NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.010.02.2018
P/18/006

04726418

WYSTĄPIENIE POKONTROLNE

(Wystąpienie pokontrolne z dnia 16 lipca 2018 r., zmienione zgodnie z treścią uchwały Zespołu Orzekającego Komisji Rozstrzygającej w Najwyższej Izbie Kontroli z dnia 4 września 2018 r. KPK-KPO.443.167.2018, podjętej w sprawie zastrzeżeń oraz w związku ze sprostowaniem oczywistych omyłek pisarskich)

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/18/006 – Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontroler	Piotr Jurkin – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/73/2018 z 4 czerwca 2018 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Starostwo Powiatowe w Bielsku Podlaskim, ul. A. Mickiewicza 46, 17-100 Bielsk Podlaski[1]
Kierownik jednostki kontrolowanej	Sławomir Jerzy Snarski – Starosta Bielski[2] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[3]

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, przyjęte i wdrożone rozwiązania organizacyjne oraz techniczne w zakresie zapewnienia bezpieczeństwa informacji przetwarzanych w Starostwie[4].

Uzasadnienie oceny ogólnej

Organizacja procesu zabezpieczania informacji została przeprowadzona właściwie, poprzez stworzenie szeregu polityk i procedur traktujących o tych zagadnieniach. Były one aktualizowane wraz ze zmieniającymi się przepisami prawa. Powołano Administratora Bezpieczeństwa Informacji (dalej: „ABI"), a od 25 maja 2018 r. Inspektora Ochrony Danych (dalej: „IOD"). Prowadzono też działania zapobiegawcze incydentom bezpieczeństwa informacji, poprzez wykonywanie cyklicznych audytów wewnętrznych, regularne tworzenie kopii baz danych oraz szkolenia pracowników.

Stwierdzone nieprawidłowości polegały w szczególności na:

- nadaniu jednemu (z 10 analizowanych) użytkownikowi nadmiernych uprawnień w systemie operacyjnym komputera,
- nieposiadaniu pełnych i aktualnych danych dotyczących użytkowanego sprzętu i oprogramowania oraz jego konfiguracji,
- nieopracowaniu planów: przeglądów Systemu Zarzadzania Bezpieczeństwem Informacji (dalej: „SZBI") oraz ciągłości działania,
- przetwarzaniu przez trzech (z 15 analizowanych) pracowników danych w zbiorze danych osobowych EZD Smart Doc, mimo nieposiadania niezbędnych upoważnień,
- niestosowaniu przez sześciu objętych analizą pracowników odpowiedniej jakości haseł dostępu do trzech systemów dziedzinowych,
- niezamieszczeniu w umowach na świadczenie usług poczty elektronicznej zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający ujawnienie osobom nieuprawnionym,
- niewłaściwym przechowywaniu kopii zapasowych trzech analizowanych programów oraz nieprzeprowadzaniu sprawdzeń wykonanych kopii z przyjętą częstotliwością,
- niezainstalowaniu na jednym (z 10 objętych oględzinami) stanowisku komputerowym oprogramowania antywirusowego.

---

[1] Dalej: „Starostwo".
[2] Pełniący funkcję od 16 listopada 2014 r.
[3] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
[4] Kontrolą objęty został okres od 1 czerwca 2017 r. do zakończenia czynności kontrolnych.

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. Zgodnie z wymogami § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[5] w Starostwie opracowano i ustanowiono System Zarzadzania Bezpieczeństwem Informacji. Dokumenty tworzące SZBI zostały zatwierdzone[6] przez Starostę 4 listopada 2015 r. i w dniu następnym ABI przekazał ich treść w wersji elektronicznej naczelnikom poszczególnych wydziałów Starostwa.

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)[7], 25 maja 2018 r. Starosta Bielski zatwierdził zmiany w SZBI, na który składały się: Polityka Bezpieczeństwa Informacji (dalej: „PBI"), Polityka Bezpieczeństwa Danych Osobowych (dalej: „PBDO"), Instrukcja zarządzania systemami informatycznymi (dalej: „Instrukcja zarządzania") oraz Instrukcja postępowania w sytuacji naruszenia Systemu Zarządzania Bezpieczeństwem Informacji (dalej: „Instrukcja postępowania"). Przedmiotowe dokumenty zawierały m.in.: regulaminy, procedury, wzory dokumentów, ewidencji i rejestrów wykorzystywanych w Starostwie tym zakresie. Instrukcja zarządzania zawierała m.in.: regulaminy korzystania z Internetu, poczty elektronicznej i urządzeń mobilnych, wzory ewidencji (np.: wykonywania kopii zapasowych, przenośnych nośników danych) i wniosków o nadanie / modyfikację / cofnięcie upoważnienia i uprawnień do przetwarzania danych. PBDO określała m.in.: procedury dostępu podmiotów zewnętrznych do danych osobowych oraz postępowania z danymi osobowymi w wersji papierowej i elektronicznej, zasady uzyskania oraz cofania zgód na przetwarzanie danych osobowych i komunikacji z osobami, których dane są przetwarzane. Z kolei w PBI ujęto m.in. procedury: przeglądu SZBI czy minimalizacji zakłóceń w realizacji działalności statutowej w związku z dysfunkcją systemu informatycznego, zakres zadań oraz odpowiedzialności IOD i Administratora Systemów Informatycznych (dalej: „ASI"), a także proces zarządzania aktywami i ryzykiem. W Instrukcji postępowania przedstawiono zaś m.in. metodykę działań w przypadku wystąpienia incydentów i naruszeń, w tym dotyczących ochrony danych osobowych.

(dowód: akta kontroli str. 4-228)

IOD 12 czerwca 2018 r. przekazał (w formie elektronicznej) naczelnikom poszczególnych wydziałów Starostwa dokumentację SZBI, w celu wewnętrznego rozpowszechnienia i stosowania przez podległych pracowników[8]. Przekazana dokumentacja nie zawierała szczegółów technicznych, procesów, instrukcji czy zasad zastrzeżonych dla pracowników odpowiedzialnych za zabezpieczenie techniczne. Dokumenty te nie zostały przekazane pracownikom w dniu ich uchwalenia, gdyż jak wyjaśnił IOD: *„Ogólne omówienie wprowadzonych zmian w Systemie Zarządzania Bezpieczeństwem Informacji w Starostwie Powiatowym w Bielsku Podlaskim nastąpiło w trakcie szkolenia w dniu 22 maja 2018 r. przeprowadzonego przez IOD. W kwestii szczegółowego zapoznania z dokumentacją pracowników Starostwa Powiatowego nastąpiło nieporozumienie. Po uzyskaniu informacji, że pracownicy nie otrzymali drogą e-mail dokumentacji do zapoznania się, IOD przesłał w dniu 12 czerwca 2018 r. dokumentację do zapoznania się i stosowania".*

(dowód: akta kontroli str. 229-231)

---

[5] Dz. U. z 2017 poz. 2247. Rozporządzenie zwane dalej: „rozporządzeniem KRI".

[6] Zarządzeniem nr 37/15 Starosty Bielskiego 4 listopada 2015 r., które uchylało poprzednie zarządzenie nr 25/07 z 12 marca 2017 r. w sprawie ochrony danych osobowych w systemach informatycznych.

[7] Dz.U.UE.L.2016.119.1. Rozporządzenie zwane dalej: „RODO".

[8] Identyczny zestaw dokumentów IOD rozesłał w tym samym dniu do wszystkich 87 pracowników Starostwa.

W rozdziale III pkt 7 PBI określono, że osobą odpowiedzialną za nadzorowanie, opracowanie, monitorowanie, aktualizowanie i doskonalenie SZBI w Starostwie jest IOD.
(dowód: akta kontroli str. 97-129)

1.2. Sporządzona w Starostwie dokumentacja w zakresie ochrony danych osobowych uwzględniała większość wymogów przewidzianych w RODO. W PBDO (rozdział XVII) opisano sposób realizacji i dokumentowania obowiązków i uprawnień przewidzianych ww. rozporządzeniem. Określono m.in. zasady komunikacji z osobami, których dane są przetwarzane, w tym prawo do sprostowania, ograniczenia przetwarzania, przenoszenia i usunięcia danych (art. 18 i 19 RODO). Opisano obowiązki Administratora Danych Osobowych (dalej: „ADO") w zakresie m.in. powiadamiania o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych osobowych oraz zasady uzyskiwania i cofania zgód na przetwarzanie danych osobowych. W PBDO ujęto także procedury dotyczące m.in.: [1] postępowania w przypadku wystąpienia incydentu, w tym zgłaszania naruszeń ochrony danych organowi nadzorczemu (art. 33 RODO); [2] nadawania, zmiany zakresu i anulowania upoważnień do przetwarzania danych osobowych oraz dostępu podmiotów zewnętrznych do tych danych. W rozdziale IX przedstawiono przyjęte środki i zasady ich wdrażania w celu zapewnienia bezpieczeństwa przetwarzania danych oraz opisano uwarunkowania, w których przeprowadzanie oceny skutków ochrony danych osobowych jest wymagane[9] (art. 32 RODO). W załączniku F do przedmiotowego dokumentu określono wzór rejestru czynności przetwarzania oraz zasady jego prowadzenia. W Starostwie nie opracowano rozwiązań technicznych i organizacyjnych uwzględniających ochronę danych osobowych w fazie projektowania oraz domyślną ochronę danych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 130-174, 234)

1.3. Od 31 lipca do 31 sierpnia 2017 r. ABI przeprowadził sprawdzenie w zakresie m.in.: realizacji przez pracowników Starostwa obowiązku informacyjnego, o którym mowa w art. 24 i 25 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[10] oraz procesu powierzania danych osobowych podmiotom zewnętrznym w oparciu o zawarte umowy / klauzule. Od 17 lipca do 12 września 2017 r. przeprowadzono również audyt wewnętrzny[11], którego celem była ocena zgodności stanu faktycznego bezpieczeństwa informacji w oparciu o wymogi przewidziane w rozporządzeniu KRI. W sprawozdaniu ze sprawdzenia zwrócono uwagę na konieczność zmian w zakresie ochrony danych (w tym osobowych) w związku z wejściem w życie nowych uregulowań prawnych wynikających m.in. z RODO. W efekcie opracowano i przyjęto do stosowania nowy SZBI, uwzględniający wymogi i rozwiązania przewidziane w ww. rozporządzeniu, czym spełniono wymogi przewidziane w § 20 ust. 2 pkt 1 rozporządzenia KRI.
(dowód: akta kontroli str. 235-238, 252-257)

1.4. Zgodnie postanowieniami rozdziału III PBI, odpowiedzialni za bezpieczeństwo informacji zostali: [1] ADO – Starosta Bielski, w szczególności za procesy zabezpieczania informacji / danych oraz za przestrzeganie wymagań związanych z zabezpieczeniem informacji i systemów informatycznych, [2] IOD – m.in. za nadzorowanie opracowania i monitorowanie standardów zabezpieczenia informacji przetwarzanych w Starostwie, aktualizowanie i doskonalenie SZBI, zarządzanie incydentami bezpieczeństwa informacji, opiniowanie dokumentów pod kątem zgodności z zasadami bezpieczeństwa informacji, [3] ASI – m.in. za zapewnienie prawidłowego funkcjonowania systemów informatycznych, w tym monitorowanie ich działania oraz kontrolę zgodności użytkowanych systemów teleinformatycznych z odpowiednimi normami, Instrukcją zarządzania, PBDO i PBI, [4] Administrator Systemu[12] (dalej: „AS") – m.in. za implementację mechanizmów bezpieczeństwa do administrowanego systemu, monitorowanie jego działania oraz informowanie ADO, ASI i IOD o jego podatnościach i zagrożeniach. Osoby odpowiedzialne

---

[9] Dotyczy to sytuacji: [1] przetwarzania na dużą skalę szczególnych kategorii danych osobowych, m.in. wyroków skazujących czy naruszeń prawa, [2] kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej, [3] systematycznego monitorowania na dużą skalę miejsc publicznie dostępnych.

[10] Dz. U. 2016 poz. 922, ze zm. Ustawa uchylona 25 maja 2018 r.

[11] Zrealizował go ABI.

[12] Osoba odpowiedzialna za zapewnienie prawidłowego funkcjonowania lokalnego systemu informatycznego, którym zarządza.

za bezpieczeństwo informacji (ADO, ASI i IOD) posiadały odpowiednie kwalifikacje i doświadczenie. Do dnia rozpoczęcia kontroli nie wyznaczono osoby do pełnienia funkcji AS. Według IOD przyjęta dokumentacja daje taką możliwość, jednak w wyniku bieżącej oceny potrzeb w tym zakresie nie wskazano takich osób. Zadania AS wykonuje ASI.

(dowód: akta kontroli str. 97-129, 268-269)

1.5. Na podstawie umowy z 20 czerwca 2015 r., zawartej z podmiotem zewnętrznym[13], świadczącym usługi związane z ochroną danych osobowych (w tym outsourcing ABI)[14], z dniem 26 lutego 2016 r. Starosta Bielski powołał ABI[15] (pracownika tej firmy). Starosta ustalił, że na podstawie art. 158 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[16] (dalej: „uoodo") osoba dotychczas wypełniająca obowiązki ABI będzie pełniła funkcję IOD[17], czym wypełniono obowiązek wynikający z art. 73 ust. 1 RODO. Osoba zajmująca to stanowisko ukończyła m.in. studia podyplomowe z zakresu zarządzania bezpieczeństwem informacji oraz uczestniczyła w szkoleniach i konferencjach dotyczących wdrożenia RODO czy zadań związanych z ochroną danych osobowych w stosunku do systemu zarządzania bezpieczeństwem informacji w kontekście normy PN-ISO 27001:2014-12 i rozporządzenia KRI. Ponadto w umowie wskazano, że w przypadku istotnego naruszenia jej postanowień lub narażenia Starostwa na straty przewidziano możliwość rozwiązania jej ze skutkiem natychmiastowym oraz odszkodowanie.

(dowód: akta kontroli str. 234, 270-284, 483-489)

1.6. W zarządzeniu w sprawie podziału zadań pomiędzy Starostę, Wicestarostę oraz ustalenia zadań Sekretarza i Skarbnika[18] wskazano, że Starosta bezpośrednio nadzoruję pracę ABI / IOD. Zakres jego zadań wskazano w § 29 Regulaminu Organizacyjnego[19]. Osobie pełniącej tę funkcję nie przypisano innych obowiązków w Starostwie, co wypełniało postanowienia art. 38 ust. 3 i ust. 6 RODO. (dowód: akta kontroli str. 234, 499-510)

1.7. Większość regulacji (planów, procedur, instrukcji) wymaganych w poszczególnych dokumentach składających się na SZBI, które opisano w pkt 1.1 niniejszego wystąpienia, zostało sporządzonych i zakomunikowanych pracownikom Starostwa. Do dnia rozpoczęcia kontroli nie opracowano jednak planów: przeglądów SZBI oraz ciągłości działania, tj. dokumentów przewidzianych w pkt 4 i 5 rozdziału VII PBI, a także listy stosowanych zabezpieczeń i ewidencji przenośnych nośników danych przewidzianych odpowiednio w pkt 2 rozdziału V i pkt 12 rozdziału IV Instrukcji zarządzania, co szerzej opisano w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 97-129, 175-217, 234)

1.8. Pracownikom Starostwa przekazano poszczególne dokumenty składającą się na SZBI, w tym wzory m.in. ewidencji przenośnych nośników danych, obowiązku informacyjnego, umowy powierzenia, zgód na przetwarzanie danych, będących załącznikami do poszczególnych jej części. Udostępnieniu wszystkim pracownikom Starostwa nie podlegały szczegóły techniczne dotyczące m.in. wprowadzonych zabezpieczeń (w tym wzoru listy stosowanych zabezpieczeń), planu archiwizacji i wykonania kopii zapasowych czy dokumentacji związanej z analizą ryzyka. O dostępie do danych dokumentów dla poszczególnych pracowników każdorazowo decydował ADO.

(dowód: akta kontroli str. 229-231, 286)

1.9. W Starostwie zidentyfikowano zbiory danych podlegające zabezpieczeniu. W rejestrze zbiorów danych oraz rejestrze czynności przetwarzania ujęto 47 takich zbiorów.

(dowód: akta kontroli str. 234, 298, 424-442)

---

[13] STS Elektronik Optimus S.A. Partner.
[14] Obowiązywanie umowy na kolejne dwa lata przedłużono 23 czerwca 2017 r.
[15] Zgłoszenia do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych dokonano 22 marca 2016 r.
[16] Dz. U. poz. 1000.
[17] IOD będzie pełnił swoją funkcje do 1 września 2018 r.
[18] Zarządzenie Nr 10/18 Starosty Bielskiego z dnia 16 kwietnia 2018 r.
[19] Uchwała Nr 45/175/17 Zarządu Powiatu w Bielsku Podlaskim z dnia 21grudnia 2017 r. w sprawie uchwalenia Regulaminu Organizacyjnego Starostwa Powiatowego w Bielsku Podlaskim.

1.10. W Starostwie prowadzono inwentaryzację sprzętu w formie elektronicznej[20]. W trakcie oględzin 10 komputerów stacjonarnych, dwóch laptopów, jednego serwera, routera oraz jednej drukarki, konfrontowano dane uzyskane z poszczególnych jednostek sprzętu informatycznego takie, jak: [1] system operacyjny, [2] nazwy dwóch zainstalowanych programów, [3] adres IP, [4] rodzaj zainstalowanej karty graficznej i [5] procesora, [6] nazwę jednostki i jej konfigurację, [7] liczbę zainstalowanej urządzeń peryferyjnych (drukarek) z danymi zapisanymi w prowadzonej ewidencji. W wyniku oględzin stwierdzono, że dla siedmiu jednostek sprzętu komputerowego (dwóch laptopów i czterech komputerów stacjonarnych oraz rutera) dysponowano wszystkimi informacjami, o których mowa w § 20 ust. 2 pkt 2 rozporządzenia KRI. Dla pozostałych czterech komputerów stacjonarnych, drukarki oraz serwera nie dysponowano kompletem danych w zakresie ich konfiguracji i oprogramowania. Dodatkowo analiza listy komputerów ujętych w prowadzonej inwentaryzacji wykazała, że cztery jednostki komputerowe (z 71 wykorzystywanych w Starostwie) nie zostały w niej zaewidencjonowane, co szerzej opisano poniżej, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 287-297)

Ustalone nieprawidłowości

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

1. W Starostwie, wbrew wymogom wynikającym z § 20 ust. 2 pkt 2 rozporządzenia KRI, nie posiadano pełnych i aktualnych danych dotyczących użytkowanego sprzętu i oprogramowania oraz jego konfiguracji. Prowadzona ewidencja nie zawierała informacji o zainstalowanym na czterech komputerach stacjonarnych (przydzielonych pracownikom Wydziału Budżetu i Finansów) oprogramowaniu księgowo-finansowym Tytan SQL. Nie dysponowano także żadnymi danymi o urządzeniu wielofunkcyjnym (drukarce) Kyocera Ecosys M6035cidn KX, natomiast dane dotyczące serwera ograniczały się do jego adresu IP. W prowadzonej ewidencji nie odnotowano informacji m.in. o jego systemie operacyjnym, zainstalowanym oprogramowaniu, karcie graficznej, rodzaju procesora. Dodatkowo cztery jednostki komputerowe (z 71 wykorzystywanych w Starostwie) nie były objęte inwentaryzacją zasobów informatycznych. Informatyk Starostwa wyjaśnił, że: *„Dla czterech wymienionych komputerów nie odnotowano w ewidencji / inwentaryzacji zasobów informatycznych zainstalowania programu Tytan SQL, ponieważ aplikacja ta nie posiada typowego instalatora. Jej instalacja – w uproszczeniu – polega na skopiowaniu plików na dysk twardy komputera i konfiguracji w taki sposób, by odwoływała się do bazy na serwerze. Okazało się, że system do inwentaryzacji oprogramowania Uplook nie był wstanie odnotować na liście zainstalowanych programów takiej aplikacji. W opisie stanowisk w programie inwentaryzacyjnym Uplook została uzupełniona informacja o licencji użytkowanego programu Tytan SQL. W związku ze stwierdzonym brakiem możliwości automatycznego uwzględnienia w rejestrze tego typu programów ustalono na przyszłość, że będą one odnotowywane ręcznie przy danych właściwych jednostek komputerowych zarejestrowanych w wykazie zasobów komputerowych prowadzonych w systemie Uplook. Urządzenie Kyocera Ecosys M6035cidn KX nie zostało odnotowane w prowadzonych rejestrach / ewidencjach dotyczących inwentaryzacji zasobów, gdyż nie należy ono do Starostwa Powiatowego w Bielsku Podlaskim, a jest jedynie dzierżawione. Z tego względu podjęto błędną decyzję w tym zakresie. Serwer Fujitsu Primergy TX 100 S1 został odnotowany w systemie Uplook, jednak jeszcze nie zainstalowano na nim tzw. agenta Uplook zbierającego dane i przesyłające je do bazy Uplooka. Dlatego w systemie tym nie było informacji o konfiguracji sprzętowej i oprogramowaniu zainstalowanym na tym serwerze. Wynika to z tego, iż system inwentaryzacyjny Uplook jest jeszcze w Starostwie w fazie wdrażania. Niezbędne czynności – tj. zarejestrowanie dzierżawionego urządzenia Kyocera w rejestrze zasobów oraz instalacja agenta Uplook na serwerze Fujitsu – zostaną dokonane przez ASI".* Dodał, że: *„W prowadzonej ewidencji / inwentaryzacji zasobów informatycznych nie ujęto czterech komputerów, gdyż elektroniczny system temu służący (Uplook) nie został jeszcze w pełni wdrożony. Tzw. agenci systemu Uplook na poszczególnych*

[20] Inwentaryzację sprzętu i oprogramowania prowadzono z wykorzystaniem programu *Uplook Zasoby*.

stanowiskach zostaną niezwłocznie doinstalowani, aby informacje w Uplooku były pełne i wiarygodne". (dowód: akta kontroli str. 287-297, 300-303)

2. W Starostwie nie opracowano planów: przeglądów SZBI oraz ciągłości działania, tj. dokumentów przewidzianych w pkt 4 i 5 rozdziału VII PBI, a także listy stosowanych zabezpieczeń i ewidencji przenośnych nośników danych przewidzianych odpowiednio w pkt 2 rozdziału V i pkt 12 rozdziału IV Instrukcji zarządzania. IOD wyjaśnił, że: „[...] *nie opracowano planu przeglądów SZBI z uwagi na natłok obowiązków oraz przeprowadzaną aktualizację dokumentacji SZBI. Opracowanie planu przeglądu przeprowadzone będzie w IV kwartale 2018 r. Lista stosowanych zabezpieczeń i ewidencja przenośnych nośników danych nie zostały sporządzone ze względu natłok pracy oraz absencję ASI. Zostanie to zaktualizowane po jego powrocie do pracy.*" Natomiast Naczelnik Wydziału Organizacyjno-Prawnego wyjaśnił, że: „[...] *Plan ciągłości działania, którego wzór stanowi załącznik C do przyjętej Polityki Bezpieczeństwa Informacji, nie został opracowany. Prace takie rozpoczęto, zostały one jednak przerwane ze względu na długotrwałą nieobecność Administratora Systemu Informatycznego przebywającego aktualnie na zwolnieniu lekarskim*". (dowód: akta kontroli str. 234, 298, 304-307)

3. Nie opracowano także rozwiązań technicznych i organizacyjnych uwzględniających ochronę danych osobowych w fazie projektowania oraz domyślną ochronę danych, mimo takiego wymogu przewidzianego w art. 25 RODO. IOD wyjaśnił, że: „*W Starostwie Powiatowym w Bielsku Podlaskim nie opracowano i nie wdrożono rozwiązań technicznych i organizacyjnych uwzgledniających ochronę danych osobowych w fazie projektowania, ponieważ w okresie wejścia w życie RODO nie wdrażano, nie projektowano oraz nie planowano wdrożenia nowego systemu informatycznego czy oprogramowania. Nie zmieniono również istniejącego oprogramowania, jak i nie planowano zmiany struktury sieci informatycznej czy też zakupu nowych rozwiązań. Nie dokonano natomiast takiej analizy pod kątem domyślnej ochrony danych, wskazanych w art. 25 RODO dla istniejących rozwiązań przyjętych w Starostwie Powiatowym w Bielsku Podlaskim. Spowodowane to było błędną interpretacją motywu 78 ww. rozporządzenia. Zostanie ona przeprowadzona w najbliższym możliwym terminie*". (dowód: akta kontroli str. 234, 285-286)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości organizację systemu bezpieczeństwa informacji w Starostwie. Przyjęte dokumenty w należyty sposób opisywały zasady zapewniające bezpieczeństwo danych.

2. Wdrożone i wykorzystywane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji

Opis stanu faktycznego

2.1. Uprawnienia użytkowników dziewięciu z 10 jednostek komputerowych objętych oględzinami[21] nie pozwalały na zainstalowanie nieautoryzowanego oprogramowania. Na jednym komputerze stacjonarnym nadane użytkownikowi uprawnienia umożliwiały zainstalowanie dowolnego oprogramowania, mimo że osoba ta nie była administratorem systemów informatycznych w Starostwie, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 308)

2.2. Analiza przyznanych uprawnień oraz nadanych upoważnień 15 z 87[22] pracowników Starostwa (w tym pięciu naczelników wydziałów) wykazała, że w 12 przypadkach posiadali oni odpowiednie uprawnienia do systemów informatycznych oraz upoważnienia do zbiorów danych zgodne z zakresami ich obowiązków. Trzy osoby (naczelnik wydziału i dwóch innych pracowników) nie dysponowały upoważnieniami do zbioru danych EZD[23], mimo przyznania im odpowiednich uprawnień, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

[21] Oględzinami objęto trzy laptopy i siedem komputerów stacjonarnych.
[22] Liczba pracowników zatrudnionych w Starostwie na 6 czerwca 2018 r.
[23] Elektroniczne Zarządzanie Dokumentami Smart Doc.

W Starostwie prowadzono ewidencję upoważnień do przetwarzania danych osobowych, w której odnotowywano: nazwę zbioru, datę nadania / odebrania uprawnień, zakres i identyfikator w systemie informatycznym, jeżeli dane przetwarzano w formie elektronicznej. Nadanie uprawnień 15 pracownikom odbyło się zgodnie z przyjętymi w Starostwie procedurami w zakresie nadawania, zmiany i anulowania upoważnień do przetwarzania danych, opisanymi w pkt 14 oraz rozdziale XIII PBDO odpowiednio z 4 listopada 2015 r. i 25 maja 2018 r. (dowód: akta kontroli str. 130-174, 309-310, 313-363)

2.3. W okresie objętym kontrolą pracę w Starostwie zakończyły dwie osoby. Każdej z nich zablokowano dostęp do systemów informatycznych oraz anulowano stosowne upoważnienia. Wnioski wymagane procedurą nadawania, zmiany zakresu i anulowania upoważnień do przetwarzania danych osobowych sporządzono w ostatnim dniu pracy tych osób, a faktyczne zablokowanie dostępu do systemów nastąpiło od dwóch do pięciu dni po zaprzestaniu świadczenia przez nich pracy. Naczelnik Wydziału Organizacyjno-Prawnego wyjaśnił, że: *„W jednym przypadku odbyło to się prawie niezwłocznie, a w kolejnym niewielka zwłoka wynikała ze znacznego obciążenia pracą ASI"*.
(dowód: akta kontroli str. 311-312, 364-365)

2.4. Zgodnie z *„Polityką haseł"*, opisaną w pkt 4 rozdziału IV Instrukcji zarządzania, użytkownicy systemów informatycznych Starostwa powinni stosować hasło o określonej złożoności. Zmiana haseł powinna następować nie rzadziej niż co 30 dni. Wymogi te były realizowane poprzez wprowadzenie odpowiednich ustawień w systemach operacyjnych, zainstalowanych na poszczególnych komputerach. Natomiast oględziny trzech programów[24] / systemów dziedzinowych zarządzanych przez Starostwo (*Comarch ERP Optima, Tytan SQL oraz Ośrodek*) wykazały, że w żadnym przypadku nie dokonywano okresowej zmiany haseł, a hasła do dwóch z trzech ww. systemów / programów nie odpowiadały wymogom zawartym w Instrukcji zarządzania, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 175-217, 366-367)

2.5. Usytuowanie wszystkich trzech monitorów komputerów (w Wydziale Komunikacji i Transportu) wykorzystywanych do zadań z zakresu rejestracji pojazdów uniemożliwiało osobom nieuprawnionym podgląd danych wyświetlanych na ekranach, co było zgodne z wymogami § 20 ust. 2 pkt 7 rozporządzenia KRI. (dowód: akta kontroli str. 366)

2.6. Starostwo dysponowało 12 komputerami przenośnymi. Stosownie do wymogów § 20 ust. 2 pkt 8 rozporządzenia KRI, w pkt 11 rozdziału IV Instrukcji zarządzania opracowano zasady dotyczące pracy zdalnej i przy przetwarzaniu mobilnym[25], w którym wskazano, że zgodę na tego rodzaju wykorzystywanie systemu informatycznego każdorazowo wyraża ADO, na wniosek przełożonego pracownika. Za nadanie odpowiednich uprawnień odpowiadał ASI. W dokumencie tym określono, że mobilny dostęp do systemu Starostwa m.in.: możliwy byłby po uwierzytelnieniu odpowiedniej jakości hasłem, z urządzenia wyposażonego w aktualne oprogramowania antywirusowe, a wymiana informacji odbywałaby się w postaci zaszyfrowanej. (dowód: akta kontroli str. 175-217, 368)

2.7. Na dzień kontroli w Starostwie nie stosowane było rozwiązanie polegające na szyfrowaniu danych zgromadzonych na dyskach twardych komputerów przenośnych, co szerzej opisano w dalszej części wystąpienia, w sekcji „Uwagi dotyczące badanej działalności". (dowód: akta kontroli str. 368)

2.8. Jedna z dwóch serwerowni[26] objętych oględzinami znajdowała się w budynku Starostwa w nieoznakowanym pomieszczeniu, wyposażonym m.in. w: klimatyzatory, zabezpieczone okna, czujnik ruchu. Serwerownia podłączona była do dwóch wydzielonych linii zasilania, a na wypadek przerw w dostawie energii oba serwery podłączono do urządzeń UPS. Informatyk wyjaśnił, że dostęp do serwerowni posiadały jedynie upoważnione osoby. Zagadnienie to omówiono również w dalszej części wystąpienia, w sekcji „Uwagi dotyczące badanej działalności". (dowód: akta kontroli str. 369)

---

[24] Oględzin dokonywano na dwóch stanowiskach użytkujących dane oprogramowanie / system dziedzinowy.
[25] Regulamin korzystania z urządzeń mobilnych stanowi załącznik nr E do Instrukcji zarządzania.
[26] Starostwo posiadało dwie serwerownie. W serwerowni objętej oględzinami zainstalowano także serwer Centralnej Ewidencji Pojazdów i Kierowców (dalej: „CEPiK").

2.9. W okresie objętym kontrolą obowiązywało m.in. pięć umów dotyczących dostawy usług IT, serwisu i aktualizacji programów wykorzystywanych w Starostwie do gromadzenia i przetwarzania danych, także osobowych[27]. W czterech z nich zawarto zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. Natomiast w umowie na świadczenie usług poczty elektronicznej, zawartej z podmiotem zewnętrznym[28], nie zamieszczono takich zapisów, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 298, 370-377)

2.10. Zasady postępowania w przypadku utylizacji nośników danych ujęto w *Polityce archiwizacji, kopii zapasowych i usuwania zbiorów danych i informacji oraz programów i narzędzi programowych służących do ich przetwarzania,* w rozdziale IX Instrukcji zarządzania. Wskazano w niej m.in., że przed przekazaniem do utylizacji, naprawy lub użytkowania podmiotowi zewnętrznemu komputerów lub przenośnych nośników danych stosować należy mechanizmy bezpiecznego kasowania informacji za pomocą specjalistycznego oprogramowania, fizycznego zniszczenia (pocięcie, spalenie) nośników danych lub przy użyciu demagnetyzacji.

W Starostwie 11 kwietnia 2018 r. dokonano oceny składników[29] majątku oraz przeprowadzono kasowanie informacji na zużytych jednostkach sprzętu komputerowego. Sprzęt przekazano do utylizacji specjalistycznej firmie.

(dowód: akta kontroli str. 175-217, 378-388)

2.11. W Starostwie na dzień 14 czerwca 2018 r. nie wykorzystywano komputerów z systemem operacyjnym Windows XP[30]. Aktualizacja oprogramowania do systemów informatycznych odbywała się według harmonogramów ustalonych przez dostawcę oprogramowania i wykonywana była automatycznie bez udziału pracowników, co spełniało wymogi § 20 ust. 2 pkt 12 lit. a i f rozporządzenia KRI. (dowód: akta kontroli str. 389)

2.12. W Starostwie do tworzenia i testowania kopii bezpieczeństwa wykorzystywano oprogramowanie Ferro Backup System. Częstotliwość wykonywania kopii zapasowych oraz zasad ich archiwizacji zweryfikowano dla trzech programów / systemów: *Ośrodek, Comarch ERP Optima* oraz *Tytan SQL*. Przeprowadzona analiza wykazała, że archiwizacja i wykonywanie kopii zapasowych użytkowanych w Starostwie programów / systemów odbywało się na podstawie *Planu archiwizacji i wykonania kopii zapasowych*, będącego załącznikiem nr C do Instrukcji zarządzania. Zgodnie z ww. dokumentem wykonywano je codziennie od poniedziałku do piątku (wg. ustawień po godz. 17). Kopie wykonywano i przechowywano na serwach backupowych, umiejscowionych w tych samych pomieszczeniach co serwery, na których zainstalowano ww. oprogramowanie, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Dla programu *Ośrodek* przechowywano 30 ostatnich kopii zapasowych. Dla programów *Comarch ERP Optima* oraz *Tytan SQL* przechowywano po dwie kopie bazy danych. Po przekroczeniu wymienionej liczby kopii, dane były nadpisywane począwszy od kopii najstarszych. Weryfikację wykonanych kopii przeprowadzano automatycznie w każdy piątek (wg. ustawień od godz. 21).

Zgodnie z wymogami zawartymi w *Planie archiwizacji i wykonania kopii zapasowych*, raz w miesiącu wykonywano kopie ww. programów (ręcznie na nośniki typu Blue-ray), które przechowywano w metalowej zamykanej szafie. Zgodnie z zasadami ujętymi w przedmiotowym dokumencie, dwa razy w roku należało dokonać sprawdzenia nośników kopii programów pod kątem możliwości odczytywania zawartych danych. Z zapisów w Dzienniku Administratora wynika, że ostatni przegląd kopii przeprowadzono 8 maja 2017 roku, tj. 14 miesięcy temu, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 175-217, 390-411)

---

[27] Weryfikowano zapisy umów dotyczących dostawy programów: Tytan SQL-FK, EWMAPA (Ośrodek i EWOPIS), CEPiK, oraz umów na dostawę usług internetowych i poczty elektronicznej.

[28] Umowa hostingu z „Nazwa.pl".

[29] Zutylizowano m.in. 62 zestawy komputerowe oraz dwa notebooki z lat 2000–2011.

[30] Z danych uzyskanych z programu Uplook wynika, że Starostwo dysponowało 67 komputerami, na których zainstalowane były systemy operacyjne: Windows 7, Windows 8.1., Windows 10.

2.13. Oględziny 10 komputerów (siedmiu komputerów stacjonarnych oraz trzech laptopów) wykazały, że na dziewięciu jednostkach zainstalowano oprogramowanie antywirusowe z aktualnymi definicjami wirusów. W jednym przypadku nie było przedmiotowego oprogramowania, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 412-413)

2.14. Oględziny trzech serwerów wykazały że każdy dysponował wolną przestrzenią zapisu. Zajętość przestrzeni dyskowej:

- na pierwszym z serwerów (dwudyskowym) wynosiła 6,6% i 78,2% pojemności całkowitej dla każdego z dysków;
- na drugim z serwerów wynosiła 68,8% pojemności całkowitej;
- na trzecim z serwerów (dwudyskowym) wynosiła 6,4% i 38,7% pojemności całkowitej dla każdego z dysków.

Informatyk wyjaśnił, że zajętość dysków poszczególnych serwerów sprawdzania jest w zależności od potrzeb, np. przy instalowaniu na nich nowego oprogramowania, ale nie rzadziej niż raz w miesiącu. (dowód: akta kontroli str. 310-391, 498)

2.15. W pkt 8 rozdziału IV Instrukcji zarządzania ujęto *Politykę wprowadzania zmian*, zgodnie z którą każda zmiana standardowa[31] powinna być wcześniej poddawana testom w środowisku testowym. Informatyk wyjaśnił, że zmiany w oprogramowaniu wykorzystywanym w Starostwie oraz instalacje nowego sprzętu w sieci lokalnej wprowadzano w sposób zapewniający, że będą one funkcjonować poprawnie. Instalowane oprogramowanie dziedzinowe pobierano / kopiowano na serwer lokalny z sieci lub nośników instalacyjnych, a następnie poddawano je testom w środowisku testowym (na komputerze Informatyka). Przed jego instalacją wykonywano kopię bazy danych na wypadek wystąpienia błędów po instalacji. W przypadku pozytywnych wyników testów, oprogramowanie instalowano na danej jednostce komputerowej z sieci lokalnej. Natomiast instalacja nowego sprzętu przeprowadzona była testowym podłączeniem go do komputera Informatyka. (dowód: akta kontroli str. 175-217, 416)

2.16. W Starostwie, zgodnie z obowiązkiem wskazanym w art. 30 RODO, prowadzono rejestr czynności przetwarzania danych, który na dzień rozpoczęcia kontroli liczył 47 pozycji, co opisano w pkt 1.9. niniejszego wystąpienia. W przedmiotowym rejestrze ujęto komplet danych wymaganych w ww. przepisie. (dowód: akta kontroli str. 234, 298, 430-442)

Ustalone nieprawidłowości

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

1. Uprawnienia nadane użytkownikowi jednego z 10 objętych oględzinami komputerów, umożliwiały mu instalację dowolnego oprogramowania i aplikacji, mimo że potrzeba posiadania takich uprawnień nie wynikała z zakres obowiązków tego pracownika. Stanowiło to naruszenie przepisów § 20 ust. 2 pkt 4 rozporządzenia KRI, zgodnie z którym zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, mających na celu zapewnienie bezpieczeństwa informacji. Naczelnik Wydziału Organizacyjno-Prawnego wyjaśnił, że: *„Konto pracownika [...] jest przypisane do grupy użytkowników o standardowych uprawnieniach, typu: „User" [...]. Możliwość instalacji oprogramowania na tym stanowisku nie jest wynikiem celowego działania Administratora Systemu Informatycznego, natomiast wynika zapewnie z błędnego działania systemu Windows na tym konkretnym stanowisku komputerowym. W celu usunięcia dysfunkcji systemu niezbędne będzie dokonanie przez Administratora Systemu Informatycznego zgłoszenia problemu do producenta oprogramowania Windows Serwer – firmy Microsoft".*
(dowód: akta kontroli str. 308, 417-419)

---

[31] W polityce określono trzy rodzaje zmian: [1] prosta – charakteryzująca się brakiem spadku bezpieczeństwa (np. rutynowa instalacja tego samego oprogramowania, w tej samej wersji w systemie operacyjnym o tych parametrach), [2] standardowa – charakteryzująca się ingerencją w konfigurację systemów (np. instalacja nowego systemu operacyjnego, instalacja nowego sprzętu w sieci lokalnej) oraz [3] krytyczna – zainicjowana przez incydent. Zmianę tą wykonuje się jak najszybciej w celu przywrócenia poziomu usług.

2. Trzem (z 15 objętych badaniem) pracownikom Starostwa nie wydano upoważnień, mimo umożliwienia im przetwarzania danych w zbiorze danych osobowych EZD Smart Doc, co naruszało art. 29 i art. 32 ust. 4 RODO w związku z § 20 ust. 2 pkt 4 rozporządzenia KRI. IOD wyjaśnił, że: *„Nienadanie trzem pracownikom Starostwa upoważnień do zbioru danych Korespondencja – EZD Smart Doc, mimo wypełnienia stosownych wniosków o przyznanie dostępu do tego systemu przez uprawnione osoby, wynikało prawdopodobnie z przeoczenia poprzedniego ABI (pełniącego tę funkcję do 26 lutego 2016 r.), który przygotowywał upoważnienia zgodnie z otrzymanymi wnioskami. Niezwłocznie stosowne upoważnienia zostaną tym osobom nadane"*. W trakcie kontroli NIK ww. osobom udzielono stosownych upoważnień.
(dowód: akta kontroli str. 309-310, 313-330, 420-421)

3. Oględziny sześciu stanowisk pracy (na których zainstalowano programy / systemy dziedzinowe zarządzane przez Starostwo, tj.: *Comarch ERP Optima, Tytan SQL oraz Ośrodek*) wykazały, że pracownicy użytkujący te jednostki komputerowe nie dokonywali zmiany haseł co 30 dni, a używane hasła do dwóch z trzech ww. systemów / programów nie odpowiadały wymogom zawartym w Instrukcji zarządzania, tj. posiadały liczbę znaków mniejszą od wymaganej. Stanowiło to naruszenie § 20 ust. 2 pkt 7 rozporządzenia KRI w związku z pkt 4 rozdziału IV Instrukcji zarządzania, zgodnie z którym użytkownicy systemów informatycznych Starostwa powinni stosować hasła o odpowiedniej długości i złożoności oraz zmieniać je nie rzadziej niż co 30 dni. Informatyk Starostwa wyjaśnił, że: *„Brak przestrzegania polityki haseł wynikał z niefrasobliwości pracowników. Zostali oni ponownie poinstruowani o obowiązujących zasadach haseł. W ramach możliwości w systemach informatycznych Starostwa zostaną podjęte również działania w celu zastosowania środków technicznych ułatwiających stosowanie tych zasad"*. (dowód: akta kontroli str. 175-217, 366-367, 422-423)

4. W umowie na świadczenie usług poczty elektronicznej zawartej z podmiotem zewnętrznym[32], wbrew przepisom § 20 ust. 1 i ust. 2 pkt 7 rozporządzenia KRI, nie ujęto zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający ich ujawnienie osobom nieuprawnionym. Informatyk wyjaśnił, że: *„Umowa hostingowa została zawarta jeszcze w 2005 roku i od tego momentu była rokrocznie przedłużana. Umowa została zawarta według standardowego wzorca poprzez zamówienie miejsca na serwerze i domen internetowych, a kontynuowana po dokonaniu kolejnych opłat rocznych. W związku z brakiem w umowie zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, Starostwo zwróci się do dostawcy usług o wprowadzenie stosownej zmiany w zawartej umowie [...], zgodnie z wymogiem przewidzianym w § 20 ust. 2 pkt 10 rozporządzenia KRI"*. (dowód: akta kontroli str. 298, 370-377, 422-423)

5. Częstotliwość wykonywania kopii zapasowych oraz zasad ich archiwizacji zweryfikowano dla trzech programów / systemów administrowanych przez Starostwo, tj.: *Ośrodek, Comarch ERP Optima* oraz *Tytan SQL*. Oględziny wykazały, że wykonywane kopie ww. programów / systemów przechowywano na serwach backupowych umiejscowionych w tych samych pomieszczeniach co serwery z danymi, dla których sporządzane były kopie zapasowe. Takie postępowanie narusza § 20 ust. 2 pkt 12 lit. b i e rozporządzenia KRI, a tym samym nie daje gwarancji dostępu do poszczególnych danych / informacji w przypadku awarii (zalania, pożaru), ponieważ zniszczeniu mogą ulec zarówno dane źródłowe, jak i wykonane kopie. Informatyk wyjaśnił, że: *„Dzienny backup systemów Starostwa jest bardzo duży (ok. 600 GB), gdyż bazy danych (m.in. mapy) użytkowane w Starostwie mocno się rozrosły. Poza tym backupowane są też maszyny wirtualne serwerów (czyli całe systemy serwerowe wraz z danymi) i dane z poszczególnych stanowisk komputerowych (z tygodniową częstotliwością dla danego stanowiska). Kopie zapasowe baz danych są składowane w pamięci masowej na dyskach twardych oraz dodatkowo comiesięcznie na płytach Blu-ray [...]. Na bieżący rok zaplanowano zakup macierzy dyskowej z przeznaczeniem na wykonywanie kopii zapasowych, co umożliwi łatwiejsze zarządzanie backupami. [...].*

[32] Umowa hostingu z „Nazwa.pl".

Docelowo pozwoli to na składowanie kopii zapasowych poza miejscem przetwarzania danych [...]". (dowód: akta kontroli str. 302-303, 390-391)

6. Od 1 stycznia 2017 r. do końca czerwca 2018 roku w Starostwie nie dokonano dwukrotnego sprawdzenia sporządzonych kopii zapasowych pod kątem prawidłowości ich odtworzenia, co było niezgodne z wymogami określonymi w *Planie archiwizacji i wykonania kopii zapasowych*. Z zapisów w Dzienniku Administratora wynika, że ostatni taki przegląd przeprowadzono 8 maja 2017 r, tj. 14 miesięcy temu. Informatyk wyjaśnił, że wynikało to z przeoczenia, spowodowanego natłokiem innych obowiązków.
(dowód: akta kontroli str. 302-303, 392-411)

7. Na jednym stanowisku komputerowym (z 10 objętych oględzinami) nie zainstalowano oprogramowania antywirusowego, co naruszało § 20 ust. 2 pkt 12 lit. f rozporządzenia KRI w związku z pkt 3.8. Listy zastosowanych zabezpieczeń, będącej załącznikiem do Instrukcji zarządzania, według którego w każdym systemie operacyjnym obowiązkowo musi być zainstalowane i aktywne oprogramowanie antywirusowe. Informatyk wyjaśnił, że: *„[...] nie zainstalowano oprogramowania antywirusowego wskutek niedopatrzenia Administratora Systemu Informatycznego [...].* W trakcie kontroli przedmiotowe oprogramowanie antywirusowe zostało zainstalowane.
(dowód: akta kontroli str. 175-217, 412-414, 498)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że w Starostwie nie stosowano rozwiązania polegającego na szyfrowaniu dysków komputerów przenośnych. Informatyk wyjaśnił, że nie wykonywano pracy na odległość i przy przetwarzaniu mobilnym, a w związku z tym nie było potrzeby używania oprogramowania do szyfrowania danych w tym zakresie. Należy jednak mieć na uwadze, że podstawową funkcją urządzeń mobilnych jest praca w dowolnym miejscu, z wykorzystaniem technik komunikacyjnych. A zatem nie można wykluczyć, że praca może być niekiedy wykonywana również poza siedzibą urzędu, co powoduje szereg zagrożeń dla bezpieczeństwa danych na nich zgromadzonych (np. kradzież, zagubienie). Biorąc pod uwagę, że wyniesienie tego typu sprzętu poza siedzibę urzędu bez uzyskania odpowiedniej zgody jest istotnym ryzykiem, które może wystąpić, warto rozważyć zastosowanie rozwiązania polegającego na szyfrowaniu dysków twardych urządzeń przenośnych, dzięki czemu w przypadku ich kradzieży lub zagubienia osoby postronne nie będą miały dostępu do danych na nich zgromadzonych. Najwyższa Izba Kontroli zwraca również uwagę na potrzebę przeanalizowania stosowanych metod fizycznego zabezpieczenia serwerowni, pod kątem zapewnienia wystarczającej ochrony przed dostępem osób nieupoważnionych. (dowód: akta kontroli str. 364-365, 369)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie wdrożenie i wykorzystanie rozwiązań technicznych, a także zastosowane rozwiązania organizacyjne w celu zapewnienia bezpieczeństwa informacji w Starostwie.

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W Starostwie w latach 2016 i 2018[33] przeprowadzano okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI. Natomiast nie wykonano jej w 2017 roku. IOD wyjaśnił, że: *„Spowodowane to było pracami nad nowym SZBI uwzględniającym wymogi RODO oraz jego wdrażaniem"*.

W zatwierdzonym 7 maja 2018 r. przez Starostę *Planie postępowania z ryzykiem* powstałym w oparciu o zidentyfikowane zagrożenia w poszczególnych aktywach zaplanowano działania w czterech obszarach, w których ryzyko oceniono jako nieakceptowalne. W celu zmniejszenia poziomu ryzyka do akceptowalnego dla poszczególnych obszarów zaplanowano działania korygujące. Naczelnik Wydziału Organizacyjno-Prawnego wyjaśnił, że: *„W Starostwie nie przystąpiono jeszcze do realizacji wytycznych wynikających z Planu postępowania z ryzykiem z powodu wdrażania nowego SZBI uwzględniającego wymogi RODO oraz długiej absencji ASI. Do następnego przeglądu wszystkie zalecenia zostaną zrealizowane"*. (dowód: akta kontroli str. 234, 364-365, 445-463)

[33] 22 lipca 2016 r. i 7 maja 2018 r.

3.2. Realizując wymagania określone § 20 ust. 2 pkt 13 rozporządzenia KRI, opracowano i przyjęto do stosowania Instrukcję postępowania w sytuacji naruszenia SZBI, w której w rozdziale III opisano zdarzenia zakwalifikowane jako incydenty bezpieczeństwa informacji i naruszenia ochrony danych osobowych, a w rozdziale IV ww. dokumentu opisano sposób postępowania w związku ze zgłaszaniem takich naruszeń. Jednocześnie zobowiązano IOD do prowadzenia w formie elektronicznej rejestru incydentów bezpieczeństwa, w którym rejestrował on wszystkie zgłaszane mu incydenty (również przekazane osobiście lub telefonicznie). Do przedmiotowej instrukcji załączono wzór zgłoszenia naruszeń ochrony danych osobowych / incydentów do organu nadzorczego. Naczelnik Wydziału Organizacyjno-Prawnego wyjaśnił, że okresie objętym kontrolą w Starostwie nie odnotowano incydentów związanych z naruszeniem bezpieczeństwa informacji.
(dowód: akta kontroli str. 218-228, 364-365, 464-467)

3.3. Od 20 do 21 października 2015 r. 81 (z 90[34]) pracowników Starostwa uczestniczyło w szkoleniu w zakresie ochrony danych osobowych oraz bezpieczeństwa informacji, które zakończono testem kompetencji. Pozostałe osoby zostały przeszkolone z tego zakresu 2 grudnia 2015 r. Ponadto 21 kwietnia 2017 r. dwóch pracowników Starostwa odbyło szkolenie dotyczące m.in.: zasad stosowania środków zapewniających bezpieczeństwo informacji oraz urządzeń i oprogramowania minimalizujących to ryzyko, stosowania polityki haseł, bezpieczeństwa w systemach teleinformatycznych oraz zagrożeń bezpieczeństwa informacji występujących w zawiązku z ich użytkowaniem czy zasad bezpiecznego użytkowania sprzętu IT. Na szkoleniu tym omawiano także zagadnienia związane z wprowadzeniem RODO. Realizując powyższe działania, Starostwo wypełniło obowiązek wskazany w § 20 ust. 2 pkt 6 rozporządzenia KRI. Naczelnik Wydziału Organizacyjno-Prawnego wyjaśnił, że: „[...] *nowi pracownicy przed przystąpieniem do wykonywania obowiązków przechodzą indywidualne szkolenie z zakresu ochrony danych oraz zasad bezpieczeństwa przy ich przetwarzaniu. Szkoli ich IOD*".
(dowód: akta kontroli str. 364-365, 468-471)

3.4. Stosownie do wymogów przewidzianych w § 20 ust. 2 pkt 14 rozporządzenia KRI, w Starostwie od 27 lipca do 17 sierpnia 2016 r. oraz od 31 lipca do 31 sierpnia 2017 r. przeprowadzano audyty wewnętrzne z zakresu bezpieczeństwa informacji. W obu przypadkach wykonał je podmiot zewnętrzny. W trakcie przeprowadzania czynności audytowych stwierdzono nieutrzymywanie aktualnej inwentaryzacji sprzętu i oprogramowania oraz zalecono zastosowanie oprogramowania antywirusowego na wszystkich użytkowanych komputerach, co – jak wykazano w pkt 1.10. i 2.13. niniejszego wystąpienia – nie zostało do końca zrealizowane. Naczelnik Wydziału Organizacyjno-Prawnego wyjaśnił, że wynikało to z wprowadzania zmian do SZBI uwzględniających zalecenia RODO oraz długiej absencji ASI w pracy. Oprogramowanie antywirusowe zostało zainstalowane, a w najbliższym czasie proces wdrożenia systemu służącego do utrzymania aktualności inwentaryzacji sprzętu i oprogramowania zostanie ukończony. (dowód: akta kontroli str. 239-267, 364-365)

3.5. Wyjaśniając przyczyny niewykonania analizy prowadzonych procesów przetwarzania danych osobowych oraz braku oceny zapewnienia ich bezpieczeństwa w stosunku do stwierdzonych ryzyk, IOD podał: „*Art. 32 ust. 1 RODO ogólnie wskazuje obowiązki Administratora w przypadku przeprowadzenia analizy ryzyka w zakresie prowadzonych procesów przetwarzania, nie wskazując szczegółów. Mając na uwadze postanowienia art. 35 ust. 4 RODO, dotyczące oceny skutków dla ochrony danych, która jest realizowana w oparciu o wykaz rodzajów operacji ustanowiony i podany do publicznej wiadomości przez organ nadzorczy, w myśl art. 172 uoodo, który mówi: „Prezes Urzędu wyda pierwszy komunikat, o którym mowa w art. 54 ust. 1 pkt 1, w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy". Oczekujemy na decyzję Prezesa Urzędu Ochrony Danych Osobowych, wskazującą dla jakich operacji należy przeprowadzić analizę prowadzonych procesów przetwarzania danych osobowych*". (dowód: akta kontroli str. 472-473, 498)

[34] Liczba pracowników zatrudnionych w Starostwie na dzień 21 października 2015 r.

3.6. W dniu 22 maja 2018 r. 71 (z 87) pracowników Starostwa odbyło szkolenie z zakresu ochrony danych osobowych po zmianach wynikających z unijnych norm prawnych oraz prawa krajowego. Obejmowało ono m.in. takie zagadnienia, jak: [1] definicje wynikające z RODO stosowane w ochronie danych osobowych i bezpieczeństwie informacji, [2] przesłanki legalności przetwarzania danych, [3] powierzanie danych, [4] rejestrowanie czynności przetwarzania, [5] obowiązek informacyjny według RODO, [6] zasady postępowania w przypadku wystąpienia naruszeń ochrony danych, [7] podstawowe zabezpieczenia informatyczne i fizyczne obszaru przetwarzania danych, [8] odpowiedzialność cywilna, karna, administracyjna wynikająca z RODO i uoodo, [9] działania zwiększające świadomość personelu. (dowód: akta kontroli str. 474-481)

Ustalone nieprawidłowości

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

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działania Starostwa dotyczące zapobiegania incydentom bezpieczeństwa informacji.

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[35], wnosi o:

1. Prowadzenie aktualnej i kompletnej inwentaryzacji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację.
2. Wywiązywanie się z obowiązków określonych w § 20 ust. 2 pkt 4 i 7 rozporządzenia KRI.
3. Opracowanie planów: przeglądów SZBI oraz ciągłości działania, a także listy stosowanych zabezpieczeń i ewidencji przenośnych nośników danych.
4. Wdrożenie rozwiązań technicznych i organizacyjnych uwzględniających wymogi przewidziane w art. 25 RODO.
5. Zawarcie w umowie na świadczenie usług poczty elektronicznej zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający ujawnienie osobom nieuprawnionym.
6. Podjęcie działań w celu przechowywania wykonanych kopii programów / systemów w sposób gwarantujący dostęp do poszczególnych informacji w przypadku awarii lub zdarzenia losowego, zgodnie z założeniami określonymi w § 20 ust. 2 pkt 12 lit. b i e rozporządzenia KRI.
7. Sprawdzanie kopii programów / systemów wykonanych na nośnikach Blue-ray pod kątem możliwości odczytywania zawartych tam danych, zgodnie z założeniami przyjętymi w *Planie archiwizacji i wykonania kopii zapasowych.*

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.

[35] Dz. U. z 2017 r. poz. 524, ze zm. Ustawa zwana dalej „ustawą o NIK".

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK, proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Białystok, dnia 27 września 2018 r.

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

.....
podpis