. Zapewnienie danym osobowym przechowywanym w archiwum i serwerowniach właściwej ochrony przed działaniem czynników fizycznych i zdarzeń losowych.

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

12. Wykonywanie kopii bezpieczeństwa danych dla wszystkich programów / systemów przetwarzających dane, których administratorem jest Starosta i ich archiwizowanie zgodnie z zasadami przyjętymi w Instrukcji zarządzania.
13. Przetwarzanie w zbiorach wyłącznie danych niezbędnych do realizacji obowiązków wynikających z przepisów prawa.

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 22 stycznia 2018 r.

Kontrolerzy:

Piotr Jurkin
starszy inspektor kontroli państwowej

podpis

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

podpis