NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.07.2017
P/17/062

00396118

WYSTĄPIENIE POKONTROLNE

Wystąpienie pokontrolne z dnia 19 stycznia 2018 r., zmienione zgodnie z treścią uchwały Zespołu Orzekającego Komisji Rozstrzygającej w Najwyższej Izbie Kontroli z dnia 23 marca 2018 r. (KPK-KPO.443.041.2018)

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	Marcin Bielawski – specjalista kontroli państwowej, upoważnienie do kontroli nr LBI/158/2017 z 17 listopada 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Starostowo Powiatowe w Białystoku, ul Borsucza 2, 15-569 Białystok (dalej: „Starostwo" lub „Urząd")
Kierownik jednostki kontrolowanej	Antoni Pełkowski – Starosta Powiatu Białostockiego[1] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

Najwyższa Izba Kontroli ocenia negatywnie zapewnienie przez Starostwo właściwej ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem[3].

Uzasadnienie oceny ogólnej

Stwierdzono bowiem nieprawidłowości polegające w szczególności na:

- nadaniu użytkownikom 13 ze 175 komputerów Starostwa uprawnień administratora systemu operacyjnego,
- przyznaniu jednemu pracownikowi uprawnień do przetwarzania danych osobowych w systemie informatycznym, mimo braku stosownego upoważnienia Administratora Danych Osobowych[4] oraz nieodebraniu uprawnień do przetwarzania danych osobowych w systemie informatycznym dwóm z 22 byłych pracowników,
- niewykorzystywaniu posiadanych narzędzi do automatycznego gromadzenia, zabezpieczenia i analizy logów dostępu do informacji,
- umożliwieniu zdalnego dostępu do zasobów firmie serwisującej składniki systemu bez konieczności autoryzacji i bez nadzoru administratora systemu,
- niewłaściwym zabezpieczeniu przed uszkodzeniem lub zniszczeniem nośników zawierających kopię baz danych sześciu programów,
- niezgłoszeniu do zarejestrowania Generalnemu Inspektorowi Ochrony Danych Osobowych[5] jednego z 56 prowadzonych zbiorów danych osobowych, w którym przetwarzane były dane osobowe wrażliwe, a w odniesieniu do trzech – niezaktualizowanie zgłoszenia,
- przetwarzaniu danych osobowych przez pięciu pracowników nieposiadających upoważnienia nadanego przez ADO do przetwarzania takich danych,
- braku właściwej ochrony zbiorów danych osobowych znajdujących się w archiwum oraz serwerowi.

---

[1] Pan Antoni Pełkowski funkcję Starosty pełni od dnia 11 grudnia 2014 r.
[2] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
[3] Kontrolą objęty został okres od 1 stycznia 2016 r. do zakończenia czynności kontrolnych.
[4] Administratorem Danych Osobowych był Starosta (dalej „ADO").
[5] Dalej: „GIODO".

III. Opis ustalonego stanu faktycznego

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

Opis stanu faktycznego

1.1. W Starostwie do gromadzenia i przetwarzania danych osobowych wykorzystywano 15 systemów informatycznych. Służyły one do: elektronicznego zarządzania dokumentami (EZD), prowadzenia elektronicznego rejestru przedsiębiorców prowadzących ośrodki szkolenia kierowców i innych upoważnionych podmiotów prowadzących szkolenia (Portal Starosty), przetwarzania danych kadrowych i płacowych (Płace; Płatnik), realizacji przelewów drogą elektroniczną (i-PKO), prowadzenia ewidencji księgowej Urzędu (Foka), rejestracji danych w ramach System Informacji Oświatowej (SIO), prowadzenia rejestru stowarzyszeń (RESTO), realizacji płatności w ramach projektu finansowanego ze środków UE (SL-2014), kierowania uczniów do szkół specjalnych lub ośrodków poza granicami powiatu (ORE), publikacji informacji publicznych (Biuletyn Informacji Publicznej[6]), ewidencji użytkowania wieczystego (UW4), ewidencji gruntów i budynków (EWOPIS), ewidencji wniosków, decyzji i zgłoszeń (RWDZ) oraz ewidencji pojazdów i kierowców (CEPiK). Z oględzin 30 komputerów wynika, że 28 z nich było podłączonych do ogólnodostępnego Internetu. Natomiast dwa stanowiska, na których gromadzono i przetwarzano dane osobowe za pomocą systemu CEPiK, zgodnie z umową określającą warunki korzystania z systemu, nie miały takiego połączenia. (dowód: akta kontroli str. 72-79, 417-424)

1.2. W latach 2016 – 2017 (do 18 grudnia) w Urzędzie nie wywiązywano się z obowiązku przeprowadzania (raz w roku oraz po każdym zgłoszonym incydencie bezpieczeństwa) analizy utraty integralności, dostępności lub poufności informacji, do czego zobowiązywał pkt IX.1 Systemu zarządzania bezpieczeństwem informacji[7] (zagadnienie to zostało opisane w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości"). Jednak w okresie tym, realizując obowiązek, o którym mowa w § 20 ust. 2 pkt 3 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], Administrator Bezpieczeństwa Informacji[9] przeprowadził analizę zagrożeń występujących w systemach informatycznych Starostwa. Wyniki tych działań zostały opisane w dokumencie *„Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych w Starostwie Powiatowym w Białystoku"*[10]. W jej wyniku wyróżniono dwa największe zagrożenia, tj.: nieuprawniony dostęp oraz kradzież (włamanie do systemu) oraz trzy inne zagrożenia (awaria sprzętu, atak wirusa, pożar obiektu). W związku z tym wskazano, że w celu zmniejszenia ww. zagrożeń należy zwrócić uwagę m.in. na:

- przetwarzanie danych osobowych tylko przez osoby upoważnione,
- zabezpieczenie obiektu i systemu informatycznego w zakresie ochrony antywłamaniowej oraz przestrzeganie ustalonych zasad w tym zakresie,
- przestrzeganie instrukcji obsługi sprzętu i zasad posługiwania się nim,
- stosowanie nowoczesnych zabezpieczeń antywłamaniowych.

---

[6] Dalej: „BIP".
[7] Zarządzenie Starosty Nr 42/2015 z 16 października 2015 r.; dalej „SZBI".
[8] Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej: „rozporządzeniem KRI".
[9] Dalej: „ABI".
[10] Data włączenia dokumentu do obowiązującej w Urzędzie dokumentacji określającej sposób przetwarzania danych osobowych, środków technicznych i organizacyjnych zapewniających ochronę tych danych: 7 grudzień 2016 r.

Ponadto określono dodatkowe działania mające skutecznie wyeliminować ww. zagrożenia:

- przestrzeganie zasad korzystania ze sprzętu informatycznego, określonych w Polityce bezpieczeństwa i instrukcjach zarządzania systemami informatycznymi[11], ze zwróceniem szczególnej uwagi na dostęp osób postronnych,
- rygorystyczne przestrzeganie przepisów dotyczących ochrony danych osobowych,
- przestrzeganie zasad posługiwania się sprzętem komputerowym (kopiowanie, przesyłanie, udostępnianie),
- stosowanie procedur określonych w Polityce bezpieczeństwa i instrukcjach zarządzania systemami informatycznymi, dotyczących korzystania z systemów informatycznych, w którym przetwarzane są dane osobowe.

Ustalenia niniejszej kontroli wykazały, że w Starostwie nie zrealizowano części działań naprawczych, co szerzej zostało opisane w dalszej części wystąpienia pokontrolnego.
(dowód: akta kontroli str. 51-61)

1.3. Uprawnienia administratorów sieci w Starostwie posiadał Administrator Systemu Informatycznego Starostwa[12], ABI oraz osoba zatrudniona na stanowisku informatyka – stosownie do wykonywanych zadań określonych w zakresach obowiązków. Poza administratorami sieci, uprawnienia administratorów lokalnych posiadało 13 użytkowników komputerów, na których zainstalowane były aplikacje do fakturowania i zarządzania środkami trwałymi. Zagadnienie nadawania uprawnień administratorów lokalnych użytkownikom komputerów, zostało opisane w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 80-126)

Analiza procesu nadawania i zmiany uprawnień 30 pracownikom, którzy przetwarzali dane osobowe w systemach informatycznych Starostwa wykazała[13], że w okresie objętym kontrolą w 27 przypadkach uprawnienia te nadano stosownie do posiadanych upoważnień oraz zmieniano lub odbierano w przypadkach rozwiązania stosunku pracy albo zmiany stanowiska. W dwóch przypadkach, mimo rozwiązania stosunku pracy, pracownikom nie odebrano uprawnień do systemu EZD. Natomiast w jednym przypadku pracownikowi nadano uprawnienia do przetwarzania danych w programie CEPiK w zbiorze danych „Ewidencja kierowców", mimo braku upoważnienia ADO do ich przetwarzania. Kwestie te zostały opisane szerzej w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 127-145)

Oględziny 30 komputerów wykazały, że na wszystkich komputerach wydzielono dwa konta (administratora i użytkownika), użytkownik nie posiadał uprawnień administratora systemu operacyjnego poza opisanymi wyżej 13 przypadkami. Wszystkie systemy operacyjne oraz programy – zainstalowane na komputerach objętych oględzinami – służące do przetwarzania danych osobowych posiadały zabezpieczenia, których stopień złożoności oraz wymuszona częstotliwość aktualizacji, spełniały wymogi 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 systemy informatyczne do przetwarzania danych osobowych[14], a także obowiązujących w Starostwie instrukcji zarządzania systemami informatycznymi.
(dowód: akta kontroli str. 6-71, 75-79)

---

[11] 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 41/2015 Starosty Powiatu Białostockiego z dnia 8 października 2015 r. Składały się na nią m.in.: Polityka bezpieczeństwa danych osobowych administrowanych przez Starostę Powiatu Białostockiego (dalej: „Polityka bezpieczeństwa"), Instrukcja zarządzania lokalnymi systemami informatycznymi „Pojazd i Kierowca" służącymi do przetwarzania danych w Starostwie Powiatowym w Białymstoku (dalej: „Instrukcji zarządzania systemem Pojazd i Kierowca"), Instrukcja zarządzania systemem informatycznym „EWOPIS" z wykorzystaniem modułu przeglądarki danych online „Geoportal" służącym do przetwarzania danych (dalej: „Instrukcja zarządzania systemem EWOPIS"), Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych innymi niż „EWOPIS" oraz „Pojazd i Kierowca" (dalej: „Instrukcja zarządzania innymi systemami").

[12] Zwany dalej „ASIS".

[13] Badaniem objęto wszystkich 22 pracowników, z którymi od 1 stycznia 2016 r. do 28 października 2017 r. rozwiązano stosunek pracy, wszystkich sześciu pracowników, którym w tym okresie zostało zmienione stanowisko oraz dwóch losowo wybranych.

[14] Dz. U. Nr 100, poz. 1024 Rozporządzenie zwane dalej „rozporządzeniem w sprawie dokumentacji oraz warunków technicznych".

1.4. Ustalenia biegłego (powołanego przez NIK) wskazują, że w Starostwie nie był prowadzony zbiorczy rejestr dostępu do systemu w formie elektronicznej. Informacje o logach gromadzone były przez kontroler domeny i w każdej z końcówek klienckich (zapisuje ona logi związane ze swoją pracą). Tryb zarządzania logami (ich zawartość i czas przechowywania) był zgodny z ustawieniami domyślnymi przewidzianymi przez producentów urządzeń czy aplikacji. Informacje zawarte w logach nie były przetwarzane automatycznie przez administratora sytemu. Starostwo posiadało, ale nie wykorzystywało narzędzi do automatycznego gromadzenia, zabezpieczania i automatycznej analizy logów dostępu do informacji. Logi generowane w systemie zabezpieczone były przed utratą integralności i zniszczeniem, co w przypadku zaistnienia sytuacji, w której doszłoby do sytuacji niepożądanej z punktu widzenia bezpieczeństwa danych, z dużym prawdopodobieństwo umożliwiłoby ustalenie sprawcy lub źródła zagrożenia. Podobne wnioski wynikają również z audytu bezpieczeństwa informacji dla Starostwa, sporządzonego w marcu 2017 roku przez zewnętrzną firmę. W dokumencie tym wskazano m. in., że Urząd nie monitoruje regularnie logów urządzeń sieciowych wchodzących w skład infrastruktury. Kwestia niemonitorowania dostępu do informacji została opisana w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 148-186)

1.5. Wg opinii powołanego przez NIK biegłego, w Urzędzie wszystkie komputery pracowały pod kontrolą domeny, co gwarantowało zabezpieczenie przed nieautoryzowanym dostępem do komputerów i usług sieciowych. Zastosowano również wymuszenie okresowej zmiany hasła. Urządzenia pracujące w serwerowni były zabezpieczone hasłem, co wykluczało nieautoryzowany dostęp do nich. Sieć WI-FI, będąca częścią LAN, była zabezpieczona poprzez filtrację adresów MAC. Druga sieć, dostępna gościom Starostwa, była zabezpieczona hasłem i odseparowana od sieci LAN. (dowód: akta kontroli str. 148-152)

1.6. W Starostwie nie wprowadzono regulacji umożliwiających wykorzystanie sprzętu nie będącego własnością jednostki do realizacji zadań powierzonych w ramach obowiązków służbowych. Z opinii biegłego wynika, że konfiguracja sieciowa umożliwiała podłączenie do infrastruktury jednostki sprzętu (laptopy, telefony, tablety) niestanowiącego własności pracodawcy, ale nie było możliwe korzystanie z jej zasobów za pomocą tych urządzeń.

Biegły w opinii wskazał, że użytkownicy komputerów mieli możliwość podłączenia do nich pamięci zewnętrznych, co stwarzało niebezpieczeństwo kopiowania danych do tego nieprzeznaczonych i zainfekowania urządzeń złośliwym oprogramowaniem. Informacja o podłączeniu do komputerów zewnętrznych nośników pamięci (np. pendrive lub dysk przenośny) zapisywana była domyślenie w logach systemu operacyjnego, lecz nie była zabezpieczona w sposób trwały. Audyt bezpieczeństwa informacji również wskazywał na konieczność zablokowania wszystkich portów USB. W trakcie oględzin 20 pomieszczeń, w których przetwarzano dane osobowe nie stwierdzono prywatnych urządzeń, które byłyby podłączone do sieci Starostwa lub wykorzystywane przez pracowników do wykonywania obowiązków służbowych. (dowód: akta kontroli str. 148-186)

1.7. Dokumentacja dotycząca zabezpieczenia danych w Urzędzie nie zawierała raportów potwierdzających wystąpienie przypadków nieautoryzowanych działań związanych z przetwarzaniem informacji. Zgodnie z wyjaśnieniami ASIS, w latach 2016 – 2017 (do 18 grudnia) w Starostwie nie odnotowano takich sytuacji.

(dowód: akta kontroli str. 187, 321-322, 436-439)

1.8. W jednostce wprowadzono regulacje bezpiecznej pracy z komputerami przenośnymi poza jednostką, co zostało opisane w pkt. 3.5 wystąpienia pokontrolnego.

Z opinii biegłego wynika, że Starostwie nie był przewidziany zdalny dostępu do zasobów sieci lokalnej. Na routerze CISCO zestawiono tunel VPN do urzędu marszałkowskiego, który był niezbędny do zarządzani routerem. (dowód: akta kontroli str. 6-71, 148-152)

1.9. Instrukcja zarządzania innymi systemami zawierała regulacje dotyczące przeglądów i konserwacji systemów informatycznych. Zgodnie z jej postanowieniami, prowadzenie wszelkich prac konserwacyjnych wymagało: zawarcia umowy uwzględniającej klauzule poufności w zakresie ochrony danych osobowych, wykonywania doraźnych czynności konserwacyjnych i naprawczych przez osoby nieposiadające upoważnień do przetwarzania

danych osobowych pod nadzorem wyznaczonych osób, przekazania sprzętu do naprawy po usunięciu dysków zawierających dane osobowe bądź usunięciu tych danych za pomocą specjalistycznego oprogramowania, a w przypadku braku takiej możliwości wymagało wykonania naprawy w obecności osoby upoważnionej. Stosownie do Instrukcji zarządzania systemem Pojazd i Kierowca konserwacja oraz naprawa systemów wykonywane były przez Państwową Wytwórnię Papierów Wartościowych S.A.[15] Zgodnie z Instrukcją zarządzania systemem EWOPIS do wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do ich przetwarzania upoważniona była osoba wyznaczona przez Dyrektora Powiatowego Ośrodka Dokumentacji Kartograficznej i Geodezyjnej w Białymstoku[16] (Starosta powierzył PODKiG prowadzenie zbioru „Ewidencja gruntów i budynków", co opisano w pkt. 4.4 wystąpienia pokontrolnego).

W okresie objętym kontrolą zawarto dwie umowy serwisowe. Zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI, w umowach tych zobowiązano wykonawców do zachowania w tajemnicy informacji uzyskanych w ramach realizacji umowy oraz realizacji zadań przez osoby, które uzyskały od Starosty imienne upoważnienie do dokonywania czynności, których treść mogłaby polegać na przetwarzaniu danych osobowych. Upoważnionych do przetwarzania danych osobowych było 12 pracowników podmiotów zewnętrznych.

Z opinii biegłego wynika, że w związku z realizacją umów serwisowych w Starostwie umożliwiono zdalny dostęp do zasobów firmie serwisującej składniki systemu bez konieczności autoryzacji (korzystanie z konta użytkownika, który udostępniał pulpit) i bez nadzoru administratora systemu. Działania te – wg biegłego – wskazują na brak ochrony zasobów Starostwa przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych, co zostało opisane w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 6-71, 148-152, 376-401)

1.10. Biegły wskazał, że wszystkie komputery wchodzące w skład sieci lokalnej zabezpieczone były dedykowanym do tego celu oprogramowaniem. Posiadały one aktualne wersje aplikacji zabezpieczających. Dostęp do sieci lokalnej kontrolowany był przez firewall zainstalowany na routerze CISCO. Zastosowano centralne zarządzanie oprogramowaniem zabezpieczającym, jednak nie wykorzystywano w pełni wszystkich jego możliwości odnośnie kontroli działania systemu. Oględziny 30 komputerów w Urzędzie wykazały, że wszystkie urządzenia miały zainstalowany aktualny program antywirusowy.
(dowód: akta kontroli str. 148-152)

1.11. Starostwo wykorzystywało dwa serwery poczty elektronicznej, zlokalizowane w Krakowie i Białymstoku. Z regulaminów korzystania z serwerów pocztowych wynika, że do obowiązków podmiotów, które udostępniły serwery pocztowe należało zabezpieczenie poczty elektronicznej przez wiadomościami typu SPAM oraz przesyłaniem plików zawierających szkodliwe oprogramowanie. (dowód: akta kontroli str. 188-191)

1.12. Zasady tworzenia kopii zapasowych zostały określone w załączniku nr 3 do Instrukcji zarządzania innymi systemami, w Instrukcji zarządzania systemem EWOPIS oraz w Instrukcji zarządzania system Pojazd i Kierowca. Zgodnie z ww. regulacjami, kopie zapasowe tworzone były dla 13 programów służących do przetwarzania danych osobowych. Nie były tworzone kopie programów SL2014 oraz ORE, ponieważ – jak wyjaśnił ASIS – Starostwo nie jest właścicielem systemów, a jedynie jedną z wielu instytucji zasilających je danymi.

Kopie ośmiu programów wykorzystywanych od przetwarzania danych[17] sporządzane i przechowywane były w Starostwie, w tym kopie zapasowe sześciu programów (Płatnik, SIO, EZD, Płace, Foka, RESTO) przechowywano w miejscu, w którym znajdowały się dane objęte procesem tworzenia kopii, tj. w serwerowni. Praktyka taka stwarzała duże ryzyko utraty danych, co zostało opisane w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Kopie pozostałych systemów, tj. i-PKO, Portal Starosty, RWDZ, BIP, EWOPIS tworzone i przechowywane były poza Starostwem. PWPW inicjowała, wykonywała i weryfikowała poprawności kopii zapasowych systemu CEPiK.

---

[15] Dalej: „PWPW".
[16] Dalej: „PODKiG".
[17] Płatnik, SIO, EZD, Płace, Foka, RESTO, UW4, CEPiK.

Kopie przechowywane w Starostwie wytwarzane były raz dziennie (kopia przyrostowa) i dwa razy w miesiącu kopia całościowa. Okres ich przechowywania wynosił miesiąc lub do sporządzenia następnej kopii (EZD). W okresie objętym kontrolą kopie zapasowe sześciu systemów wytwarzanych i przechowywanych w Urzędzie były testowane. Nie testowano kopii zapasowej systemu EZD. W jednym przypadku zachodziła konieczność odtworzenia zbioru danych z kopii bezpieczeństwa w związku przeinstalowaniem systemu UW4. W wyniku testów udało się przywrócić wszystkie dane znajdujące się w systemach przed utworzeniem kopii lub przed przeinstalowaniem. W latach 2016 – 2017 (do 18 grudnia) w Starostwie nie było przypadków utraty danych.

(dowód: akta kontroli str. 6-71, 192)

1.13. Z opinii biegłego wynika, że pracownicy Starostwa dysponują możliwością ściągania aplikacji i plików wykonalnych, ale nie posiadają uprawnień do instalowania ich na stacjach komputerowych, do których mają dostęp. Wyjątek stanowiło 13 komputerów służących do obsługi finansów Starostwa, ponieważ praca na nich odbywała się na koncie administratora, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Z oględzin 30 komputerów wynika, że zainstalowane na nich systemy operacyjne były aktualne. W Starostwie użytkowanych było 39 komputerów z systemami Windows XP i Vista, które to systemy nie były objęte wsparciem producenta, co zostało opisane w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności". W opinii biegłego podłączenie do sieci LAN wspomnianych komputerów stanowiło zagrożenie bezpieczeństwa sieci. Starosta wyjaśnił, że wyeliminowanie ww. systemów operacyjnych wymaga wymiany sprzętu komputerowego. Odbywa się to sukcesywnie w miarę posiadanych środków (w 2016 roku zakupiono dziewięć komputerów, w 2017 roku 15), jednak stały wzrost zapotrzebowania na sprzęt i szacowany na 200 tys. zł koszt wymiany nie pozwalają na całkowite wyeliminowanie problemu.

Programy zainstalowane na poszczególnych komputerach nie były przypisane do poszczególnych stacji (za wyjątkiem oprogramowania firmy Microsoft). Ewidencję programów wykorzystywanych do przetwarzania danych osobowych prowadzona była oddzielnie. (dowód: akta kontroli str. 75-79, 148-186, 440-443)

1.14. Biegły stwierdził, że wszystkie zbadane komputery 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. 148-152)

1.15. Zasady realizacji płatności wykonywanych drogą elektroniczną zostały określone w umowie na prowadzenie bankowej obsługi budżetu z 27 kwietnia 2017 r. oraz w Instrukcji użytkowania innych systemów. Płatności wykonywane były przy wykorzystaniu systemu bankowości elektronicznej i-PKO, a stanowiska komputerowe, z których wykonywane były przelewy, stanowiły własność Urzędu. Oględziny czterech komputerów wykorzystywanych do wykonywania płatności drogą elektroniczną wykazały, że: zainstalowano na nich aktualne systemy operacyjne posiadające wsparcie producenta oraz programy antywirusowe; dostęp do systemów operacyjnych został zabezpieczony, zgodnie z wymogami Instrukcji zarządzania innymi systemami i rozporządzenia w sprawie dokumentacji oraz warunków technicznych; płatności dokonywane były przez pracowników posiadających narzędzie uwierzytelniające określone w umowie rachunku.

(dowód: akta kontroli str. 75-79, 193-195)

Ustalone nieprawidłowości

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

1. Użytkownicy 13 komputerów posiadali uprawnienia administratora systemu operacyjnego tych urządzeń, mimo iż – zgodnie z ich zakresami obowiązków – nie realizowali oni zadań dotyczących administrowania systemami. W wyniku tego, jak ustalił biegły, dysponowali oni możliwością ściągania aplikacji i plików wykonalnych oraz instalowania ich na stacjach komputerowych, do których mieli dostęp. Było to sprzeczne z przepisem § 20 ust. 2 pkt 4 rozporządzenia KRI, zgodnie z którym

kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających, aby osoby zaangażowane w proces przetwarzania informacji posiadały stosowne uprawnienia i uczestniczyły w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków, mających na celu zapewnienie bezpieczeństwa informacji.

ASIS wyjaśnił, że nadanie uprawnień administratorów systemów operacyjnych 13 użytkownikom wynikało z wymagań dostawcy kompleksowych narzędzi wspomagających realizację zadań finansowo-księgowych. Problem był kilkukrotnie zgłaszany, jednak do zakończenia kontroli NIK nie udało się wypracować odpowiedniego rozwiązania. (dowód: akta kontroli str. 75-79, 92-126, 148-152, 436-439)

2. W latach 2016 – 2017 (do 18 grudnia) w Urzędzie nie wywiązywano się z obowiązku przeprowadzania – raz w roku i po zgłoszonym incydencie bezpieczeństwa – analizy utraty integralności, dostępności lub poufności informacji, do czego zobowiązywał pkt IX.1 SZBI.

   Odpowiedzialny za koordynację zarządzania ryzykiem w Starostwie ASIS wyjaśnił, że przyczyną niewywiązywania się z tego obowiązku była konieczność zmiany opisu stanowisk pracy, celem stworzenia możliwości przypisania danych aktywów dla danego stanowiska pracy. Zmiany te wg ASIS były w końcowej fazie opracowania. Ponadto wskazał, że złożoność problemu i ograniczenia kadrowe uniemożliwiły przeprowadzenie analiz w wymaganym terminie.

   (dowód: akta kontroli str. 51-61, 268-270, 278-295, 444-445)

3. Dwóm z 22 pracowników, z którymi 23 września i 31 grudnia 2016 r. rozwiązano stosunek pracy, nie odebrano uprawnień do systemu EZD. Jeszcze 7 grudnia 2017 r. znajdowali się oni na liście aktywnych użytkowników tego systemu. Natomiast byłemu pracownikowi Wydziału Komunikacji nadano uprawnienia do przetwarzania danych osobowych w systemie CEPiK, mimo że nie był upoważniony przez ADO do przetwarzania danych znajdujących się w tym systemie. Powyższe działania stanowią naruszenie § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI, zobowiązującego do podejmowania działań zapewniających, aby osoby zaangażowane w proces przetwarzania informacji posiadały stosowne uprawnienia, a także bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań tych osób.

   ASIS wyjaśnił, że w wyniku przeoczenia uprawnienia w systemie EZD nie zostały odebrane w chwili ustania stosunku pracy. W stosowanej – w chwili rozwiązania z tymi pracownikami stosunku pracy – karcie obiegowej nie przewidziano bowiem potrzeby uzyskiwania potwierdzenia o uprawnieniach w systemie. W lutym 2017 roku do kart obiegowych dodano stosowną pozycję, co pozwala zapobiec podobnym przeoczeniom. Konta tych osób zostały zdezaktywowane w trakcie kontroli NIK.

   Dyrektor Wydziału Komunikacji wyjaśniła, że pracownik posiadający uprawnienia do systemu CEPiK został przeniesiony do Wydziału Komunikacji z innej komórki organizacyjnej, wobec czego należałoby przypuszczać, że posiadał upoważnienie do przetwarzania danych. Ponadto wskazała, że pracownik ten posiadał upoważnienie Starosty do wydawania decyzji administracyjnych, a w podpisanym przez Starostę zakresie obowiązków zobowiązano go do ochrony danych osobowych. Z powyższego wg opinii Dyrektor wynikała zgoda i uprawnienie do przetwarzania danych.

   W ocenie NIK, stosownie do art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[18], pracownik ten powinien posiadać nadane przez ADO upoważnienie do przetwarzania danych osobowych znajdujących się w systemie, do którego miał uprawnienia. (dowód: akta kontroli str. 127-145, 436-439)

4. W Starostwie nie wdrożono narzędzi do automatycznego gromadzenia, zabezpieczenia i analizy logów dostępu do informacji, mimo ich posiadania. Monitorowanie dostępu do informacji jest – w myśl § 20 ust. 2 pkt 7 lit. a rozporządzenia KRI – jednym z elementów zarządzania bezpieczeństwem informacji, zmierzającym do zapewnienia

[18] Dz. U. z 2016 r., poz. 922.

ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.

ASIS wyjaśnił, że automatyczna analiza logów nie była prowadzona, ponieważ wymaga zastosowania odpowiednich rozwiązań i narzędzi oraz właściwego przeszkolenia pracowników do wykonywania związanych z tym czynności. Wskazał również, że kwestia jest w toku analizy i projektowania odpowiednich rozwiązań.

(dowód: akta kontroli str. 148-152, 436-439)

5. W Urzędzie umożliwiono zdalny dostęp do zasobów firmie serwisującej składniki systemu bez konieczności autoryzacji (z wykorzystaniem kont użytkowników systemu) i bez nadzoru administratora systemu, czym nie zapewniono właściwej ochrony informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniem lub zakłóceniami. Zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji jest – stosownie do § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI – jednym z elementów zarządzania bezpieczeństwem informacji, zmierzającym do zapewnienia ochrony przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.

   ASIS wyjaśnił, że zostaną wypracowywane sposoby rozwiązania tego problemu.

   (dowód: akta kontroli str. 148-152, 436-439)

6. Kopie zapasowe obejmujące bazy danych programów: Płatnik, SIO, EZD, Płace, Foka, RESTO gromadzono na nośnikach przechowywanych w tym samym pomieszczeniu, co urządzenie z którego dane były archiwizowane. Było to niezgodne z przepisem cz. A pkt IV ust. 4 lit. a załącznika do rozporządzenia w sprawie dokumentacji oraz warunków technicznych, stosownie do którego kopie zapasowe przechowuje się w miejscach zabezpieczających je przed uszkodzeniem lub zniszczeniem. Przechowywanie tych kopii w miejscu skąd pochodzą dane stwarza duże ryzyko ich utraty, np. w przypadku wystąpienia pożaru, w wyniku którego zniszczeniu może ulec baza danych i jej kopia zapasowa.

   ASIS wyjaśnił, że 8 grudnia 2017 r., po wykonaniu odpowiedniej infrastruktury, przeniesiono serwer archiwizujący do innego pomieszczenia.

   (dowód: akta kontroli str. 6-71, 148-152, 192, 436-439)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że na 39 ze 175 komputerów wykorzystywanych w Urzędzie zainstalowane były systemy operacyjne Windows XP i Vista , które nie były objęte wsparciem producenta. Podłączenie do sieci LAN wspomnianych komputerów w opinii biegłego stanowiło zagrożenie bezpieczeństwa sieci.

(dowód: akta kontroli str. 75-79, 148-152, 440-443)

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 danych.

2. Dokumentacja i procedury dotyczące ochrony danych

Opis stanu faktycznego

2.1. Dane w Starostwie przetwarzane były w 56 zbiorach. W rejestrze zbiorów osobowych, prowadzonym przez ABI, na podstawie art. 36 ust. 2 pkt 2 ustawy o ochronie danych osobowych, wg stanu na 27 listopada 2017 r., znajdowały się 53 zbiory danych (zagadnienia dotyczące tego rejestru zostały opisane w pkt 2.3 wystąpienia pokontrolnego). Do rejestru zbiorów danych osobowych, prowadzonego przez GIODO, wg stanu na 27 listopada 2017 r. zgłoszono 43 zbiory. Nie zgłoszono dziewięciu zbiorów danych przetwarzanych w związku zatrudnieniem i świadczeniem usług cywilno-prawnych oraz jednego utworzonego na podstawie przepisów dotyczących referendum lokalnego. Trzy zbiory zostały zgłoszone do rejestru prowadzonego przez GIODO w trakcie kontroli NIK, w tym jeden w którym przetwarzane były dane wrażliwe. Kwestie nieuwzględniania zbiorów w rejestrze ABI i niezgłoszenia jednego z nich do rejestru GIODO zostały opisane w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Analiza czterech ostatnich zgłoszeń dotyczących rejestracji zbiorów w rejestrze prowadzonym przez GIODO wykazała, że zawierały one wymagane elementy, określone w art. 41 ust. 1 ustawy o ochronie danych osobowych, tj. wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych, oznaczenie administratora danych i adres jego siedziby, cel przetwarzania danych, opis kategorii osób, których dane dotyczą oraz zakres przetwarzanych danych, sposób zbierania oraz udostępniania danych, a także informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane.

W latach 2016 – 2017 (do 18 grudnia) nie wystąpiły przypadki odmowy rejestracji zbioru danych przez GIODO. Od 27 października 2003 r. do 18 grudnia 2017 r. Starostwo 13 razy wnioskowało o wykreślnie zbiorów danych z rejestru i raz o zmianę nazwy. W 11 przypadkach powodem złożenia wniosku o wykreślenie i zmianę nazwy było uporządkowanie prowadzonych zbiorów, w trzech zmieniające się przepisy. Po dokonanych zmianach jeden zbór został przekazany wojewodzie podlaskiemu, jeden komisyjnie zniszczony (prowadzony był w wersji papierowej), jeden prowadzony jest pod inną nazwą, a 11 zbiorów włączono do innych w dalszym ciągu przetwarzanych zbiorów.

(dowód: akta kontroli str. 196-228)

2.2. Starosta 24 marca 2015 r. powołał pracownika Wydziału Organizacyjnego na stanowisko ABI i w tym samym dniu fakt ten zgłoszono do GIODO. Zgłoszenie zawierało wszystkie elementy wymagane art. 46b ust. 2 ustawy o ochronie danych osobowych i nastąpiło na wzorze określonym w rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji[19]. Od dnia powołania do dnia 18 grudnia 2017 r. nie było zmian na tym stanowisku. (dowód: akta kontroli str. 235-239)

2.3. Stosownie do art. 36a ust. 2 pkt 1 ustawy o ochronie danych osobowych, ABI realizował obowiązki dotyczące zapewnienia przestrzegania przepisów o ochronie danych osobowych.

W latach 2016 – 2017 (do 18 grudnia) sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych realizowane było na podstawie harmonogramów zatwierdzonych przez ADO. Sprawdzenie obejmowało przestrzegane procedury korzystania z Internetu, zasad czystego biurka i czystego ekranu, analizę dokumentów i informacji publikowanych w BIP pod względem ochrony danych osobowych, weryfikację dokumentacji przetwarzania danych osobowych oraz środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych, a także zgłoszonych do GIODO zbiorów danych osobowych. W PODKiG, z którym Starostwo zawarło umowę powierzenia przetwarzania danych w zbiorze „Ewidencja gruntów i budynków", sprawdzono: wydawanie danych osobowych dla gmin powiatu oraz Starostwa, udostępnianie danych ze zbioru za pomocą przeglądarki online, aktualność ewidencji osób upoważnionych, aktualność dokumentacji i procedur obejmujących ochronę danych osobowych, aktualność oprogramowania, wykonywanie analizy logów systemowych, sporządzanie kopii zapasowych oraz stan bezpieczeństwa infrastruktury IT.

Czynności dokonywane w ramach sprawdzeń dokumentowane były sprawozdaniami spełniającymi wymogi art. 36c ustawy o ochronie danych osobowych, zatwierdzanymi przez ADO. W efekcie dokonywanych przez ABI czynności, w 2016 roku zaktualizowano 26 zgłoszeń zbiorów do GIODO, uzupełniono Politykę bezpieczeństwa o analizę zagrożeń i ryzyka przy przetwarzaniu danych osobowych, usunięto z dwóch komputerów oprogramowanie, które nie było użytkowane w Starostwie, zwrócono ADO potrzebę zmiany lokalizacji serwera tworzącego kopie zapasowe oraz zmianę komputerów z nieaktualnymi systemami operacyjnymi.

Ponadto w okresie objętym kontrolą, zgodnie z pkt 9 Polityki bezpieczeństwa, ABI reagował na incydenty bezpieczeństwa, którymi było zalanie archiwum oraz upublicznienie danych osobowych w BIP. Skutkiem pierwszego było zamoczenie 2,5 tys. teczek aktowych, a drugiego upublicznienie w latach 2004 – 2017 uchwał Zarządu Powiatu Białostockiego zawierających niezanonimizowane dane osobowe[20] (32 przypadki). W związku z tymi incydentami wszczęte zostały postępowania sprawdzenia doraźnego, z których ABI

[19] Dz. U. poz. 1934.

[20] Upublicznione zostały imiona i nazwiska użytkowników wieczystych nieruchomości oraz adresy tych nieruchomości.

sporządził sprawozdania i przedstawił ADO. Wdrożono również działania naprawcze w postaci osuszenia zamoczonych akt, naprawy uszkodzonej instalacji i przeniesienia archiwum do innego pomieszczenia oraz zanonimizowania akt i zmiany przepisów wewnętrznych w zakresie publikowania informacji.

W latach 2016 – 2017 (18 grudnia) cztery razy aktualizowana była dokumentacja określająca sposób przetwarzania danych osobowych, co opisano szerzej w pkt 2.10 wystąpienia pokontrolnego.

ABI w okresie objętym kontrolą przeprowadził 112 szkoleń stanowiskowych pracowników Starostwa z zakresu regulacji ustawowych, aktów wykonawczych i wewnętrznych dotyczących ochrony danych osobowych. Ponadto w ramach wykonywania obowiązków w zakresie sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, ABI informował pracowników o obowiązujących przepisach i procedurach w przypadku ich naruszenia. (dowód: akta kontroli str. 5-6, 240-270, 296)

Zgodnie z art. 36b ust. 2 pkt 2 ustawy o ochronie danych osobowych, ABI prowadził w formie papierowej rejestr zbiorów danych przetwarzanych przez ADO, który stosownie do art. 41 ust. 1 pkt 2-4a i 7 ustawy o ochronie danych osobowych, zawierał oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania oraz numer identyfikacyjny REGON, podstawę prawną upoważniającą do prowadzenia zbioru, cel przetwarzania danych, opis kategorii osób, których dane dotyczą, zakres przetwarzanych danych, sposób zbierania oraz udostępniania danych i informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane. W dniu 27 listopada 2017 r. w rejestrze tym znajdowały się 53 zbiory danych z 56 przetwarzanych w Starostwie. Nie uwzględniono w nim trzech zbiorów, w których przetwarzano dane osobowe, co zostało opisane w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 196-199, 223, 446)

2.4. W Urzędzie, stosownie do art. 39 ust. 1 ustawy o ochronie danych osobowych, prowadzono ewidencję osób upoważnionych do przetwarzania danych osobowych. Zawierała ona elementy określone w art. 39 ust 1 pkt 1 – 3 ww. ustawy, tj.: imię i nazwisko osoby upoważnionej, datę nadania i ustania upoważnienia do przetwarzania danych osobowych, zakres upoważnienia oraz identyfikator. W ewidencji tej znajdowały się również osoby upoważnione do przetwarzania danych osobowych w zbiorze „Ewidencja gruntów i budynków", którego prowadzenie powierzono PODKiG. (dowód: akta kontroli str. 271-272)

Porównanie zakresów obowiązków z upoważnieniami do przetwarzania danych osobowych 30 pracowników Starostwa wykazało, że 23 pracowników posiadało upoważnienia do przetwarzania danych osobowych adekwatne do zadań wykonywanych i przypisanych w zakresach obowiązków. W czterech przypadkach pracownicy posiadali upoważnienie do przetwarzania danych osobowych w zbiorze BIP, mimo braku w zakresach swoich obowiązków zadań dotyczących publikacji informacji w BIP, co zostało opisane w dalszej części wystąpienia, w sekcji „Uwagi dotyczące badanej działalności". Z kolei w czterech przypadkach pracownicy otrzymali upoważnienia do przetwarzania danych osobowych w trakcie kontroli NIK, mimo że z zakresów obowiązków wynika, że dane te przetwarzali wcześniej[21]. Ponadto analiza procedury nadawania i zmiany uprawnień do systemów informatycznych, w których przetwarzane były dane osobowe opisana w pkt 1.3. wystąpienia pokontrolnego wykazała, że jeden z 30 pracowników przetwarzał dane osobowe w zbiorze „Ewidencja kierowców", mimo braku upoważnienia ADO. Zgodnie z pkt 11.1 c Polityki bezpieczeństwa za kontrolę, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone odpowiadają dyrektorzy wydziałów i samodzielne stanowiska pracy. Zobowiązani są oni do informowania ABI o prowadzonych zbiorach, zaistniałych w nich zmianach, a także o osobach, którym należy wydać, cofnąć lub zaktualizować upoważnienie do przetwarzania danych osobowych. Kwestia braku posiadania upoważnień do przetwarzania danych osobowych została opisana w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 6-71, 127-139, 144-145, 273-277, 447-497, 499-501)

[21] Archiwistka, specjalista ds. BHP, audytor wewnętrzny, główny specjalista w Wydziale Kultury, Sportu, Turystyki i Promocji.

2.5. W Urzędzie obowiązywały wewnętrzne akty prawne dotyczące m.in. sposobu gromadzenia i przetwarzania zasobów informacyjnych. Zgodnie z pkt VII.5. SZBI, do uregulowań tych należały m.in: dokumentacja stanowiąca przyjęte zasady (politykę) rachunkowości; instrukcja inwentaryzacyjna; instrukcja sporządzania, obiegu, kontroli i ochrony dokumentów finansowo-księgowych; regulamin udostępniania informacji publicznej; zasady organizacji i funkcjonowania kontroli zarządczej; Instrukcja Bezpieczeństwa Pożarowego dla obiektu Starostwa Powiatowego w Białymstoku położonego w Białymstoku przy ul. Borsuczej 2; zasady postępowania w przypadku zalania lub zatopienia pomieszczenia, w którym są przetwarzane dane osobowe w Wydziale Komunikacji. Dokumentacja ta była aktualizowana, np. w związku z wystąpieniem incydentu bezpieczeństwa związanego z udostępnieniem w BIP danych osobowych, zmieniono zasady udostępniania informacji publicznej. Ponadto w okresie objętym kontrolą aktualizowane były instrukcja inwentaryzacyjna, instrukcja sporządzania, kontroli i ochrony dokumentów finansowo-księgowych oraz zasady organizacji i funkcjonowania kontroli zarządczej. (dowód: akta kontroli str. 278-294, 334-374, 429)

2.6. Na podstawie § 20 ust. 2 rozporządzenia KRI oraz pkt VI.1.3 SZBI, 7 grudnia 2015 r. Starosta wyznaczył pracownika Wydziału Organizacyjnego na ASIS. Posiadał on upoważnienie do przetwarzania danych osobowych w administrowanych systemach. (dowód: akta kontroli str. 295)

2.7. Od 16 do 17 marca 2017 r. w Starostwie przeprowadzano audyt z zakresu bezpieczeństwa informacji. Audytu takiego nie przeprowadzono w 2016 roku, wbrew obowiązkowi wynikającemu z § 20 ust. 2 pkt. 14 rozporządzenia KRI, co zostało opisane w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Audyt bezpieczeństwa informacji w 2017 roku przeprowadziła firma zewnętrza. W jego wyniku rekomendowano: wprowadzenie rocznego harmonogramu dedykowanych szkoleń dla informatyków, wymianę systemów operacyjnych niewspieranych przez producenta, wprowadzenie imiennego rejestru poboru kluczy do wszystkich pomieszczeń, wdrożenie oprogramowania do czynnego monitoringu środowiska teleinformatycznego pod kątem włamań i przeprowadzonych wewnątrz działań, zdeponowanie haseł administracyjnych do systemu w bezpiecznym miejscu, opracowanie planów awaryjnych na wypadek wystąpienia niestandardowych okoliczności, doposażenie serwerowni w czujniki zalania i dymu, poblokowanie portów USB, rejestrowanie wszystkich nawiązywanych połączeń, aktualizowane systemów operacyjnych oraz zabezpieczenie wszystkich urządzeń przed nieuprawnionym wpięciem. Ustalenia kontroli NIK wykazały, że w Starostwie nie zrealizowano części wniosków z audytu, co szerzej zostało opisane w wystąpieniu pokontrolnym. (dowód: akta kontroli str. 153-186)

2.8. W okresie objętym kontrolą 72 pracowników Starostwa brało udział w szkoleniu prowadzonym przez podmiot zewnętrzny, dotyczącym zagadnień bezpieczeństwa pracy w systemach informatycznych. Prowadzone były również szkolenia stanowiskowe, co zostało opisane w pkt 2.3 wystąpienia pokontrolnego. ABI wyjaśnił, że w Starostwie planowane są szkolenia w związku ze zmianą przepisów o ochronie danych osobowych, które mają wejść w życie 25 maja 2018 r., 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)[22]. (dowód: akta kontroli str. 296, 430-435)

2.9. W okresie objętym kontrolą w Urzędzie nie były prowadzone zewnętrzne kontrole w zakresie bezpieczeństwa danych osobowych. Do Starostwa nie wpływały również skargi związane z przypadkami ujawnienia danych osobowych. (dowód: akta kontroli str. 297-298)

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 8 października 2015 r. Składały się na nią Polityka bezpieczeństwa, Instrukcja zarządzenia systemem Pojazd

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

i Kierowca, Instrukcja zarządzania systemem EWOPIS, Instrukcja zarządzania innymi systemami, a także analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych.

Dokumentacja ta w latach 2016 – 2017 (do 18 grudnia) była cztery razy aktualizowana[23]. Zmiany obejmowały: wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (trzykrotnie), Instrukcję zarządzania systemem EWOPIS, Instrukcję zarządzania innymi systemami, analizę zagrożeń i ryzyka przy przetwarzaniu danych osobowych, opis struktury zbiorów danych wskazujący na zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

Polityka bezpieczeństwa, w myśl przepisu § 4 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, zawierała: wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposób przepływu danych pomiędzy poszczególnymi systemami, określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Wszystkie trzy instrukcje zarządzania systemem informatycznym służącymi do przetwarzania danych, stosownie do § 5 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, zawierały: procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności, stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem, procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu, procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych danych, sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, a także procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych. Ponadto we wszystkich ww. dokumentach określono wysoki poziomu bezpieczeństwa przetwarzania danych osobowych.

(dowód: akta kontroli str. 5-71)

W Starostwie, zgodnie z obowiązkiem wynikającym z § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI, opracowano i wdrożono SZBI, który określał m.in. zadania i obowiązki w zakresie: [1] aktualizacji regulacji wewnętrznych dotyczących zmieniającego się otoczenia; [2] przeprowadzania okresowych analiz ryzyka utraty integralności; [3] zarządzenia uprawnieniami dostępu; [4] zapewnienia szkoleń; [5] zapewnienia ochrony przetwarzanych danych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami; [6] przetwarzania mobilnego; [7] zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych; [8] zapewnienia w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa; [9] zgłaszania incydentów w przypadku naruszenia bezpieczeństwa informacji.

(dowód: akta kontroli str. 278-294)

Ustalone nieprawidłowości

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

1. Wbrew obowiązkowi wynikającemu z art. 40 ustawy o ochronie danych osobowych, do rejestru zbiorów danych osobowych, prowadzonego przez GIODO, nie został zgłoszony zbiór danych osobowych o nazwie „Kierowanie do szkół lub ośrodków poza granicami powiatu", w którym od 1999 roku przetwarzane były dane wrażliwe wymienione w art. 27 ust. 1 ww. ustawy.

[23] Zarządzeniami Starosty Powiatu Białostockiego nr 11/2016 z dnia 22 lutego 2016 r., nr 25/2016 z dnia 30 czerwca 2016 r, nr 37/2016 z dnia 7 grudnia 2016 r, nr 23/2017 z dnia 15 listopada 2017 r.

Przyczyną powstania nieprawidłowości było niezgłoszenie ABI faktu prowadzenia zbioru przez dyrektora wydziału, zobowiązanego do tego na podstawie pkt 11.1c Polityki bezpieczeństwa. ADO wyjaśniła, że zbiór danych został zgłoszono do rejestru GIODO w trakcie kontroli NIK.

(dowód: akta kontroli str. 6-71, 196-199, 223, 309-310, 430-435, 498-500)

2. W rejestrze zbiorów danych osobowych przetwarzanych przez ADO – wbrew obowiązkowi wynikającemu z art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych – nie uwzględniono trzech zbiorów danych osobowych, które były przetwarzane w Starostwie, tj. Rejestru roślin i zwierząt podlegających ograniczeniom na podstawie umów międzynarodowych, Rejestru wypadków przy pracy oraz Kierowania do szkół specjalnych lub ośrodków poza granicami powiatu.

   ABI prowadzący rejestr wyjaśnił, że zbiory te nie zostały mu zgłoszone przez dyrektorów wydziałów i samodzielne stanowiska, wbrew wymogom pkt 11.1c Polityki bezpieczeństwa. Dyrektorzy Wydziału Środowisk i Rolnictwa oraz Wydziału Spraw Społecznych i Zarządzania Kryzysowego wyjaśnili, że konieczność zgłoszenia zbiorów stwierdzono w toku kontroli. Natomiast Specjalista ds. BHP wskazał, że nie zgłaszał takiego zbioru, ponieważ ABI wiedział o jego istnieniu z faktu publikowania rejestru wypadków przy pracy w BIP. W trakcie kontroli NIK ww. zbiory danych osobowych zostały ujęte w rejestrze prowadzonym przez ABI.

   (dowód: akta kontroli str. 6-71, 196-199, 223, 307-310, 313-320, 430-435)

3. Pięciu[24] z 58 objętych badaniem pracowników Starostwa przetwarzało dane osobowe, mimo braku stosownych upoważnień ADO. Przetwarzanie danych bez upoważnienia nadanego przez ADO stanowi naruszenie art. 37 ustawy o ochronie danych osobowych.

   ADO wyjaśnił, że w przypadku audytora wewnętrznego brak upoważnienia do przetwarzania danych osobowych wynikał z faktu, iż w jego ocenie przepis art. 282 ust. 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[25] zapewniał mu dostęp do tych danych przy zastosowaniu zasady adekwatności. Specjalista BHP otrzymał odpowiednie upoważnienie w chwili zgłoszenia zbioru „Rejestr wypadków przy pracy" do GIODO, tj. w dniu 1 grudnia 2017 r. Natomiast archiwistka otrzymała upoważnienie w związku z analizą materiału przekazywanego do archiwum. Wskazał również, że posiadała ona niezbędną wiedzę na temat bezpieczeństwa przetwarzanych danych osobowych. Pracownikowi nie wydano upoważnienia do przetwarzania danych w „Rejestrze stowarzyszeń i fundacji", ponieważ przetwarzane są w nim dane jawne i ogólnodostępne. Z kolei pracownik Wydziału Komunikacji posiadał upoważnienie do wydawania decyzji administracyjnych, a brak upoważnienia do przetwarzania danych osobowych wynikał z niezgłoszenia do ABI konieczności nadania takiego upoważnienia przez bezpośredniego przełożonego (wyjaśnienia Dyrektor Wydziału Komunikacji w tej kwestii zostały przywołane w pkt 1 wystąpienia pokontrolnego, w pkt 3 sekcji „Ustalone nieprawidłowości").

   Zdaniem NIK, ww. przepis ustawy o finansach publicznych określa kompetencje audytora wewnętrznego, nie zwalania zaś z obowiązku posiadania upoważnienia nadanego przez ADO do przetwarzania danych osobowych, o którym mowa w art. 37 ustawy o ochronie danych osobowych. Z konieczności nadania upoważnienia do przetwarzania danych osobowych nie zwalnia również fakt jawności przetwarzanych danych, na co wskazuje fakt zgłoszenia GIODO zbioru, w którym przetwarzano te dane w 2003 roku. Do zakończenia kontroli NIK ww. pracownikom zostały nadane uprawnienia ADO do przetwarzania danych osobowych.

   (dowód: akta kontroli str. 127-139, 144-145, 196-199, 273-277, 303-304, 430-435, 447-497, 499-501)

---

[24] Specjalista ds. BHP od 3 czerwca 2014 r. do 1 grudnia 2017 r., archiwistka od 19 maja 2009 r. do 29 listopada 2017 r., audytor wewnętrzny od 23 grudnia 2002 r. do 24 października 2017 r. oraz podinspektor w Wydziale Komunikacji od 22 lipca 2016 r. do 24 stycznia 2017 r. przetwarzali dane osobowe, mimo że nie posiadali upoważnienia do ich przetwarzania. Główna specjalistka w Wydziale Kultury, Sportu, Turystyki i Promocji od 3 marca 2016 r. do 30 listopada 2017 r. przetwarzała dane w „Rejestrze stowarzyszeń i fundacji" bez upoważnienia do przetwarzania tych danych (posiadała upoważnienie ADO do przetwarzania danych tylko w zbiorze „Rejestr klubów sportowych").

[25] Dz. U. z 2017 r. poz. 2077.

4. Od 1 stycznia 2016 r. do 15 marca 2017 r. w Starostwie nie przeprowadzano corocznego audytu wewnętrznego z zakresu bezpieczeństwa informacji, mimo wymogu wynikającego z § 20 ust. 2 pkt. 14 rozporządzenia KRI.

   Starosta wyjaśnił, że obowiązek wykonania audytu został nałożony na samorząd bez zapewnienia jakichkolwiek środków na jego realizację. Pod koniec 2015 roku w Starostwie audyt w zakresie bezpieczeństwa informacji zrealizowała komórka wewnętrzna. Jednak w związku ze stanowiskiem Departamentu Informatyzacji Ministerstwa Administracji i Cyfryzacji z 25 kwietnia 2013 r., stosownie do którego sformułowanie „audyt wewnętrzny" nie oznacza obligatoryjnego wykonywania audytu przez komórki wewnętrze i z uwagi na wymóg posiadania wiedzy eksperckiej w zakresie audytowanego obszaru zdecydowano się powierzyć te zadanie instytucji zewnętrznej. Środki na ten cel zaplanowano w budżecie 2016 roku. W trakcie 2016 roku, na skutek zmiany przepisów, samorząd został zobowiązany do sfinansowania nieplanowanej usługi doradztwa podatkowego w zakresie prac związanych z centralizacją VAT, co spowodowało konieczność przesunięcia audytu na 2017 rok.

   (dowód: akta kontroli str. 440-443)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że czterech pracowników Urzędu zostało upoważnionych do przetwarzania danych osobowych w zbiorze BIP, mimo braku stosownych zapisów w zakresach obowiązków. W myśl § 20 ust. 2 pkt 4 rozporządzenia KRI osoby zaangażowane w proces przetwarzania informacji powinny uczestniczyć w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków.

Dyrektorzy wydziałów, w których zatrudniono osoby upoważnione do przetwarzania danych osobowych z zbiorze BIP wskazali, że zakresy obowiązków tych pracowników nie uwzględniały zadań związanych z przetwarzaniem danych w tym zbiorze, ponieważ były w trakcie opracowywania (w jednym przypadku) bądź publikacja w BIP była elementem wykonywanych zadań i nie wymaga odrębnego ujęcia w zakresie obowiązków (w trzech przypadkach). (dowód: akta kontroli str. 273-277, 303-308, 311-312)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości, 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 fizyczne pomieszczeń z danymi osobowymi w wersji papierowej i elektronicznej, na które składały się: system alarmowy, całodobowy dozór (monitoring i firma świadcząca usługi ochrony), wzmocnione drzwi, kraty w oknach, kontrola dostępu, klimatyzacja oraz sygnalizacja. Oględziny 20 pomieszczeń Starostwa znajdujących się przy ul. Borsuczej 2, w tym serwerowni oraz archiwum zakładowego wykazały, że przetwarzanie danych osobowych odbywało się w 19 przypadkach w pomieszczeniach wskazanych w Polityce bezpieczeństwa, a w jednym przypadku w innym pomieszczeniu (kwestia ta opisana została w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości"). Budynek przy ul. Borsuczej 2 objęty był całodobowym dozorem, monitoringiem wizyjnym, a między godziną 22^{00} a 6^{00} włączany był system alarmowy. Zgodnie z Polityką bezpieczeństwa, wszystkie pomieszczenia objęte oględzinami były zamykane na klucz, w 10 z nich zainstalowano wzmocnione drzwi, w tym w serwerowni, archiwum zakładowym oraz w ośmiu pomieszczeniach, w których przetwarzane były dane zawarte w zbiorach „Ewidencja pojazdów" i „Ewidencja kierowców". W pomieszczeniach serwerowni oraz w czterech pomieszczeniach, w których przetwarzane były dane zawarte w zbiorach „Ewidencja pojazdów" i „Ewidencja kierowców", zainstalowana została klimatyzacja. Kraty w oknach, zgodnie z Polityką bezpieczeństwa, znajdowały się we wszystkich pomieszczeniach zlokalizowanych w piwnicy budynku oraz w pokoju 122 (pomieszczenie na pierwszym piętrze z oknem przylegającymi do budynku parterowego). Stosownie do wewnętrznych regulacji w zakresie ochrony danych osobowych w 16 z 20 pomieszczeń objętych oględzinami dane osobowe przechowywane były w zamykanych na klucz szafach (w serwerowni i trzech pomieszczeniach przetwarzano dane tylko w formie elektronicznej) – w jednym przypadku była to szafa pancerna, a w dwóch – szafy metalowe. W budynku przy ul. Borsuczej 2 nie zainstalowano systemu

przeciwpożarowego, znajdowały się w nim gaśnice, system hydrantów oraz system ostrzegający o pożarze. W pomieszczeniach serwerowni i archiwum znajdujących się w piwnicy budynku nie zainstalowano czujników dymu, temperatury oraz zalania, przez co nie zapewniono danym przechowywanym w tych pomieszczeniach właściwej ochrony przed działaniem czynników fizycznych i zdarzeń losowych (zalanie, pożar). Kwestia ta została opisana w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

W Instrukcji zarządzania innymi systemami określono politykę kluczy. W wyniku oględzin ustalono, że zgodnie z nią szafy z aktami osobowymi zamykane były na klucz, który przechowywany był w bezpiecznym miejscu. Klucze do pomieszczeń, w których przetwarzane były dane osobowe, zgodnie z tą polityką, po zakończeniu pracy, pracownicy zostawiali w portierni, monitorowanej przez całą dobę. Odpowiedzialni za klucze od serwerowni i archiwum pracownicy oświadczyli, że przechowywano je w bezpiecznych miejscach.

Jednym z wniosków audytu bezpieczeństwa informacji było wprowadzenie imiennego rejestru poboru kuczy do wszystkich pokoi, co pozwoliłoby na pełną weryfikację incydentów. ABI wyjaśnił, że nie było potrzeby realizacji wniosku, ponieważ portiernia, w której deponowane i pobierane są klucze objęta była monitoringiem wizyjnym.

(dowód: akta kontroli str. 6-71, 321-329, 430-435)

3.2. W Starostwie, stosownie do § 20 ust. 20 pkt 2 rozporządzenia KRI, za pomocą programu Qasystent, gromadzono bieżące informacje w zakresie sprzętu i oprogramowania służącego do przetwarzania danych osobowych. Program ten umożliwiał sprawdzenie danych o: użytkowanych komputerach stacjonarnych, komputerach przenośnych, serwerach, rodzaju użytkowanych urządzeń, nr ewidencyjnym, nr seryjnym, dacie upływu gwarancji, komórce organizacyjnej, w której było użytkowane urządzenie, pracowniku odpowiedzialnym za urządzenie, zainstalowanych systemach operacyjnych, zainstalowanych programach (nie były przypisane do poszczególnych stacji z wyjątkiem oprogramowania Microsoftu), licencjach na oprogramowanie (nie były przypisane do poszczególnych stacji z wyjątkiem oprogramowania Microsoftu).

(dowód: akta kontroli str. 330-331)

3.3. W latach 2016 – 2017 (do 18 grudnia) w Starostwie zlikwidowano pięć nośników danych typu pendrive. Likwidacji dokonywały dwie komisje poprzez przecięcie układu scalonego pamięci. Sposób likwidacji odpowiadał wymogom Instrukcji zarządzania innymi systemami. W okresie tym nie wystąpiły przypadki naprawy sprzętu komputerowego przez podmioty zewnętrzne. (dowód: akta kontroli str. 6-71, 332)

3.4. Niszczenie dokumentów zawierających dane osobowe do 28 kwietnia 2017 r. realizowane było przez pracownika odpowiedzialnego za archiwum, po uprzednim uzyskaniu zgody Archiwum Państwowego w Białymstoku. Niszczenie dokonywane było przy pomocy niszczarki dokumentów. Począwszy od 14 listopada 2017 r. zadanie to realizuje firma zewnętrzna. Przyjęte rozwiązania były zgodne z obowiązującymi procedurami.

(dowód: akta kontroli str. 6-71, 333)

3.5. Regulamin użytkowania komputerów przenośnych stanowił załącznik nr 1 do Instrukcji zarządzania innymi systemami. Wykorzystanie urządzeń poza obszarem przetwarzania danych osobowych wymagało m.in. zaszyfrowania nośników z danymi osobowymi, regularnego tworzenia kopii bezpieczeństwa i przechowywania w bezpiecznym miejscu oraz zabezpieczenia przed kradzieżą. Jak wyjaśnił ABI, w okresie objętym kontrolą nie było zgłoszeń przypadków wykorzystywania poza jednostką komputerów przenośnych przetwarzających dane osobowe.

Pracownicy mieli możliwość korzystania z programu EZD poza siedzibą Starostwa. Zgodnie z Instrukcją zarządzania innymi systemami wymagało to uwierzytelnienia. Biegły w opinii wskazał, że aplikacja EZD nie była utrzymywana w infrastrukturze sieci LAN Starostwa. Administrowana była przez firmę Maxto, będącą pełnomocnikiem urzędu marszałkowskiego. (dowód: akta kontroli str. 6-71, 148-152)

3.6. Sprzątaniem pomieszczeń zajmowali się pracownicy Starostwa – trzy sprzątaczki i czterech rzemieślników. Pomieszczenia sprzątane były po zakończeniu pracy, od godziny 15^{30} lub od 16 do 22. Pracowników sprzątających zobowiązano do zachowania w tajemnicy danych osobowych oraz zgłaszania ABI lub bezpośredniemu przełożonemu incydentów związanych z naruszeniem zasad ochrony danych osobowych. Serwerownia i archiwum sprzątane były przez pracowników odpowiedzialnych za te pomieszczenia.

Pracownicy Starostwa Instrukcją zarządzania innymi systemami zobowiązani zostali do zabezpieczenia dokumentów przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniu lub po zakończeniu pracy (tzw. polityka czystego biurka).

(dowód: akta kontroli str. 6-71, 321-329)

3.7. Zgodnie z Instrukcją zarządzania innymi systemami, za terminowość i prawidłowy przebieg konserwacji i przeglądów systemu informatycznego odpowiada ASIS. Wykonywanie prac konserwacyjnych i napraw sprzętu obywało się zgodnie z umową, z uwzględnieniem klauzuli poufności danych osobowych oraz pod nadzorem osób wyznaczonych. Szerzej kwestia ta została opisana w pkt 1.9 wystąpienia pokontrolnego.

(dowód: akta kontroli str. 6-71, 376-401)

3.8. W Urzędzie (z wyjątkiem instrukcji bezpieczeństwa pożarowego oraz zasad postępowania w przypadku zalania lub podtopienia pomieszczeń, w których przetwarzano dane osobowe w Wydziale Komunikacji) nie opracowano wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia innych sytuacji nadzwyczajnych. Nie opracowano także procedur przywracania systemów po awarii oraz planu ciągłości działania, umożliwiającego kontynuację wykonywania zadań publicznych, chociaż jednym z zaleceń audytu bezpieczeństwa informacji było opracowanie planów awaryjnych na wypadek wystąpienia sytuacji nadzwyczajnych. ASIS wyjaśnił, że nie było potrzeby opracowania takich procedur, ponieważ w przypadku wystąpienia sytuacji nadzwyczajnych w systemach przetwarzających dane będzie wiedział jakie działania podjąć. Kwestię ta została opisana w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności".

Możliwość pracy w przypadku braku energii elektrycznej zapewniały urządzenia typu UPS (do którego podłączonych było 21 z 28 objętych oględzinami komputerów stacjonarnych[26] i wszystkie serwery Starostwa) oraz automatyczny awaryjny układ zasilania w postaci agregatu prądotwórczego (pozostającego pod dozorem technicznym i bieżącą konserwacją). (dowód: akta kontroli str. 6-71, 75-79, 321-329, 334-353, 436-439)

3.9. Jak wyjaśniła ASIS, w okresie objętym kontrolą w Starostwie nie wystąpiły przypadki fizycznej utraty danych. Procedury postępowania w przypadku wystąpienia incydentu bezpieczeństwa danych osobowych stosowane były w sytuacjach opisanych w pkt. 2.3. wystąpienia pokontrolnego. (dowód: akta kontroli str. 267-270, 444-445)

Ustalone nieprawidłowości

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

1. Zbiór danych osobowych „Wnioski konsumentów w sprawie udzielenia pomocy prawnej przy dochodzeniu roszczeń konsumenckich" przetwarzany były w pokoju nr 210, co było niezgodne z Polityką bezpieczeństwa, stosownie do której powinien być przetwarzany w pokoju nr 2.

   ABI wyjaśnił, że wynikało to z niezaktualizowania Polityki bezpieczeństwa, po zmianie pomieszczenia zajmowanego przez Rzecznika Praw Konsumentów.

   (dowód: akta kontroli str. 6-71, 321-329, 430-435)

2. Pomieszczenia archiwum zakładowego i serwerowni, znajdujące się w piwnicy budynku Starostwa przy ul. Borsuczej 2, nie posiadały czujników ostrzegających o pożarze oraz zalaniu. Przyjęcie takich rozwiązań nie zapewnia właściwej ochrony zbiorów danych przed działaniem czynników fizycznych i zdarzeń losowych (pożar, zalanie) i stanowi naruszenie art. 36 ust. 1 ustawy o ochronie danych osobowych, stosownie do którego ADO powinien zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych

[26] Na siedmiu komputerach, które nie posiadały urządzeń typu UPS zainstalowano programy do przetwarzania danych EZD, EWOPIS oraz rejestr korespondencji wychodzącej. Dane z tych systemów zapisywane i archiwizowane były na serwerze.

danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane m.in. przed ich uszkodzeniem lub zniszczeniem. Ponadto stosownie do § 6 załącznika nr 6 do rozporządzenia w sprawie działania archiwów zakładowych[27], pomieszczenie archiwum powinno posiadać system przeciwpożarowy oraz być zabezpieczone przed zalaniem. Konieczność stosowania takich zabezpieczeń uzasadnia także fakt zalania 2,5 tys. teczek z aktami w archiwum zakładowym w 2016 roku.

Starosta wyjaśnił, że budynek Starostwa pochodzi z lat 70-tych, który był wielokrotnie modernizowany i remontowany (m.in. wymieniono instalację elektryczną, podłączono agregat prądotwórczy, w niektórych pomieszczeniach zainstalowano czujniki dymu, monitoring oraz system alarmowy). W 2015 roku przyjęto koncepcję jego rozbudowy, która jednak była stale przez Radę Powiatu zmieniana. W związku brakiem rozstrzygnięć dotyczących dalszej rozbudowy siedziby Starostwa, podjęto decyzje o przeniesieniu archiwum zakładowego na parter budynku przy ul. Borsuczej 2.

(dowód: akta kontroli str. 267, 321-329, 440-443)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na potrzebę opracowania wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np.: długotrwałego braku zasilania bądź przywracania systemów po awarii, a także planu ciągłości działania, umożliwiającego kontynuację wykonywania zadań. Plan ten powinien określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany. Istotne jest, aby plany te były jasno udokumentowane, przekazane pracownikom i aktualizowane w celu odzwierciedlenia bieżącej działalności Starostwa.

(dowód: akta kontroli str. 6-71, 153-186, 75-79, 321-329, 334-353, 436-439)

Ocena cząstkowa

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

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności kontrolowanej jednostki

Opis stanu faktycznego

4.1. W Starostwie (wg stanu na 15 listopada 2017 r.) dane osobowe przetwarzane były w 56 zbiorach danych, z których 35 przetwarzano w wersji papierowej i elektronicznej, 15 w wersji papierowej oraz sześć w wersji elektronicznej. Dane osobowe przetwarzane były w 15 programach, wymienionych w pkt. 1.1. wystąpienia. W wykazie zbiorów danych osobowych, stanowiącym element Polityki bezpieczeństwa, ujętych zostało tylko 52 z 56 prowadzonych zbiorów danych[28], co zostało opisane w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 6-74, 196-199, 223)

4.2. W okresie objętym kontrolą, tj. w latach 2016 – 2017 (do 28 listopada) zaktualizowano 22 zbiory danych w rejestrze prowadzonym przez ABI, co zgłoszono do rejestru GIODO. Za analizy ośmiu wniosków wynika, że siedem dotyczyło wykreślenia zbioru i przeniesienia danych w nim przetwarzanych do innego zbioru, natomiast jeden dotyczyły zmiany nazwy zbioru. Ponadto w trakcie kontroli (28 listopada 2017 r.) zaktualizowano zakres danych przetwarzanych w czterech zbiorach. (dowód: akta kontroli str. 196-199, 226-228)

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

---

[27] 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.).

[28] Jeden zbiór nie został ujętych w wykazie, ponieważ do 27 listopada 2017 r. nie gromadzono i nie przetwarzano w nim danych osobowych.

Zgodnie z regulaminem naboru na wolne stanowiska urzędnicze w Starostwie[29], warunkiem udziału w naborze na wolne stanowiska pracy było wyrażenie zgody przez kandydata na przetwarzanie danych osobowych zawartych w ofercie, niezbędnych do realizacji procesu rekrutacji. W dwóch ogłoszeniach o naborze wskazano informacje wymagane art. 24 ust. 1 ustawy o ochronie danych osobowych.

(dowód: akta kontroli str. 229-234, 353-374)

4.4. Starosta był administratorem zbiorów danych, do których dostęp posiadali pracownicy, z wyjątkiem elektronicznej wersji zbiorów „Pojazd" i „Kierowca" oraz „Ewidencja gruntów i budynków".

Dostęp do danych elektronicznej wersji zborów „Pojazd" i „Kierowca" (prowadzonych za pomocą systemu CEPiK), Starosta uzyskał na podstawie umowy zawartej 27 grudnia 2016 r. z PWPW. Zgodnie z jej postanowieniami warunkami dostępu do tych danych było m.in. wykorzystywanie dedykowanej sieci teleinformatycznej, obostrzonych środków uwierzytelniania oraz posiadanie uprawnień nadawanych przez PWPW. Z oględzin dwóch stanowisk komputerowych, na których przetwarzane były dane w elektronicznym zbiorze „Pojazd" 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.

Przetwarzanie danych w zbiorze „Ewidencja gruntów i budynków" umową powierzenia z 14 października 2011 r. przekazane zostało PODKiG. Uzyskanie dostępu do tego zbioru nie wymagało spełnienia specjalnych warunków takich, jak np. stworzenie wydzielonego łącza internetowego czy budowy określonej struktury sieci.

(dowód: akta kontroli str. 6-71, 74-75, 402-424)

Ustalone nieprawidłowości

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

1. W wykazie zbiorów osobowych, stanowiącym załącznik do Polityki bezpieczeństwa, wbrew wymogom § 4 pkt 2 rozporządzenia w sprawie dokumentacji i warunków technicznych, nie zawarto trzech zbiorów danych osobowych[30] przetwarzanych w Starostwie.

   ABI wyjaśnił, że przyczyną niezaktualizowania wykazu było niezgłoszenie przez dyrektorów Wydziałów i samodzielne stanowisko pracy faktu prowadzenia takich zbiorów. (dowód: akta kontroli str. 6-71, 196-199, 430-435)

2. W trzech zbiorach danych osobowych przetwarzano dane osobowe nie wymienione w zgłoszeniach do rejestru prowadzonego przez GIODO[31]. Stanowiło to naruszenie art. 41 ust. 1 pkt 3a ustawy o ochronie danych osobowych, zgodnie z którym zgłoszenie powinno zawierać m.in. zakres przetwarzanych danych.

   Na podstawie pkt 11.1c Polityki Bezpieczeństwa odpowiedzialność za zgłoszenie zbiorów danych do rejestracji ponosi Dyrektor Wydziału Komunikacji, która wyjaśniła, że przyczyną niezgłoszenia aktualizacji zbioru były sukcesywnie następujące zmiany przepisów. W trakcie kontroli NIK zgłoszenia do rejestru zostały zaktualizowane.

   (dowód: akta kontroli str. 229-234, 299-300)

Ocena cząstkowa

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

---

[29] Zarządzenie Starosty z 22 stycznia 2009 r.

[30] Rejestru roślin i zwierząt podlegających ograniczeniom na podstawie umów międzynarodowych, Rejestru wypadków przy pracy, Kierowania do szkół specjalnych lub ośrodków poza granicami powiatu.

[31] W rejestrach „Ewidencja stacji kontroli pojazdów i diagnostów", „Ewidencja Ośrodków Szkolenia Kierowców i Instruktorów Jazdy" oraz „Ewidencja Kierowców" przetwarzano dane o nazwisku rodowym matki, nr i serii dowodu osobistego, wizerunku, adresie poczty elektronicznej oraz wykształceniu, które nie zostały wskazane w wniosku o rejestrację 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[32], wnosi o:

1. Nadanie użytkownikom komputerów uprawnień w systemach operacyjnych odpowiadających ich zakresom obowiązków.
2. Przeprowadzanie analiz utraty integralności, dostępności lub poufności informacji raz w roku, a także po każdym zgłoszonym incydencie, stosownie do postanowień pkt IX.1 Systemu zarządzania bezpieczeństwem informacji.
3. Nadawanie uprawień do przetwarzania danych osobowych w systemach informatycznych wyłącznie pracownikom, którzy posiadają upoważnienia ADO do przetwarzania takich danych oraz niezwłoczne obieranie takich uprawnień pracownikom, z którymi rozwiązano stosunek pracy.
4. Wdrożenie narzędzi do automatycznego gromadzenia, zabezpieczenia i analizy logów dostępu do informacji.
5. Umożliwienie zdalnego dostępu firmie serwisującej składniki systemu po uzyskaniu autoryzacji i pod nadzorem administratora systemu.
6. Wywiązywanie z obowiązku wynikających z § 20 ust. 2 pkt. 14 rozporządzenia KRI przeprowadzania corocznego audytu wewnętrznego z zakresu bezpieczeństwa informacji.
7. Zaktualizowanie wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz uwzględnienie w wykazie zbiorów osobowych wszystkich przetwarzanych w Starostwie zbiorów danych.
8. Zapewnienie danym osobowym przechowywanym w archiwum i serwerowni właściwej ochrony przed działaniem czynników fizycznych i zdarzeń losowych (pożar, zalanie).

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 30 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 28 marca 2018 r.

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

podpis

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